

FINAL REPORT

Internet Security – Information Sharing and Analysis
Organization (IS-ISAO) Pilot Program 18PDSA000002



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Protection Through Partnership

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Report date	Project Name	Submitted by
March 31, 2020	Internet Security – Information Sharing and Analysis Organizations (IS-ISAO) Pilot - 2018	<p>Joshua Belk <i>Executive Director, LA Cyber Lab</i> jbelk@lacyberlab.org 213-978-3125</p> <p>Christopher Covino <i>Project Lead & Grant Representative</i> christopher.m.covino@lacity.org 213-978-0689</p>

PROGRESS REPORTING PERIOD	FEDERAL AGENCY	RECIPIENT ORGANIZATION
October 1, 2019 – March 31, 2020	U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)	Los Angeles Cyber Lab, Inc. 200 N Spring Street, STE 303 Los Angeles, CA 90012-3239

GRANT PERIOD	FEDERAL GRANT	DUNS & EIN
September 30, 2018 – March 31, 2020	18PDSAO00002	<p>DUNS - 081371107</p> <p>EIN - 83182160</p>

This report was prepared by the Los Angeles Cyber Lab, Inc. in cooperation with the City of Los Angeles, the Mayor’s Office of Public Safety for Los Angeles Mayor, Eric Garcetti, and with the support of its members OSPEC360, TruSTAR, IBM, and The Rosslyn Group.

Mandatory Statements

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 18PDSAO00002-01-00.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of the U.S. Department of Homeland Security.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Table of Contents

Overview.....	1
Mission	2
Vision	2
Structure	2
Review of Grant Objectives	2
Key Performance Metrics	3
LA Cyber Lab Use Cases	4
LA Cyber Lab Outreach	5
Bi-Lateral Cybersecurity Information Sharing	7
The Questions.....	8
Background Research	8
Hypothesis	9
The Pilot Program	9
Pilot Project Timelines	10
The Case For Information Sharing	11
Benefits of Cyber Threat Intelligence	12
Establish a Fully Functional IS-ISAO	15
Threat Intelligence Platforms (TIP).....	17
Threat Intelligence Platform Capabilities	17
Operational Deployments	19
Types of Threat Intelligence	19
The Threat Intelligence Lifecycle	20
LACL Threat Intelligence Sharing Platform (TISP).....	22
Sharing Threat Information	24
XFE Threat Intelligence Sources	27
Risk Score Calculation.....	27
IBM Sourced Content Contributing To The Risk Score	28
Understanding The Risk Score	28
Traffic Light Protocol	29
Generating and Sharing Analytic Reports	31
Categorizing Indicators & MITRE ATT&CK.....	31
How to Share and Export Information with the TruSTAR Platform	35

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Data Format and Transport Standards	40
Minimum Technical Requirements	40
Integrating with the TruSTAR Platform	41
LACL Mobile Application.....	46
Understanding The Risk Score.....	49
Products and Services.....	50
Identify Barriers to Information Sharing	53
LA Cyber Lab Overview and Progress	53
Impacts of the Pilot Project What is the impact of the project? How has it contributed?	63
Develop Documentation	65
Policies, Procedures, Techniques	65
Social Media Outreach	67
Work with Academic Partners.....	69
Cyber Work Force Development	73
LACL Sustainability & Future Recommendations	75
LACL Conclusions	80
Appendix A – Financial Accounting	82
Appendix B – Outreach Activities	84
Appendix C – Pilot Project Participants	89
Appendix D – CTI Sharing Partners.....	94
Appendix E – TISP Value Proposition.....	98
Appendix F – LACL In Publications & Media.....	104
Appendix G – List of Known ISAOs/ISACs	106

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

(THIS PAGE INTENTIONALLY LEFT BLANK)

“Information sharing is the thoughts and prayers of the cybersecurity community.”

- Ms. Jordan Rae Kelly, Former National Security Council Director of Cyber Incident Response

Overview

The Los Angeles Cyber Lab, Inc. (“LACL” or “Cyber Lab”) is a 501(c)3 California Nonprofit Public Benefit Corporation formed in August 2017 and located in the Los Angeles downtown area. The LA Cyber Lab is a first of its kind public-private partnership and operates with the motto *“Protection Through Partnership.”*

The LA Cyber Lab is dedicated to sharing the latest cybersecurity threat intelligence and alerts gathered by the City of Los Angeles and its public and private partners. A board of advisors, led by Mayor Eric Garcetti and consisting of leadership from over 30 cross-sector businesses and government entities, develops policies and practices to help guide the Cyber Lab’s mission. Membership in the Los Angeles Cyber Lab is open to all business and residents at no cost.

The LACL is recognized by the Department of Homeland Security (DHS) as an Internet Security – Information Sharing and Analysis Organization (IS-ISAO). As such the LACL regularly communicates threat information to its members and builds greater alliances within the public and private sector business community. The LACL currently operates direct, bilateral channels with the Multi-State Information Sharing and Analysis Center (MS-ISAC). These engagements will allow the IS-ISAO to be integrated in a community of industry-leading cyber experts which will benefit the lab’s private sector members, and ultimately with state, local, tribal and territorial (SLTT) governments.

LACL’s core initiative is the mutual exchange of cyber threat intelligence (CTI) across private and public sectors, creating collaborative, real-time identification and analysis of threats by the City of Los Angeles, businesses of all sizes, and state and federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA). In addition to information-sharing, the Cyber Lab performs widespread outreach activities including offering research and development opportunities for academia, job opportunities for entry-level, career training for professionals, and innovative conferences and events for all customers and stakeholders. It is dedicated to protecting personal and proprietary information from malicious cyber threats by facilitating and promoting innovation, education, and information-sharing between Los Angeles’ public and private sectors.

Since founded in 2017, the Cyber Lab has engaged more than 500 small, medium, and large-size businesses in the Los Angeles region, and expanding to establish strategic cross-sector partnerships across the state and nation. The Cyber Lab currently pulls Indicators of Compromise (IOCs) from all departments of the City of Los Angeles and multiple large Los Angeles based private corporations and pushes those IOCs to CISA through their Automated Information Sharing (AIS) platform. The LACL shares its IOC reports to the public on a daily basis, helping businesses across the region protect themselves from newly discovered cyber threats. LACL’s outreach efforts have effectively engaged hundreds of cybersecurity professionals, students, academics, and policymakers, and have received positive feedback from the community.

Mission

The mission of the LACL is to provide the greater Los Angeles business community and local government organizations with greater cybersecurity awareness and access to trained and capable workforce.

Vision

LACL is shaping the Cybersecurity ecosystem in Los Angeles through information sharing and workforce development as a center of excellence.

Structure

The LACL is located at 200 N. Main Street, STE 303, Los Angeles, California 90012. The LACL is staffed by contractors and fellows who perform the following roles: Executive Director, Program Director, Policy Director, Outreach Director, Senior Cyber Analyst, Data Scientist, Program Specialist, and Policy Specialist. These roles supported the LACL in its initiatives towards this pilot program. These roles were funded through the pilot program with the exception of the two specialist roles (fellows) which were provided as in-kind support by LACL's members. Technical development and support for the creation of the LACL information sharing tools was completely outsourced for this project.

The award for this grant was \$2,992,863.00, no additional funds were added to this grant during this period and all funds were expended following the guidelines provided for with the notice of the grant award. The pilot program budget was amended and approved twice in accordance with requested extensions.

The LACL is managed by a board of directors and three officers (president, secretary, treasurer) who are responsible for the oversight and financial responsibilities of the organization. The majority of these tasks were delegated to the LACL staff. Additionally, a board of advisors, exists to provide the LACL support in networking, fund raising, outreach, technical guidance, and business leadership. The Advisory Board consists of public and private sector organizations and is by invitation only, there is no fee to participate in the advisory board and a full list of organizations involved is listed on the LACL website under the "about us" section (<https://www.lacyberlab.org/advisory-board/>).

Review of Grant Objectives

The nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share information and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.

The purpose of this financial assistance action was to establish a pilot program to create the IS-ISAO to explore and evaluate the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education,

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

research and development for the improvement of SLTT government capabilities and capacity. The IS-ISAO will develop the full capability to perform information sharing and analysis of cybersecurity threats, gather, and disseminate government and critical infrastructure information, for the purpose of:

- Cyber threat analysis and information sharing
- Education/training/workforce development
- Technical research and development to support effective information sharing
- Share best practices IS-ISAO will promote and develop a collaboration

Pursuant to these goals, the following grant objectives and key performance metrics for the pilot program were established as follows:

IS ISAO Grant Objectives		
No.	Grant Objective	Grant Objective Description
1	Bi-Lateral Cybersecurity Information Sharing	Explore the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of SLTT government capabilities and capacity.
2	Establish Fully Functional IS-ISAO	Establish a fully functional IS-ISAO that can allow real time or near-real time sharing of cyber threat information between IS-ISAO and CISA.
3	Identify Barriers to Information Sharing	Identify barriers to cyber information sharing in DHS' AIS and how do we incentivize SLTT to share both with the government and one another to improve the collective defense posture of the nation and key private sector entities.
4	Develop Documentation	Develop documentation including design, policies and procedures, CONOPS, and operations manual(s).
5	Work with Academic Partners	Work with academic partners who will utilize the IS-ISAO operation center to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology.
6	Cyber Work Force Development	Develop hands-on cyber work force development programs in collaboration with academia.

Key Performance Metrics

Measurements/Targets	Threshold	Objective	Current	Current - Objective	Objective Status	Outcome
----------------------	-----------	-----------	---------	---------------------	------------------	---------

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Number of New members	10 - 50	50	277	227	Exceeded	
Number of Private Sector / Business Members	10-50	50	307	257	Exceeded	
Number of Federal Government members	0	0	4	4	Exceeded	
Number of State Government members	5-10	10	5	-5	Under	
Number of Local Government Members	5-10	10	44	34	Exceeded	
Number of Tribal Members	4-6	6	0	-6	Under	
Number of Territorial Members	0-1	1	0	-1	Under	
Number of Fusion Members	4-6	6	6	0	Met	
Number of Academia Members	1-2	2	26	24	Exceeded	
Number of Other Members*	4-6	6	96	90	Exceeded	
Number of Foreign Members	0	0	9	9	Exceeded	
Number of Individuals Representing Total Membership	10 - 50	50	543	493	Exceeded	
Average monthly growth rate	1% - 2%	2%	13.26%	11.26%	Exceeded	
Number of outreach (conference or event) presentations	2 - 4	4	29	25	Exceeded	
Number of cybersecurity tool training events	1 - 2	2	7	5	Exceeded	
Number of Membership Online Teleconference Calls	2-4	4	4	0	Met	
Number of Situational Awareness Room Events	1-2	2	3	1	Exceeded	

* Other Members are defined as private citizens receiving information from the LACL
% of net increase / decrease in membership

LACL Use Cases

A series of use cases were defined by the LACL to help guide its approach to information sharing during the pilot project. Several programs and themes were developed which further defined these use cases. Namely, the idea of information sharing was defined along with threat intelligence sharing, and public-private partnerships all became a theme under the larger strategy of connecting the community. LACL sought to find disarming ways to connect with a skeptical cybersecurity workforce. Often there were generalized and vague discussions about the limitations of what we were attempting, the impacts the pilot program might have on protecting organizations, and worthiness of this effort in its entirety were questioned. Developing good use cases became the key to defining the deliverables of the LACL and its ability to succeed.

Use Case #1: Connecting the Community - bring technology professionals, businesses and municipalities together to discuss cybersecurity related topics. LACL is in its infancy compared to many older, more established organizations. The benefit being that it remains flexible in many ways and able to adapt to

a variety of audiences, organizations, and establishments. Organizations rarely connect with the intent to provide protection to each other, but since people seeing the benefit of friendly neighbors and good samaritans are more inclined to collaborate. The basic psychology of group dynamics often lends itself to people's perceptions of what is happening and results in more inclusivity. By placing LACL at the center of groups, organizations, and people it would be in the position to increase its relevance within the community, build its brand, and foster greater interest in information sharing.

Use Case #2: Public-Private Partnerships - establish trust and confidence among technology professionals, business leaders, and government employees. LACL began with the strong support of the Mayor and City of Los Angeles. It had an advisory board and limited business connections within the community. Trust is a critical component in the cybersecurity industry, perhaps more so than in regular business because cybersecurity professionals often know about vulnerabilities which could have devastating impacts. These industry professionals occupy positions of trust within their organizations and are naturally apprehensive about collaborating with foreign (anyone outside their organization) groups. Skepticism is a common professional trait among them. No cybersecurity professional has the ability to master all aspects of the industry which creates the need to collaborate. LACL recognized the limitations among knowledge, skills, and resources which every organization struggles with and identified opportunities to create relationships beneficial to the parties involved.

Use Case #3: Threat Intelligence Sharing - promote the bidirectional exchange of cybersecurity information to protect municipalities, SMBs, and organizations. Every organization has a need for cybersecurity and one component of a mature security program is threat intelligence. Commonly among larger security teams, analysts will collaborate and share tools, tactics, and procedures. It is uncommon for these analysts to work with analysts outside their organization. Threat feeds exist in free to download and paid versions, there are known limitations within threat data, and no one threat feed can be the all-in-one source. LACL identified a robust group of sources to include within its feed which increased the value of LACL data and to differentiate itself from similar threat feeds.

LACL Outreach

A critical component to the success of the pilot program was the LACL's ability to get the word out about CTI sharing and organically grow the LACL's membership. The LACL began attending and participating in local conferences. For the first 11 months LACL promoted the CTI sharing as a concept while the design, construction and launch of the TISP occurred. Thereafter, the LACL promoted genuine information sharing amongst public-private sectors. During the pilot project the LACL staff engaged in 46 events to promote information sharing and collaboration. Through these events the LACL supported its use cases and the grant objectives. The LACL outreach strategy was designed to 1) evolve the LACL brand, 2) increase the credibility and legitimacy of the LACL, 3) be informative, and 4) to drive information sharing.

Outreach events included the following: webinars, video teleconferences, face to face meetings, conferences, seminars, public meet-ups, teleconferences, and training. Outreach methods included

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

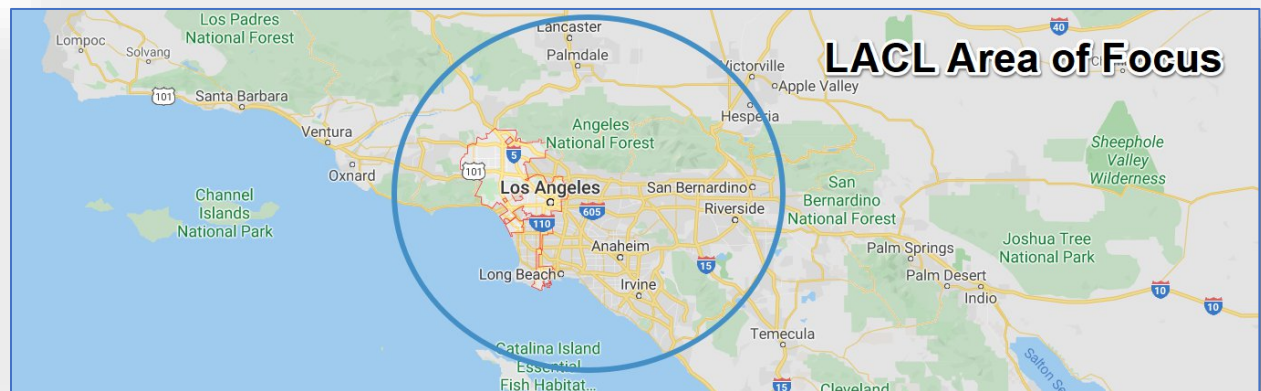
the use of social media, email, telephone, fliers, ads, short films, and publications. The LACL worked with its Advisory Board to host a series of trainings during the pilot project. These training sessions consisted of hands-on labs for cybersecurity professionals, ranging from novice to advanced skill levels and are further discussed in the “*Cyber Workforce Development*” section.

LACL Security Summit 2019: LACL launched the TISP and mobile app to increase information sharing and public-private sector partnerships on 9/17 & 9/18; over 350 attendees from SLTT, academia, and business communities participated. There were 527 registered attendees, we have confirmed 40 speakers, 5 moderators and Mayor of Los Angeles, Eric Garcetti provided the welcome address and keynote. Themes for the event include the following categories: aviation security panel, privacy and law discussions, space security panel, cybersecurity risk and best practices along with at least one panel focused on women in tech. CISA Region 9 representative moderated several panels and the LACL Executive Director provided multiple presentations all focused on information sharing via the TISP or mobile app. The overall event was very successful as it greatly increased the awareness of the LACL in the community and provided a positive experience for all.

Bi-Lateral Cybersecurity Information Sharing

Explore the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of SLTT government capabilities and capacity.

The LACL conducted a pilot program over the course of 18 months, from October 1, 2018 through March 31, 2020. The pilot program focused initially on the greater metropolitan area of Los Angeles encompassing the five counties of Los Angeles, Orange, Ventura, San Bernardino, and Riverside. The Los Angeles Cyber Lab is located at 200 North Main Street, Suite 303, Los Angeles, California 90012 and operates as a 501(c)3 non-profit/public benefit corporation. The LACL is a virtual lab and shares a close relationship with the City of Los Angeles and the Mayor of Los Angeles. During the program period the LACL made use of a DHS CISA \$2,992,863.00 grant to perform the pilot project.



The purpose of this pilot was to examine information sharing methods for CTI amongst public and private sectors and to identify challenges or obstacles related to CTI sharing. The intent and vision of this pilot was to potentially create or design methods (tools, tactics, procedures) to mitigate CTI sharing constraints and establish a model for future CTI sharing endeavors. CTI sharing is widely believed to be the next logical step in the establishment of a national collective cyber defense strategy. Private sector participation is voluntary and public sector resources are limited. Creating connections between these groups by which they might gain greater access to CTI and thereby begin implementing security strategies and processes faster would result in decreases of cyber-crime, data breaches, and economic losses.

Utilizing the scientific method to explore the most effective methods for bi-lateral cybersecurity information sharing, (focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of SLTT government capabilities and capacity to collaborate with the private sector) a series of questions were developed.

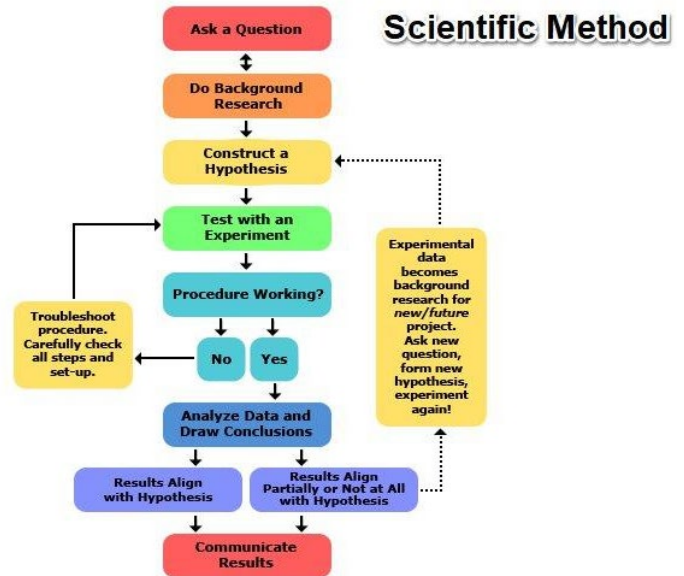
The Questions

- What existing examples exist of public - private sector threat intelligence sharing?
- How do we share information [CTI] between public and private sectors?
- How do we do it better [defined as increased ease of sharing and gaining greater participation]?

Background Research

The nature of the cybersecurity threats in the United States mandates the need for leadership in preventing, mitigating, and recovering from adverse events in cyberspace. As the recent attacks on the cities of Atlanta, Baltimore, New Orleans, and 23 municipalities in Texas, Equifax, Sprint, Yahoo! and Capital One, all indicate a critical need for enhanced bilateral information sharing and collective cyber defense. The Los Angeles metropolitan area is the 13th largest metropolitan area in the world and the second-largest metropolitan area in the United States with nearly 18 million inhabitants.¹ Over 460,000 businesses and 1,000 public SLTT organizations in the region contribute to the largest economy in the United States.²

Existing efforts in CTI sharing were reviewed and briefly evaluated as to not recreate an existing model. Several of the most prominent efforts existing in CTI sharing are CISA AIS (Automated Indicator Sharing)³, FBI's Infragard⁴ and Cyberhood Watch, and MS-ISAC⁵ (Multi-State Information Sharing and Analysis Center); additionally, there are numerous existing CTI feeds both open source (OSINT) and commercially available (e.g. IBM X-Force Exchange⁶, CISCO TALOS⁷, Symantec DeepSight⁸). However, each of these has limitations which impact adoption and information sharing. Additionally, is the



¹ United States Census Bureau, 2017.

² <https://www.latimes.com/business/story/2019-12-19/los-angeles-largest-economy>

³ <https://www.us-cert.gov/ais>

⁴ <https://www.infragard.org/>

⁵ <https://www.cisecurity.org/ms-isac/>

⁶ <https://exchange.xforce.ibmcloud.com/>

⁷ <https://talosintelligence.com/>

⁸ <https://www.symantec.com/services/cyber-security-services/deepsight-intelligence>

movement to create ISAOs⁹ across the country. These ISAOs are, with few exceptions, limited in their ability to share information or have a meaningful impact on CTI sharing because they lack resources, experience, and direction. A brief review of existing ISAC and ISAOs uncovers a vast web of organizations, not all organizations are even focused on CTI sharing, and of those that are, the majority of these groups were focused on a specific industry. There are no comprehensive efforts to connect existing ISAOs and ISACs to create synergistic efforts in CTI sharing or cyber defense. At best, these organizations communicate ad hoc and irregularly. Our research failed to identify any existing organization with the charter to share CTI across public and private sectors. Existing ISACs/ISAOs either serve only public sector organizations or focus on one niche area of industry.

CTI is a highly involved and technical discipline which requires a great deal of organizational resources to be effective. It is often reserved for only the largest organizations due to available budgets and the ability to attract and retain skilled professionals. Security architectures are designed based upon the priority of current leadership and often lack a comprehensive and strategic vision. Gaps exist even among the most advanced organizations. Medium organizations do not have mature security programs and generally lack the ability to implement tools or techniques needed to protect their environments. Small organizations are even more limited in their ability to protect themselves and range between outsourcing their security needs or not addressing them at all.

Hypothesis

LACL is an Internet Security - Information Sharing and Analysis Organization (IS-ISAO) providing a means of CTI sharing across all sectors and industries, public and private which can be emulated by other cities.

The Pilot Program

In partnership with the City of Los Angeles and Los Angeles Mayor Eric Garcett, the LACL established a network of private sector subject matter experts and leaders with ties to the information technology industry, creating a unique partnership aimed at protecting the business community of Los Angeles. The intent of the LACL was to create a regional CTI sharing model which could serve as an example for other cities to emulate across American and internationally.

The LACL embarked on a journey over the duration of 18 months to discover the elements of success and failure associated with CTI sharing. During this period, LACL emphasized a focus on how to advance the cyber threat intelligence sharing ecosystem by reimagining the tools, tactics, and procedures associated with CTI sharing. Recognizing that existing and previous efforts in CTI sharing have struggled in adoption, impact on small and medium business, and overall have had limited success; LACL sought to connect the community and find ways to surpass these obstacles.

In order to connect public and private sectors, the LACL created an IS-ISAO, established a threat intelligence sharing platform (TISP), launched a mobile application and conducted outreach to the

⁹ <https://www.isao.org/>

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

greater Los Angeles community. The pilot program connected with 800 organizations and over 2,000 individuals. Attempting to problem-solve CTI sharing was not easy and the LACL creatively approached this challenge by recruiting a top industry leader to represent the LACL and provide visionary guidance as the Executive Director. The LACL staff of six contractors and three fellows planned and executed all the business tasks of the Los Angeles Cyber Lab.

From October 2018 through February 2019, the LACL began organizing its plans, recruiting staff and forming the concept of operations which would become the vehicle by which organizations would share via the IS-ISAO. Over a period of six months from March to September 2019 the LACL managed the creation of the LACL mobile application, TISP and hosted Los Angeles’ first major cybersecurity conference, the LACL Security Summit 2019. Managing three major projects under 120 days through an agile process was extremely difficult as the LACL initially intended to meet a project deadline of September 30, 2019. While the LACL successfully completed these projects within the timeline, the true benefits of the TISP were not realized and three-month extension was granted to allow LACL to continue engaging organizations to participate in CTI sharing. During this period, LACL was able to onboard four organizations completely and had begun dialogs with another 21 interested organizations. A final three-month extension approved to give the LACL time to complete these dialogs and fully explore obstacles to CTI sharing.

45 organizations (public and private) were engaged during the pilot program to participate in CTI sharing through the TISP. Of these organizations six successfully completed the process of bidirectional information sharing. Details of the LACL TISP, the LACL mobile application, and LACL services can be found in the “Establishing a Fully Functional ISAO” section of this report. The LACL participated in extensive outreach and grew its total individual membership to 543 with a membership of 307 unique organizations.

Pilot Project Timelines

Project Date	Goal	Actual Date	Notes
April 10, 2019	Closing of RFP	April 10, 2019	
April 19, 2019	Complete internal review of the vendor proposals	April 19, 2019	
May 10, 2019	Interview vendors	May 10, 2019	
May 15, 2019	Award contract	May 20, 2019	Formal notice to non-selected vendors took longer than expected.
May 2019	Execute Contract with Vendor	August 26, 2019	IBM took 89 days to finalize the contract which greatly impacted the timeline of the partner onboarding.
June 6, 2019	Project Kickoff Meeting	June 6, 2019	
July 3, 2019	Kickoff +30 days – Complete Use Cases,	July 3, 2019	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

	identify data flows and cloud infrastructure, design platform and interface.		
August 1, 2019	Kickoff +60 days – Identify analytical tool(s) and reports, test utilization and data flows.	September 1, 2019	Data flows from the mobile application could not occur until the application was built; IBM would not test until a contact was in place.
September 1, 2019	Kickoff +90 days – Complete data flows, incorporate partner integration, create interface, platform and access controls.	March 31, 2020	Onboarding partners became more complex than originally anticipated, as documented in the obstacles to information sharing section of this report.
September 30, 2019	Kickoff +120 days – Complete project	March 31, 2020	Two extensions were provided to complete the project.

Metrics: (include membership growth / sector diversity)

The Case For Information Sharing

We are all part of the cyber ecosystem. Threats are evolving daily, and security needs to evolve in a similar manner to protect us. We each have a responsibility to protect our data, but we can also be socially responsible by getting involved with the LACL. The LACL information sharing initiative brings together the best of industry and government and you, to protect our communities and our economy from cyber-crime. Through the crowdsourcing of CTI, LACL provides public and private sector partners the opportunity to increase their response to cyber-attack and build a collective cyber defense.

Crowdsourcing CTI isn't a new concept it has existed within the industry since at 2010 and there have been and are many efforts from the government and security companies to collaborate in this manner. The majority of these efforts have fallen short of their intended goal either because of a lack of participation or for a lack of strategy. The LACL believes the best way to protect our communities is through the sharing of information related to cyber attacks and criminals. Crowdsourcing is relatively simple strategy, *collect information into a single location for all to use as needed*. The complexities of crowdsourcing fall into the following five categories:

Contribution v Consumption: Are enough organizations contributing and are the right organizations consuming CTI? If there aren't enough contributors, the data will lack value. If the right organizations aren't consuming the information, the entire point of crowdsourcing is missed, and the effort is greatly diminished in its ability to be effective in helping protect against cyber-attacks.

Content v Indicators: Everyone in the industry wants more content around their indicators, we refer to this as *contextualized information*, which is how a cybersecurity analyst will quickly observe TTPs and apply logic to associate them within their organization's environment. Indicators are only one half of the equation, without indicators there is no conversation. However, indicators alone (without contextualized information) slows the process of cybersecurity analysts considerably.

Quality v Quantity: Generally speaking, quality has been the desired of every crowdsourcing effort. Too many false negatives cause analysts to move away from the CTI feed and stop sharing. Too much information is a typical problem among crowdsourced CTI because the value of the data is less attractive, but many industry analysts still prefer too much information verses none at all. The quantity of CTI data available is growing exponentially and with it tools are developing to manage massive amounts of data. Therefore, the issue of quantity will at some point no longer be an outright issue, but a distraction from sharing.

You being able to provide to many v Many being able to provide to you: Perhaps the greatest issue with CTI sharing is the actual process of sharing. Being able to share information requires a series of prerequisites which are not common knowledge. The challenges for all are similar in terms of desire to share or technology limitations. LALC explores these in detail and provides thoughts and ideas about the future of CTI sharing.

Benefits of Cyber Threat Intelligence

Threat intelligence benefits abound, and virtually every big company employs threat intelligence to secure itself from hackers and cyberthieves. Correctly applied, threat intelligence provides you the chance to proactively allay your most unrelenting threats, instead of just responding to attacks or a stream of incoming alerts. This occurs by comprehending your cyber risk and raising effectiveness and confidence in your security processes. Here are some key benefits of threat intelligence.

Comprehending Your Cyber Risk

It's not pragmatic to make a company 100 percent safe, so the only rational method to security is one based on risk. For the average SME, protecting against state-sponsored advanced persistent threat groups (APTs) is simply unthinkable. Given the small probability of such an attack, investing massively in its prevention defies logic.

Similarly, since organizations of all sizes across all industries are convinced to obtain malevolent email (phishing) attacks, investing in a fundamental content filtering solution does make sense. Obviously, prioritizing most threats isn't quite easy. There is the likelihood that those responsible for making decisions on security investments will only react to marketing, industry catchwords, and newspaper headlines.

The worst consequence is that these organizations then apportion resources based on fear, rather than knowledge. This is where threat intelligence comes in. A powerful threat intelligence competence can

help you recognize the particular threats your organization, your industry, or your architecture, is faced with.

Performing Efficient Security Operations

Just adding new processes to your security strategy should not center around threat intelligence. The fact of the matter is that a powerful threat intelligence competence should be the core of your security processes. The blend of external intelligence combined with internal data is possibly a massive input for prevailing security procedures. Vulnerability management and incident response are predominantly good candidates, as they both demand a high degree of background and prioritization to be effective.

On a daily basis, most companies experience scores of security events, most of which are innocuous irregularities. Threat intelligence can provide the answer this question and enable you to perform a solid baseline for your organization to clearly identify the alerting security events and discard other unimportant regular anomalies

Other Important Benefits

- Identify leaked credentials
- Prioritize vulnerability remediation
- Monitor for mentions of your brand online
- Uncover emerging threats
- Track hacktivist activity in your industry
- Study threat actor tactics, techniques, and procedures (TTPs)

Why should I care about Cybersecurity?

As a society we depend more and more on technology, it's important to take steps to protect your personal data and your business. Your data holds information about not just yourself, but your family, friends, and coworkers - so good data security practices benefit everyone. You also want to protect your business, a cyber event can impact your operations, reputation, and create risk for employees and customers.

LACL Supports the Public Sector

With over 300 Ransomware attacks on local and state government since 2013, the City has made it a strategic priority to help other cities regionally and nationally. Through the LACL TISP, the City shares its threat intelligence to a growing network of regional and national partners.

Who can take advantage of LACL services?

LACL services can benefit everyone, anyone can sign up for our daily threat report or download the mobile app. Larger business with advanced cybersecurity tools can be integrated into our threat

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

sharing platform, giving them data on the latest threats and sharing suspicious activity with the community.

What		Who	How
Daily Threat Report	Daily email with articles on the latest threats	Everyone C-Suite & Business Leaders	Sign up here https://www.lacyberlab.org/tools-for-la-businesses/
LACL Mobile Application	beta web application that gives tips and a guide for sharing suspicious emails. Sharing bad emails is like a cyber tip line.	Everyone, especially SMBs	Download from Apple app store or Google play store
Threat Intelligence Sharing Platform (TISP)	Automated threat sharing platform for public and private sectors partners	Business with advanced Security tools or teams	Contact us LACL at TISP@lacyberlab.org
Daily IOC Report	Daily email with IOCs	Everyone, security teams with limited automation	Sign up here https://www.lacyberlab.org/tools-for-la-businesses/
Trainings and workshops	Free Security trainings for all	Everyone, primarily analysts, researchers	Check LACL website or follow on Social Media https://www.lacyberlab.org/cyber-events/

Establish a Fully Functional IS-ISAO

Establish a fully functional IS-ISAO that can allow real time or near-real time sharing of cyber threat information between IS-ISAO and CISA.

As part of the pilot project, the LACL established a fully functional IS-ISAO, registered with the International Information Sharing Organization, recognized by DHS and providing CTI to CISA. The efforts to create the IS-ISAO were a lengthy process of identifying CTI use cases, partners, members, defining requirements and operationalizing the information sharing process. LACL developed a request for proposal (RFP) with the City of Los Angeles and solicited the private sector for technical assistance in creating a means by which the LACL could create a CTI sharing community. The process of developing the RFP, selecting a vendor, and executing a contract took 11 months. Work based on the project began in June 2019 with informal agreements in place between LACL, IBM, and The Rosslyn Group (TRG). The original RFP intended to create a platform capable of completing a full cycle of intelligence and dissemination to members. Through the RFP review and interview process the LACL identified an opportunity to connect with SMBs in a unique way which had never been attempted before in the information security industry.

The LACL boldly took a direction to create a mobile application to support SMBs and individuals with business email compromise (BEC), also known as *phishing*, by splitting the RFP and awarding two contracts within the same allotted budget. The uniqueness of the LACL app is that it takes advantage of enterprise cybersecurity information and analysis and provides access to this information vis-a-vie the app response to the user's inbox. To create this capability two things needed to occur: 1) create a CTI platform, 2) create an app capable of connecting to the CTI platform. LACL simultaneously began efforts to establish what would become the LACL TISP and the LACL mobile app. IBM was selected, along with its partner TruSTAR, to provide the CTI platform and the analytics which would serve both LACL partners and members, and the mobile app. The TISP is the source of all LACL threat intelligence. The TRG was selected to create the mobile app which would allow users to submit suspicious emails by forwarding them to the LACL inbox (gophish@lacyberlab.net) from which they would receive an answer about their submission inside their mobile app in-box. Small, Medium Size Businesses (SMB)s have historically been difficult to assist from an information security discipline. They have limited resources, access to information, and capabilities to allow them to make use of existing resources. Often SMBs fall into one of three categories of cybersecurity related risk: 1) outsourced Information Technology (IT) and security offering some protections, 2) internal attempts to secure their business offering little protections, and 3) ignoring security offering no protections. SMBs represent a significant portion of existing businesses within the community. The LACL created the following use cases for assisting SMBs:

SMB Use Case #1) Define the lowest common denominator of cyber-crime/attacks against SBMs

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

SMB Use Case #2) Create a no cost service

SMB Use Case #3) Offer a simple way to assist SMBs with cybersecurity

SMB Use Case #4) Bring SMBs into the information sharing community

From these use cases the LACL established that offering a means to validate phishing attempts would be an imaginative and creative way to engage SMBs and the community. LACL wanted to find ways to bring the SMBs and individuals into the cybersecurity ecosystem. The result was the creation of the LACL mobile app.

The LACL identified existing CTI platforms on the market, despite these existing products, no commercially available product has a mobile version or the ability to integrate with SMBs. CTI platforms are strictly for advanced users and mature security operations. The challenge created by these platforms is that medium business and many SLTT organizations do not have the ability to utilize CTI even if it is provided at no cost. The LACL identified this challenge immediately and began engaging large corporations and large municipalities to become *partners* in CTI sharing which would in turn be leveraged to provide CTI to *members*. Members were defined as those receiving information from the LACL in any form. The LACL established the following use cases for the TISP:

TISP Use Case #1) Establish a cloud-based platform for the exchange of threat intelligence

TISP Use Case #2) Create a manageable platform capable of providing CTI via API or Structured Threat Information Expression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII)

TISP Use Case #3) Retain data for at least 90 days

TISP Use Case #4) Perform automated analysis of threat data within the platform

TISP Use Case #5) Capable of anonymizing sensitive data

TISP Use Case #6) Leverage the MITRE ATT&CK Framework with threat data

TISP Use Case #7) Utilize the Traffic Light Protocol for community sharing

TISP Use Case #8) Connect via API with the LACL mobile app

TISP Use Case #9) Control access by role (RBAC)

These use cases guided the development of the LACL TISP as it worked with IBM and TruSTAR to create these functions within the TruSTAR Station platform. The TISP is a cloud-based application which houses all cyber threat data in enclaves which are provisioned to members. Members are able to access LACL community CTI and interact with the data inside the platform. Members can also use the TISP to create their own cases and manage their cyber threats, they can collaborate with other analysts either in their team or in other organizations within the LACL community and can access CTI reports.

Threat Intelligence Platforms (TIP)

A TIP is a tool which provides a place to collect and analyze threat intelligence. TIPs are used by organizations to gain an advantage over the adversary by detecting the presence of threat actors, blocking and responding to their attacks. Using threat intelligence, businesses and government agencies can identify the threat sources and data that are the most useful and relevant to protecting their own environment, potentially reducing the costs and dependencies associated with commercial paid threat feeds.

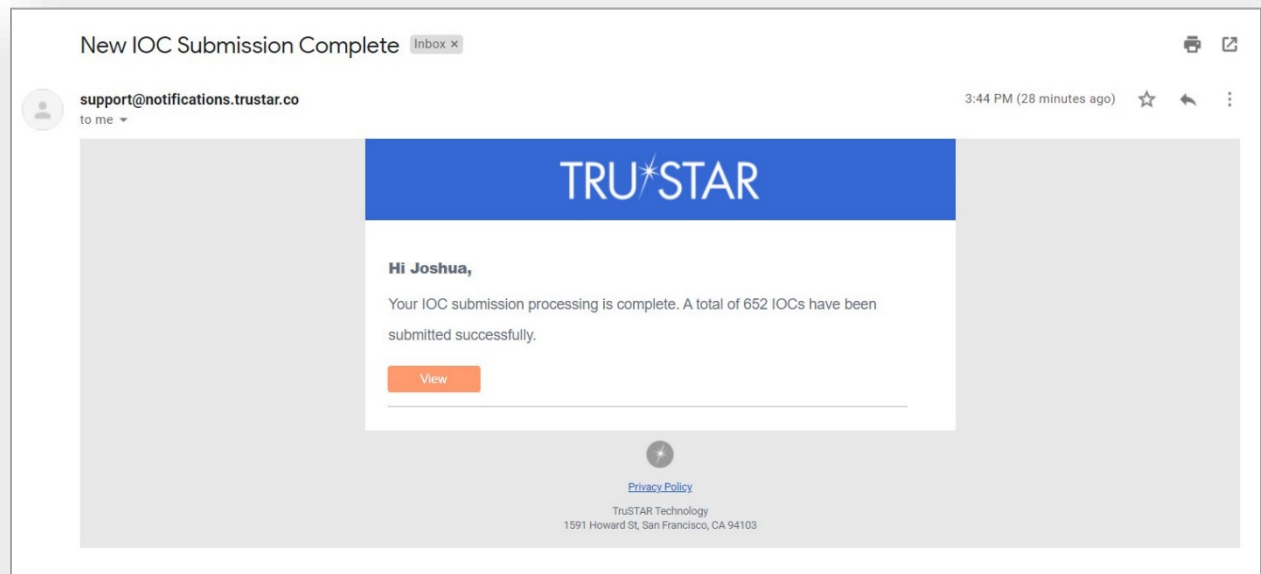
Tactical use cases for threat intelligence include security planning, monitoring and detection, incident response, threat discovery and threat assessment. A TIP also drives smarter practices back into Security, Information and Event Management (SIEM)s, intrusion detection, and other security tools because of the finely curated, relevant, and widely sourced threat intelligence that a TIP produces.

An advantage held by TIPs, is the ability to share threat intelligence with other stakeholders and communities. Adversaries typically coordinate their efforts, across forums and platforms. A TIP provides a common environment for security teams to share threat information among their own trusted circles, interface with security and intelligence experts, and receive guidance on implementing coordinated counter-measures. Full-featured TIPs enable security analysts to simultaneously coordinate these tactical and strategic activities with incident response, security operations, and risk management teams while aggregating data from trusted communities.

Threat Intelligence Platform Capabilities

Threat intelligence platforms are made up of several primary feature areas that allow organizations to implement an intelligence-driven security approach. These stages are supported by automated workflows that streamline the threat detection, management, analysis, and defensive process and track it through to completion:

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



- **Collect** – A TIP collects and aggregates multiple data formats from multiple sources including CSV, STIX, XML, JSON, IODEK, OpenIOC, email and various other feeds. In this way a TIP differs from a SIEM platform. While SIEMs can handle multiple TI feeds, they are less well suited for ad hoc importing or for analyzing unstructured formats that are regularly required for analysis. The effectiveness of the TIP will be heavily influenced by the quality, depth, breadth and timeliness of the sources selected. Most TIPs provide integration to the major commercial and open source intelligence sources.
- **Correlate** – The TIP allows organizations to begin to automatically analyze, correlate, and pivot on data so that actionable intelligence in the who, why and how of a given attack can be gained and blocking measures introduced. Automation of these processing feeds is critical.
- **Enrichment and Contextualization** – To build enriched context around threats, A TIP must be able to automatically augment, or allow threat intelligence analysts to use third party threat analysis applications to augment threat data. This enables the SOC and IR teams to have as much data as possible regarding a certain threat actor, his capabilities, and his infrastructure to properly act on the threat. A TIP will usually enrich the collected data with information such as IP geolocation, ASN networks and various other information from sources such as IP and domain blocklists.
- **Analyze** – The TIP automatically analyzes the content of threat indicators and the relationships between them to enable the production of usable, relevant, and timely threat intelligence from the data collected. This analysis enables the identification of a threat actor's tactics, techniques and procedures (TTPs). In addition, visualization capabilities help depict complex relationships and allow users to pivot to reveal greater detail and subtle relationships. A

proven method for analysis within the TIP framework builds a clear picture of how adversaries operate and inform an overall response more effectively. This process helps teams refine and place data in context to develop an effective action plan. For example, a threat intelligence analyst may perform relationship modeling on a phishing email to determine who sent it, who received the email, the domains it is registered to, IP addresses that resolve to that domain, etc. From here, the analyst can pivot further to reveal other domains that use the same DNS resolver, the internal hosts that try to connect to it, and what other host/domain name requests have been attempted. This ensures a more effective overall response.

- Integrate – Integrations are a key requirement of a TIP. Data from the platform needs to find a way back into the security tools and products used by an organization. Full-featured TIPs enable the flow of information collected and analyzed from feeds, etc. and disseminate and integrate the cleaned data to other network tools including SIEMs, internal ticketing systems, firewalls, intrusion detection systems, and more. Furthermore, APIs allow for the automation of actions without direct user involvement.
- Act – A mature threat intelligence platform deployment also handles response processing. Built-in workflows and processes accelerate collaboration within the security team and wider communities like Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs), so that teams can take control of course of action development, mitigation planning, and execution. This level of community participation can't be achieved without a sophisticated threat intelligence platform. Powerful TIPs enable these communities to create tools and applications that can be used to continue to change the game for security professionals. In this model, analysts and developers freely share applications with one another, choose and modify applications, and accelerate solution development through plug-and-play activities. In addition, threat intelligence can also be acted upon strategically to inform necessary network and security architecture changes and optimize security teams.

Operational Deployments

Threat intelligence platforms can be deployed as a software or appliance (physical or virtual) on-premises or in dedicated or public clouds for enhanced community collaboration.

Types of Threat Intelligence

Cyber security threat intelligence is often broken down into three subcategories:

- Strategic — Broader trends typically meant for a non-technical audience
- Tactical — Outlines of the tactics, techniques, and procedures of threat actors for a more technical audience
- Operational — Technical details about specific attacks and campaigns

Strategic Threat Intelligence

This strategy provides a comprehensive summary of an organization's threat landscape and is intended to inform high-level decisions made by a company's managers and executives. Effective tactical

intelligence should provide understanding into domains like the risks related to certain lines of action, extensive designs in threat actor strategies and targets.

Tactical Threat Intelligence

This type of intelligence plans the strategies, methods, and measures of threat actors. It should help protectors comprehend, in precise terms, how their company might be attacked and the best ways to protect against or alleviate those attacks. It typically includes technical setting and is used by personnel directly involved in the security of a company.

Operational Threat Intelligence

This type of intelligence is knowledge about cyber-attacks, events, or campaigns, giving specific understandings that help incident response teams comprehend the nature, intent, and timing of precise attacks. Since this typically comprises technical information, this kind of intelligence is also referred to as technical threat intelligence.

The Threat Intelligence Lifecycle

The importance of threat intelligence in today's world can hardly be overlooked. The following are the phases of the threat intelligence lifecycle.



1. **Planning & Direction**

This is the phase when goals are set for the threat intelligence program involving comprehension and articulation. Once advanced intelligence needs are found out, a company can frame questions that channel the need for information into separate requirements.

2. **Collection**

It is the method of collecting information to address the most significant intelligence requirements. Information collection can happen naturally through such means as pulling metadata and logs from inner networks and security devices; subscribing to threat data feeds from industry organizations and cybersecurity retailers; holding discussions and targeted interviews with well-informed sources; skimming open source news and blogs; and more.

3. **Processing**

This is the change of gathered information into a setup an organization employs. Nearly all raw data gathered ought to be handled in some way, whether by humans or machines. Various collection systems often need different means of dispensation, while human reports may need to be interrelated and graded, deconflicted, and checked.

“Solutions like SIEMs are a good place to start because they make it relatively easy to structure data with correlation rules that can be set up for a few different use cases, but they can only take in a limited number of data types.”

4. **Analysis**

The next step is to make sense of the processed data. The goal of analysis is to search for potential security issues and notify the relevant teams in a format that fulfills the intelligence requirements outlined in the planning and direction stage. Based on the situations, the decisions might involve whether to probe a possible threat, what actions to take directly to block an attack, how to reinforce security controls, or how much investment in additional security resources is vindicated.

5. **Dissemination**

Dissemination involves having the complete intelligence productivity to the places it ought to go. A majority of cybersecurity organizations have at least six teams that can take advantage of threat intelligence. This type of intelligence entails you to ask what threat intelligence the audiences need, and how external information can support their activities.

6. **Feedback**

It is the final phase of the lifecycle that is making it closely related to the initial planning and direction phase. After receiving the finished intelligence product, whoever makes the initial request reviews it and determines whether their questions were answered. You need steady feedback to ensure you

appreciate the requirements of each group, and to make changes as their requirements and priorities vary.

Cyber-threat Intelligence Tools

Commercial Tools

It's a very important threat intelligence platform. The commercial tools generally happen to be very expensive. It is often hard to persuade upper management of the need of some of these types of tools, particularly with their annual upkeep fees. The benefit of these tools is that a lot of them accelerate the penetration test and SOC operations. Another advantage of using commercial tools is that they are highly automated and save a lot of time, but this is also considered a drawback because the user cannot learn how to achieve the same procedure independently.

- [FireEye iSIGHT Threat Intelligence](#)
- [IBM X-Force Exchange](#)

Open Source Tools

This refers to a program or tool that carries out a very particular task, in which the source code is openly published for use and/or alteration from its unique design, absolutely free. Open-source intelligence tools generally gather data on Open-Source Intelligence (OSINT), which is one of the most popular feeding processes and techniques.

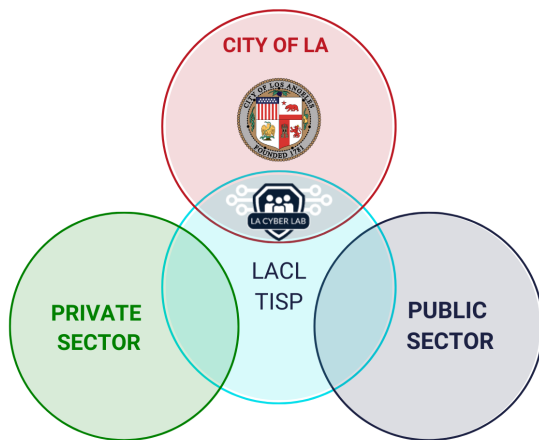
- [MISP – Malware Information Sharing Platform](#)
- [OSINT Framework](#)

Community Platforms

Community Platforms manage the procedure of producing and upholding a space for prolific debate among community members who can share their opinions, ideas, and worries. There are various types of community platforms that debate, discuss, and describe the latest and emerging threat actors and vectors that could help professionals to use this information as feed and get prepared for the underground ongoing and emerging threats.

LACL Threat Intelligence Sharing Platform (TISP)

Upon its launch, the LACL joined with the City to publish a daily threat report, documenting the “indicators of compromise” identified by the City each day, in hopes that the data would help businesses protect their systems from common attackers. LACL partnered with IBM and TruSTAR to develop the LACL Threat Intelligence Sharing Platform (TISP). The TISP allows for real-time automated threat indicator sharing between the private and public sector. Features of the TISP include:



Automated Threat Sharing: Using their existing security tools, partners can connect to the TISP to exchange threat data with one another, machine-to-machine, in real time. It enables members to leverage the insights and analysis developed by DHS, the City of LA, and other partners to protect their own systems.

- Connects LACL Partners, a group consisting of nearly 40 organizations, sharing IOCs for greater community good and consumption.
- Accessible to LACL Members at no cost.

Threat Intelligence Platform: The TISP gives analysts and Threat Intelligence interface to pull in additional threat data sources, see trends, and perform research. The Threat Intelligence Platform can be used by organizations lacking the infrastructure for automated sharing.

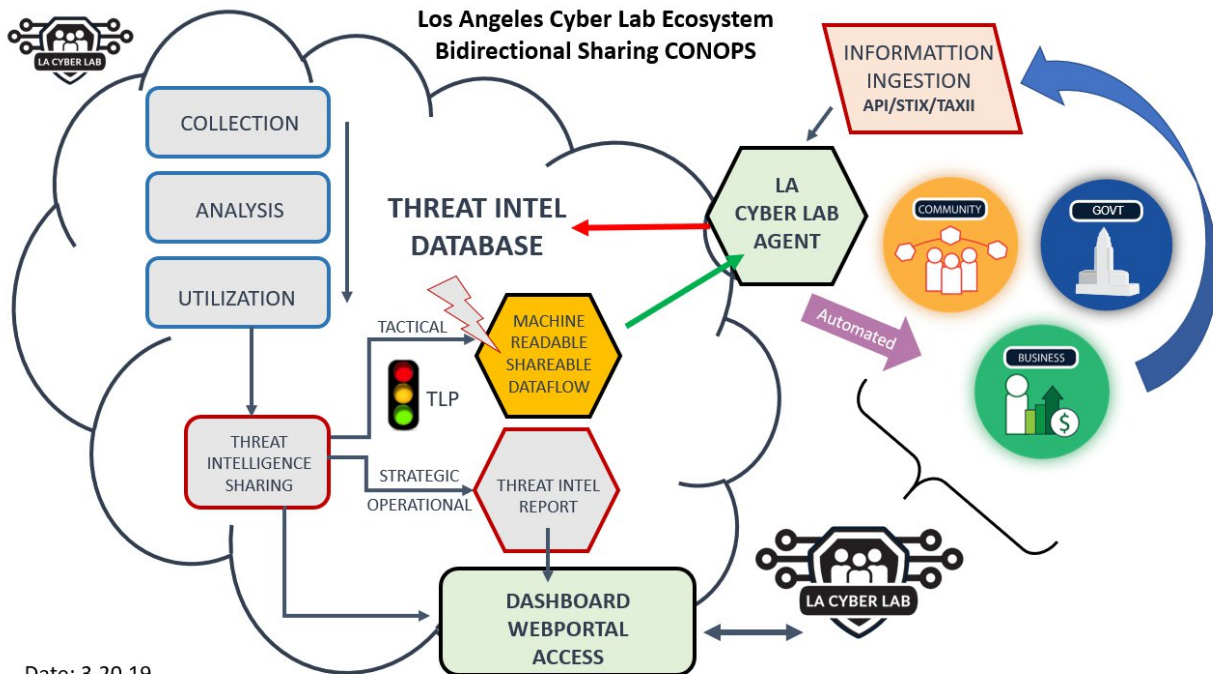
- Threat Reports for Emerging Malware
- Platform for Analysts to Interact with and Research Threats
- Trending data for threats across the LA region

Security Tool Integration: The TISP includes pre-built applications that integrate with existing security tools, such as Security Information and Event Management systems.

LACL Mobile Application: providing phishing analysis which connects SMB and individual citizens to business email compromise information.

- Trending phishing threats across the LA region
- Analysis of suspicious emails for evidence of malware or malicious links
- Individual access to threat intelligence

TISP Concept of Operations: utilizing a cloud-based SAAS TIP to ingest CTI from public, private, and community members, the TISP automatically correlates information with existing CTI via IBM X-Force Exchange IRIS analytics and produces reports which can be exported in a variety of formats.



Date: 3.20.19

Sharing Threat Information

The concept of sharing cyber threat information immediately begs the questions of what kind of information to share and how to share it. This policy guidance provides answers to these and related issues, such as what are the typical sources of threat information that an organization may wish to share; deciding on what information to share and when to share it; how such information might be categorized according to relevant models and frameworks; and how to protect privacy when sharing information. The below information provides guidance on how to address these questions and issues within the LACL ISAO.

Sources of Threat Information

The term “threat information” refers to any information related to a cyber threat that may help an organization identify an attacker’s activities or defend against a cyber threat. Threat information often refers to specific indicators (also called Indicators of Compromise (IOC)) such as IP addresses or phishing emails and may also include a broad range of cyber threat-related information, such as attacker’s behavior or “tactics, techniques, and procedures” (TTPs); security alerts such as advisories or bulletins; vulnerability notifications; or threat intelligence reports.

LACL ISAO Partners/Members are likely to possess a variety of threat information that can be used to support the information sharing community. Such data/information may originate from within an organization’s security tools as well as reside in suspicious emails sent to the Partner organization or its members. Typical security tools that contain threat information include firewalls, intrusion detection/prevention tools (IDS/IPS), anti-virus products, operating system artifacts and logs, browser

history and caches, Security Information and Event Management (SIEM) tools, email systems, case management systems, and other system artifacts.¹⁰

Systems and tools that are already in place and designed to gather threat information to assist decision-making regarding cyber threats—such as SIEMs—are likely to be a good starting point for automatically sharing information such as IOCs to other Partners within the LACL ISAO. Threat information derived from incident response engagements conducted in response to potential cyber threats, such as TTPs and IOCs, is also likely to be useful to other Partners within the LACL ISAO. Finally, inbound emails that suggest an organization is being targeted for attack are likely to contain threat information of value.

There are several types of organizations which represent the community of the LACL. Large corporations and public entities are the ideal candidates for Partners to the LACL. These organizations are self-sustaining, have mature information security teams and capabilities, and resources to contribute to the LACL. Due to their size and maturity, they have the potential to offer the LACL higher quality information (IOCs) and greater volume. Of the public sector entities within the region, roughly 20, are deemed mature enough to be considered Partners. Medium size businesses and public entities vary greatly in their capabilities and resources. They often have gaps within their information security structures (e.g. intermittent funding, manpower shortages, skills shortages, etc.) These organizations represent the best category of members for the LACL because they are somewhat mature but could still benefit greatly from the services offered by the LACL. Small businesses and individuals are typically neither a partner or member of the LACL. Their limited resources and skills make it impractical to provide IOCs or other technical information to because they have no means by which to employ the data. Essentially, they can receive IOCs but cannot put them into use. Instead, this particular group represents a category of people who can engage the LACL via mobile platforms and who can contribute to the LACL by providing random but unique data in the form of business email compromise threat data.

Choosing What To Share and When To Share It

Organizations are typically inundated with potential threat information derived from their internal security operations, many of which are likely to be classified as false positives. When deciding whether to share threat information, organizations should first apply an internal vetting process to determine that the indicator may pose harm to an organization and therefore may also threaten other Partners with the ISAO. Once an organization has decided that there is a reasonable case to be made that the threat information e.g. an IOC may be malicious, the organization should consider sharing that information within the LACL ISAO.¹¹

¹⁰ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

¹¹ https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

WHAT TO SHARE

CYBER THREAT SHARING MATRIX				
SOURCE	IDENTIFY	IOC	CORRELATE	SHARE
Networks	Firewall logs	IPs / Domains	External Threat Intel	TISP
	Web Content Filter			
	Irregular Activity			
	hashes/Fingerprints from SSL inspection			
Emails	User reporting phishing	Senders/ URLS		Email/Reports/T ISP
	Email logs			
Endpoint	Antivirus triggers	Hashes/ SHA/ MD5		TISP
	Endpoint detection			
	Window Event Logs			
	Application Whitelist/Blacklist			
Analyst	Analyst investigation/findings	TTPs	Reports/Calls	

After having made a decision that threat information may be of value to other Partners within the ISAO it should be shared as quickly as possible. This is especially important in the case of IOCs such as IP addresses, domain names, or file hashes which may have a very short lifespan. Attacker behavior or TTPs should also be shared quickly as such information could be particularly valuable to Partners' Incident Response teams who might be investigating a similar incident.

The TruSTAR platform currently supports processing of the following IOC Types:

- IPV4
- IPV6
- CIDR BLOCK
- URL (Domains are currently categorized as URL's)
- MD5
- SHA1
- SHA256
- CVE (based on NIST's CVE Standard)
- BITCOIN ADDRESSES
- SOFTWARE (file names are currently treated as Software)
- EMAIL ADDRESS
- REGISTRY KEY

- MALWARE
- THREAT ACTOR
- PHONE NUMBERS

Analysis of Data

XFE threat intelligence analysis and risk scoring methodology for the LACL TISP and mobile application are outlined within this document.

XFE Threat Intelligence Sources

The following are the data sources utilized for the LACL TISP:

- Botnet Traps
- Web Crawling
- Email/Phishing Honeypots
- Open Relay Proxies
- X-Force Vulnerability Database
- WhoIs
- ASN
- Cert Stream
- Regional Internet Registries
- Tor Nodes
- DNS Analytics from PCH/Quad9
- IBM Customer Feedback about URLs, IPs, DGA matches, Squatting matches

Concerning the distribution proprietary threat intel versus external 3rd party feeds we have:

- 89% is XFE proprietary threat intel
- 11% is coming from external feeds

Risk Score Calculation

XFE's analytics engine manages the life-span of an indicator of compromise (IOC) dynamically per source and per category.

Risk Scoring Factors:

- How often have we seen an IOC (e.g. Phishing website observed in initial compromise)
- In how many sources have we seen an IOC (e.g. does a Malware Downloader occur in parallel on our Email Honeypots and on our OpenRelays)
- Is the IOC reoccurring from time to time
- When did we see the IOC the last time
- Is the IOC after a rescanning/recrawling clean now? (e.g. after the owner has fixed the vulnerability / removed an exploit)

XFE normalizes the risk scoring factors. XFE recommends taking steps to defend, block or filter when a risk score is ≥ 5.0 .

XFE uses dynamic risk scoring per IOC Category. For example, the lifespan of a phishing URL differs from a Botnet C2 Server.

XFE maintains an IP Reputation database. For example, a spearphishing email's originating source IP is recorded in the IP Reputation database with a risk score ≥ 5 . If XFE no longer sees spearphishing from this IP, the risk score lessens stepwise. Within a few days it will be below 5 (5 is the recommended threshold for which an action should be taken like a QRadar Offense being created).

For example, in other categories, an IP in our botnet traps or 3rd party list receives a risk score ≥ 5 . XFE lowers the risk score and within in few days it will be below 5 if the IP is not observed.

XFE uses customer feedback to permanently adjust and improve our algorithms to ensure coverage and a low false positive rate.

IBM Sourced Content Contributing To The Risk Score

Data processed per day

- 13M crawled and analyzed web pages and images
- 17M spams received via our spam honeypots

Data processed ever

- 40B analyzed web pages and images
- 3B known web hosts
- 9B unique email bodies
- 4.6M malware samples
- 18k identified Bad Actors
- 800 TB of Threat Intelligence Data in the X-Force Content Intelligence Data Center
- Updates for our consumers (such as XFE, QRadar, XGS, Lotus Protector for Mail Security, update frequency: 3-5 minutes)
- 230k new or updated URL categorizations per day
- 460k new or updated IP categorizations per day
- 1.2M new or updates spam hashes per day

Understanding The Risk Score

XFE aligned the risk score range with the Common Vulnerability Scoring System (CVSS), see <https://www.first.org/cvss/specification-document#5-Qualitative-Severity-Rating-Scale>.

XFE uses colors to express the rating:

Score	Rating	Color
1 - 3	Low	Green
4 - 6	Medium	Yellow
7 - 10	High*	Red

*Unlike CVSS, XFE does not distinguish between High and Critical

Traffic Light Protocol

Los Angeles Cyber Lab Partners/Members are expected to adhere to the Traffic Light Protocol (TLP) when sharing threat intelligence to ensure that sensitive information is distributed only to those who are authorized to receive it.

The TLP provides a mechanism for sharing threat intelligence that is widely accepted among cybersecurity threat researchers, vendors, ISACs and ISAOs. The protocol provides instructions for handling information that are designed to be easy and intuitive to understand. It does not apply to licensing, encryption, or other handling rules.

LACL ISAO Partners should label threat intelligence submitted to the TruSTAR platform or otherwise shared within the LACL ISAO using the instructions and appropriate TLP color codes provided below. Partners/Members shall also respect the TLP designations on information submitted to the ISAO with respect to sharing this information with other entities. If the Partner/Member desires to share the information beyond what is indicated in the TLP designation, they must receive permission from the originator.





TLP use based on sharing mechanism

- TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color should be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.¹²
- TLP-designated documents should indicate the TLP color of the information in the header and footer of each page. To avoid confusion with existing control marking schemes, it is advisable to right-justify TLP designations. The TLP color should appear in capital letters and in 12-point type or greater.
- Threat information submitted through an automated tool using an acceptable format and standard e.g. the Structured Threat Information Expression (STIX), should apply the appropriate TLP marking within the schema.

It is possible that information submitted to the TruSTAR platform as part of the LACL ISAO will not bear a TLP marking. In these cases, Partners/Members should treat such information as TLP:AMBER and should only share this information with members of their own organization or with clients or customers who need to know the information to protect themselves or prevent further harm.

¹² <https://www.us-cert.gov/tlp>

Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

Source: <https://www.us-cert.gov/tp>

Within TruSTAR, there are several mechanisms through which a Partner/Member can annotate the TLP level of the information being shared.

- TLP markings can be added to the Report Title when uploading a report and within the body of the Report itself.
- Reports and Indicators of Compromise (IOCs) can be tagged with the appropriate TLP level.
- Email submissions can be marked with the TLP level directly in the email subject line or via tags.

For more information on how to submit Reports, IOCs, and Emails to TruSTAR see the section below: *How to Share and Export Information with the TruSTAR Platform.*

Generating and Sharing Analytic Reports

LACL ISAO Partners may also consider sharing threat intelligence reports with the community. Such reports are typically unstructured prose or text as opposed to machine-readable data and go beyond atomic indicators to convey “information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making.” (NIST SP 800-150). Such threat reports may also employ data visualization techniques to convey the results of analyzing large data sets.

There are several different types of threat intelligence reports that Partners may wish to generate and share. Trend analysis and emerging threats reports aggregate and analyze indicators (e.g. hashes, IP addresses, domain names) to identify trends over time that may point to existing or emerging threats to an organization’s security. Other information derived from open source intelligence (OSINT) or the dark web may also be added to provide historical context or point to planning or intentions. These reports may also include suggestions or methods to neutralize these threats.

Other reports analyze threat information related to a specific threat actor or campaign, such as ransomware or phishing campaigns, together with the actor’s indicators, TTPs, and goals or motivations, including the capabilities of the malware used during attacks. Rich with technical details, these reports will help other Partners to understand the threat actor’s capabilities and how it affects their threat environment and security posture.

These reports may leverage analytic techniques, such as “data storytelling” and “analytic stories,” to enhance their effectiveness. These methods typically involve addressing a new development that is being analyzed (e.g., a series of phishing attacks against a particular industry); a key question that is being answered or “what’s the so what?” of the new development (e.g., why the campaign is important to an industry)¹³; the exploration of data over time through a narrative that adds context and explains events in ways that are easy to follow; and leveraging a series of data visualizations that help to convey this narrative. In addition, a key component of a threat intelligence analytic story is not only the narrative regarding the cyber threat, but also information and analysis that can help operations personnel and decision makers, such as how the threat can be detected, mitigated, or defeated. Finally, an analytic threat intelligence report should be transparent about the level of confidence in any analytic assessments as well as any specific analytic method that is being used.

Categorizing Indicators & MITRE ATT&CK

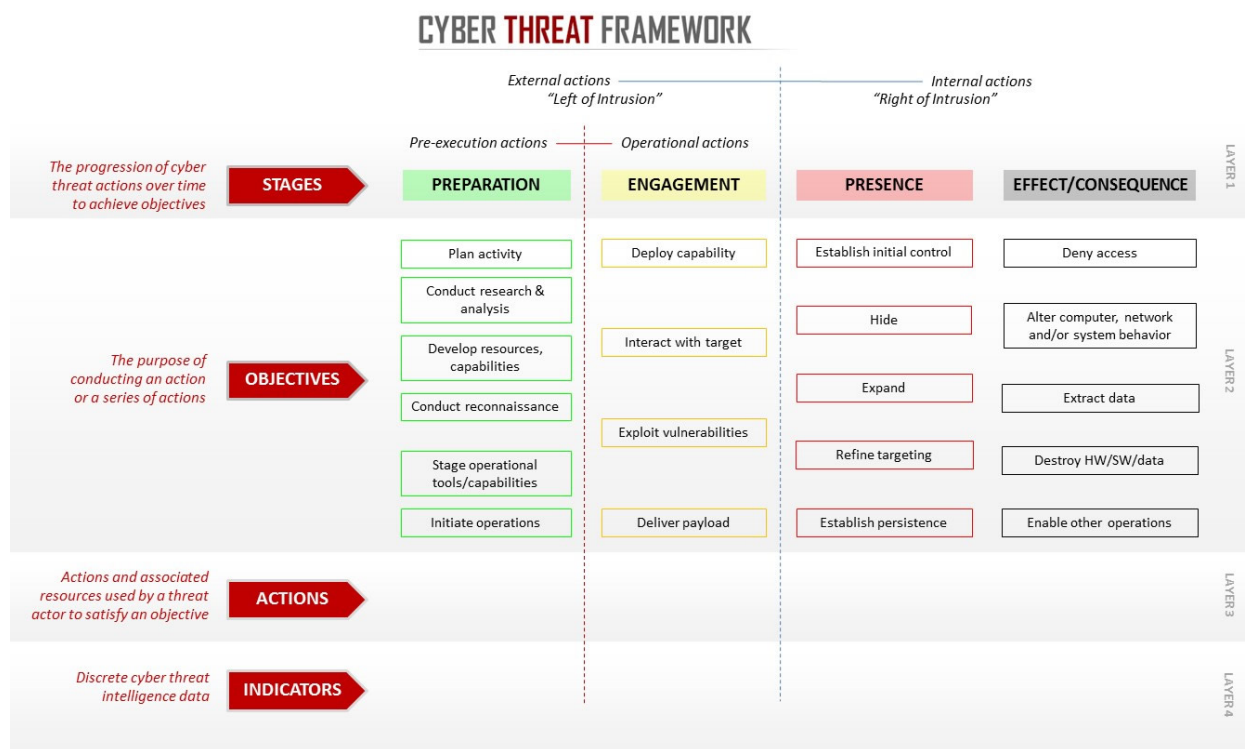
Multiple frameworks have emerged in recent years to assist cybersecurity analysts with categorizing malicious behavior using common lexicon and concepts. These frameworks are also important to information sharing through enabling the use of common terms and concepts. Two noteworthy examples are the Office of the Director of National Intelligence (ODNI) Cyber Threat Framework and

¹³ <https://www.isao.org/storage/2018/06/ISAO-700-1-Introduction-to-Analysis-v1.0.pdf>

the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework. ISAO Partners/Members are encouraged to use the concepts and terms present in these frameworks where appropriate when describing cyber threat actor behavior to facilitate information sharing. In addition, the TruSTAR platform by October 1st 2019 will enable Partners/Members to tag indicators with the related ATT&CK tactic and technique.

ODNI Cyber Threat Framework

The ODNI Cyber Threat Framework “captures the adversary life cycle from PREPARATION of capabilities and targeting to initial ENGAGEMENT with the targets or temporary nonintrusive disruptions by the adversary, to establishing and expanding the PRESENCE on target networks, to the creation of EFFECTS and CONSEQUENCES from theft, manipulation, or disruption.”



The ODNI offers this high-level model as a tool to describe cyber activity in a consistent and repeatable fashion and as a common reference for other models. More information about the ODNI Cyber Threat Framework can be found here: <https://www.dni.gov/index.php/cyber-threat-framework>

MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a knowledge base of adversarial techniques that can be used against particular platforms e.g. Windows or Linux. The focus of the ATT&CK framework goes beyond

describing an adversary's life cycle and focuses on the tactics, techniques and procedures that adversaries use during their attacks. The emphasis is on how the adversary interacts with the system during their campaign as opposed to the specific tools or malware they deploy. More information on the ATT&CK Framework can be found here: <https://attack.mitre.org/>

The ATT&CK Framework begins with 12 "Tactics" that cover higher-level adversary activities performed during a campaign such as Initial Access, Persistence, Lateral Movement, and Execution. Tactics may also be thought of as goals that an adversary is pursuing e.g. the Tactic Lateral Movement represents the adversaries' goal i.e. to move across the network. These 12 Tactics are enumerated by different "Techniques" to achieve the Tactic. Techniques include the means by which an adversary achieves the Tactic e.g. the Tactic "Persistence" includes Techniques such as Scheduled Tasks, Registry Run Keys / Startup Folder, and New Service.

One noteworthy benefit of the MITRE ATT&CK Framework is the ability to compare different adversary threat groups and their campaigns through their use of different Techniques. An increased understanding of these Techniques and how different threat actors have used them successfully against different organizations can provide valuable information on what types of defenses work best.

To facilitate this kind of analysis, the TruSTAR platform will integrate with the MITRE ATT&CK Framework and Partners and Members may annotate submissions with the corresponding ATT&CK Framework Tactic/Technique and to also search for other indicators based on their ATT&CK Tactic or Technique.

Protecting Privacy

Attention to privacy considerations is a critical part of the information sharing process and is fundamental to the success of the ISAO in which information sharing is voluntary and based on trust. Moreover, the improper disclosure of such information could cause harm to individuals, companies and others and be in violation of applicable laws and regulations. As a result, Partners/Members should consider the privacy implications of information they are considering sharing, such as personal information about a specific individual; whether or not that information is directly related to a cybersecurity threat; and if not, whether that information has been removed. This section is intended to provide guidance to ISAO Partners/Members on how to adequately protect privacy while also fulfilling the goals of the ISAO to enable the sharing of relevant and timely cybersecurity threat information.

The Cybersecurity Information Sharing Act of 2015 permits organizations to share personal information as part of a cyber threat indicator only in circumstances where it is directly related to the threat at the time of sharing. This may include information necessary to deter or protect against the threat such as IOCs; threat actor TTPs; and malicious files.

- For a phishing email, information relevant to a threat could include personal information about the sender of the email ("From"/"Sender" address), a malicious URL in the e-mail,

malware files attached to the e-mail, the content of the e-mail, and additional information related to the malicious email or potential cybersecurity threat actor, such as Subject Line, Message ID, and X-Mailer. However, this would typically not include the phishing target email address and names (i.e. the “To” address) because they are considered personal information not directly related to the threat.

The following guidance, drawn from ISAO Standards Organization guidelines¹⁴, is provided to help Partners and Members address privacy concerns when sharing information with the LACL ISAO:

1. Before sharing cybersecurity information, remove or redact information that is known at the time of sharing to be information about a specific individual or that identifies a specific individual, unless it relates directly to the detection, prevention, or mitigation of a cybersecurity threat.
2. Upon receiving information known at the time of sharing to identify a specific individual or is of a specific individual that is not information directly related to a cybersecurity threat, securely dispose of or anonymize such information as soon as practicable.
3. Upon receiving information not related to cybersecurity, promptly notify the submitter or originator.
4. Update cybersecurity information repositories upon receiving a notice of information erroneously identified as cybersecurity information. Securely return, dispose of, or anonymize any such information.
5. Where appropriate, use tools such as the Traffic Light Protocol or similar approaches to designate the sensitivity of cybersecurity information and govern its sharing within and among organizations.
6. Protect cybersecurity information from unauthorized access or acquisition.
7. Regularly review cybersecurity information to ensure it remains useful for cybersecurity purposes.
8. Regularly review the receipt, retention, dissemination, and use of cybersecurity information for consistency with these practices and associated organizational policies.
9. Consistent with organizational privacy policies, provide appropriate transparency about cybersecurity information sharing practices and potential partners, including notice that information that identifies a specific individual may be shared outside the organization for

¹⁴ https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

“cybersecurity purposes,” including with the government, which may result in the government’s use of the information for purposes authorized under ISAO-SP-4000.¹⁵

Redacting Information from TruSTAR Submissions

TruSTAR provides the ability to redact sensitive information such as employee names, identification numbers, birth dates, etc. from Reports at the time they are manually uploaded into the system. This feature is an automatic part of the process when uploading Reports to TruSTAR.

Partners/Members can also upload a pre-selected list of terms that they wish to be redacted automatically from all submissions. This feature can be found in the Settings on the TruSTAR user interface, and then selecting Redaction.¹⁶

For more information on redacting information from TruSTAR submissions, please see:

<https://support.trustar.co/article/f45yzob9b9-report-submission>

How to Share and Export Information with the TruSTAR Platform

There are a number of options for sharing information such as Reports and IOCs with the TruSTAR platform, including using the User Interface, by Email, and by API.

HOW TO SHARE

THREAT SHARING FRAMEWORK		
1. IDENTIFY	2. CORRELATE	3. SHARE
Identify log sources and potential IOC's from the logs	Correlate potential IOCs with external threat intel	Share IOC with partners

User Interface

Partners/Members can submit reports through the User Interface (UI), by email, and by the TruSTAR API. Once submitted, the indicators within the report are automatically correlated and visible in the TruSTAR UI:

¹⁵ <https://www.isao.org/storage/2017/07/ISAO-SP-4000-Protecting-Consumer-Privacy-in-Cybersecurity-Information-Sharing-v1-0.pdf>

¹⁶ https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

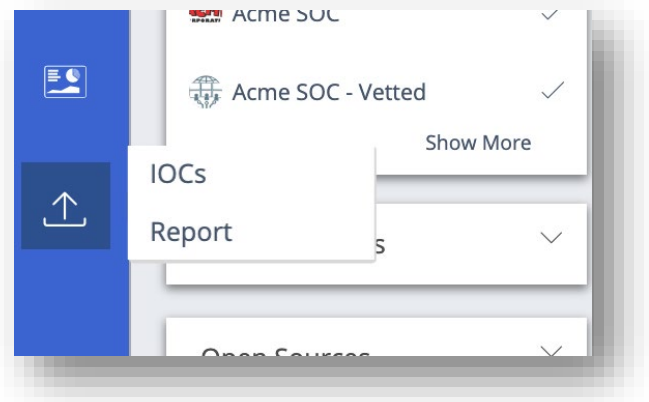
User Interface (Reports):

Through the UI, click the “Import” icon seen in the left side of the bar and select “Report” from the drop-down. (See the box to the right.)

From here, the Partner/Member can upload or drag/drop a file into the Upload File field. File types that can be uploaded include: JSON, DOC, DOCX, XML, XLS, XLSX, EML, MSG, CSV, PDF, STIX, TAXII and TXT files.

For additional and updated information on submitting reports through the UI, please see:

<https://support.trustar.co/article/f45yzob9b9-report-submission>



User Interface (IOCs):

After clicking on the Import icon, select “IOCs” from the dropdown menu. Partners/Members can either paste in a list of indicators or upload a file (DOC, PDF, CSV, XLS, TXT, JSON, XML). Partners/Members will be guided through a series of steps in the UI to submit their IOCs.

For additional and updated information on submitting IOCs through the UI, please see:

<https://support.trustar.co/article/redq0g4hq3-ioc-management>

Email Submissions

TruSTAR allows Partners/Members to submit incident and alert information directly to their enclaves by email. For example, a Partner who belongs to an email listserv for exchanging IOCs, but there is no straightforward way to extract valuable context may choose to share with the LACL ISAO via email submission. Another example, a Partner may setup automated SIEM alerts or case management system and automatically submit the details of an alert or case as a TruStar report.

- Submit phishing emails as an attachment to phishing@lacyberlab.org
- Summit IOC's, analyst investigation/findings, and other information at analyst@lacyberlab.org

Configuration

- Destination Enclave: LACL TISP
- Send to Email Address: lacl_tisp_lro3bflhmcbco@enclave.trustar.co
- LACL TISP Enclave processes emails every minute.
- As with all other submissions, TruSTAR automatically extracts and correlates IOCs.

Email Submission Guidance

- Partners need to send emails from the email account provided during configuration.
- Partners need to use the subject line prefix(s) provided during configuration.

- Partners should verify the subject line prefix is in square brackets [].
- If multiple subject line prefixes exist, then each one has to be in its own square [] bracket.
- Submitted Emails become TruSTAR reports. TruSTAR uses the Subject line Prefix as the Report's Title.
- Partners may include descriptive information about the email submission using tags.
 - Use the subject line. Insert tags as a comma separated list within { } brackets.
 - In the first line of the email body. Insert tags as a comma separated list within { } brackets.
- TruStar uses the email body as report content and automatically extracts IOCs found in the email body.

Email Attachments

TruSTAR automatically connects the email's attachment (PDF, Word, Text file, CSV, Excel or JSON) to the report body. If the attachments have any IOCs, then TruSTAR automatically extracts the indicators. During the email ingestion process, the original format of the attachment may not remain.

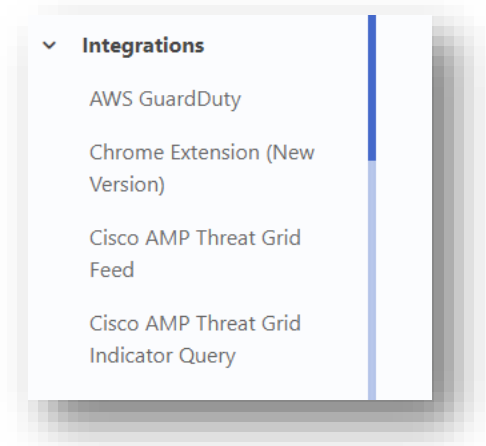
For additional and updated information on email submissions, please see:

<https://support.trustar.co/article/xr5632rgzp-email-ingest>

Native Integrations

TruSTAR integrates with a number of security tools including SIEMS, Case Management systems, and Orchestration tools that enable LACL ISAO Partners/Members to upload information into TruSTAR. For a full list of available integrations, please see: <https://www.trustar.co/integrations>

More information on how to set up these integrations can be found here <https://www.trustar.co/integrations> and on the TruSTAR support page: <https://support.trustar.co/> (select "Integrations" on the menu on the left).



STIX/TAXII enabled Tools

Partners may choose to use existing tools enabled with TAXII. A TAXII Server is software that offers automated exchange services by listening for connections from TAXII Clients looking to ingest data from the available services. Integration information for Partner Tools enabled with TAXII can be found [here](#).

Partners may use the TAXII Message Module Structure to send threat information to TruSTAR. In the TAXII message modules (`libtaxii.messages_10` and `libtaxii.messages_11`), there is a class corresponding to each type of TAXII message.

For example, there is a `DiscoveryRequest` class for the Discovery Request message:

```
import libtaxii.messages_11 as tm11
discovery_request = tm11.DiscoveryRequest( ... )
```

For types used across multiple messages (e.g., a Content Block can exist in both Poll Response and Inbox Message), the corresponding class (`ContentBlock`) is defined at the module level.

```
content_block = tm11.ContentBlock( ... )
```

Other types used exclusively within a TAXII message type defined as nested classes on the corresponding message class and now defined at the top level of the module. For example, a Service Instance is used in a Discovery Response message, so the class standing for a Service Instance, now just `ServiceInstance`, was previously `DiscoveryResponse.ServiceInstance`. The latter name works for backward compatibility but deprecated and may be removed in the future.

```
service_instance = tm11.ServiceInstance( ... )
service_instance = tm11.DiscoveryRequest.ServiceInstance( ... )
```

See the TAXII [API Documentation](#) for proper constructor arguments for each type above.

API & Python SDK

The TruSTAR REST API allows organizations to easily synchronize the incident report information available in the TruSTAR platform to the monitoring tools and analysis workflows within the organization's infrastructure. TruSTAR suggests using the Python SDK to develop specific integrations for workflow automation. All API access is over HTTPS, and all data is transmitted securely in JSON format.

Submit Report [POST /1.3/reports]

1. Submit a new incident report and receive the ID assigned in TruSTAR's system.
2. The ID can be used to find the report through Station, or issue subsequent calls on the API.
3. Note that that a report cannot be tagged during submission. Tags can only be applied afterwards, through a separate call.
4. If a report contains more than 500 indicators, it will be rejected with a `413` (payload too large) error code.

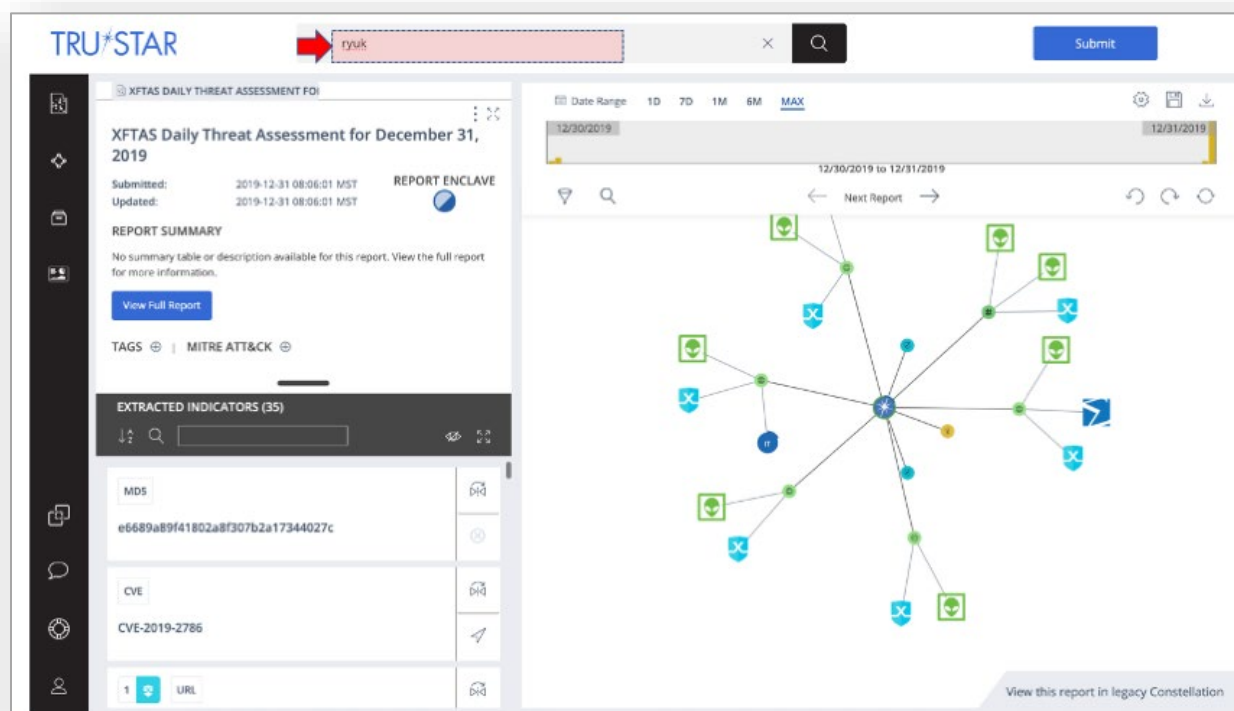
More information about the TruSTAR API and Python SDK can be found here <https://support.trustar.co/article/9u4paxdtdj-api> and here <https://docs.trustar.co/api/index.html>.

Exporting Data

Partners/Members can export data from the TruSTAR platform from the UI or the API. From the UI, there are two options to export or download information. More information on these options can be found here: <https://support.trustar.co/article/d5dct2lxf8-extract-data>

The first option allows the user to export indicators exposed in the graph view in CSV format by selecting the download button on the upper right of the graph.

The example below reflects a query for Ryuk malware information. The report in the example lists 35 IOCs which the user can download to a CSV file by clicking the download icon at the top right of the screen.



The screenshot displays the TruSTAR interface. At the top, a search bar contains the text "Ryuk" and a "Submit" button. The main content area is divided into two panels. The left panel shows the "XFTAS Daily Threat Assessment for December 31, 2019" report, including submission and update timestamps, a "REPORT ENCLAVE" button, and a "View Full Report" button. Below this, there are tags for "MITRE ATT&CK" and a section titled "EXTRACTED INDICATORS (35)". The right panel features a network graph with nodes and connecting lines, and a date range selector set to "12/30/2019 to 12/31/2019". A "Next Report" button is visible below the date range. The graph contains several nodes, some with green download icons and others with blue 'X' icons. A "View this report in legacy Constellation" link is located at the bottom right of the graph area.

The second option allows the user to export a file containing report indicators and all data sources from the graph including intel reports, correlated reports, and community reports.



Data Format and Transport Standards

TruSTAR supports a wide variety of data format and transport standards for uploading and retrieving information to and from the platform.

Report Submission: The following file types can be uploaded via the User Interface (Station): JSON, DOC, DOCX, XML, XLS, XLSX, EML, MSG, CSV, PDF, STIX, TAXII and TEXT files.

IOC Submission: The following file types are supported when submitting a file containing a list of IOCs: DOC, PDF, CSV, XLS, TXT, JSON, XML.

Email Submission: The following file types can be processed when submitted as an attachment to an email: PDF, DOC, TXT, CSV, XLS or JSON.

API: All API access is over HTTPS, and all data is transmitted securely in JSON format.

Export: TruSTAR's export options support the following formats: CSV, STIX, JSON, and FireEye TAP.

Minimum Technical Requirements

The minimum technical requirements for Partners/Members to share and receive threat intelligence data are a modern browser and an Internet connection. These are the only requirements needed to access the TruSTAR platform and manually upload and retrieve threat information.

Partners/Members with existing security tools such as SIEMs, Case Management systems, Orchestration tools, or a TAXII client would be able to automatically share and integrate threat information with their existing workflows.

Partners/Members able to implement the TruSTAR API and Python SDK (a Python package that can be used to easily interact with the TruSTAR Rest API from within any Python program) would be able to further integrate TruSTAR threat information with the monitoring tools and analysis workflows used in their infrastructure.

Integrating with the TruSTAR Platform

The TruSTAR platform is able to integrate with a variety of security tools and platforms, including SIEMs, Case Management systems, and Orchestration tools. More information about these integrations can be found here: <https://www.trustar.co/integrations>

The TruSTAR support page <https://support.trustar.co/> provides step by step instructions on how to integrate these tools with the TruSTAR platform. Below we provide an overview of the most popular integrations with TruSTAR, including QRadar, Splunk, and TAXII:

IBM QRadar:

The TruSTAR - QRadar App allows Partners/Members to integrate context from TruSTAR's IOCs and incidents within their QRadar workflow. This integration requires QRadar V7.2.8 and above. Several features of this integration include:

- Submit QRadar offenses and events to your TruSTAR enclave as reports. This can be performed as a manual or automated action.
- Search TruSTAR for all indicators correlated to indicators of interest in QRadar.
- Populate QRadar reference lists with indicators from TruSTAR.
- Age TruSTAR indicators in the QRadar reference list to keep it relevant and actionable.

For more information on setting up the QRadar-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that app, please see: <https://www.trustar.co/integrations/ibm-gradar-siem-integration-partner> and <https://support.trustar.co/article/oUXRwHSmim-gradar>

Splunk

The TruSTAR Splunk app allows Partners/Members to integrate TruSTAR's IOCs and incidents within their Splunk analysis workflow. Several features of this integration include:

- Dashboard displaying IOCs and reports from TruSTAR that match log and event data stored in Splunk indexes.
- View TruSTAR reports in the Splunk app and launch IOC search and investigations against Splunk data.
- SplunkES capability to generate notable events from matched data.

For more information on setting up the Splunk-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that app., please see: <https://www.trustar.co/integrations/splunk-siem-integration-partner> and <https://support.trustar.co/article/zsgux8lk9e-splunk-v-2>

TAXII

LACL ISAO Partners with a TAXII client are able to ingest indicators in STIX format from the TruSTAR TAXII Server for use within their environment. A TAXII Server is software that offers one or more TAXII

Services by listening for connections from TAXII Clients looking to ingest data from the available services. In order to take advantage of this service, Partners must meet the following prerequisites:

- TAXII client running TAXII version 1.1
- TAXII client with ability to connect to a TAXII server running TAXII software version 1.1
- TAXII client with access to connect to TruSTAR TAXII server supported services (Discovery, Collection-Management and Collection Polling)
- TAXII client should be able to accept STIX 1.2 formatted packages

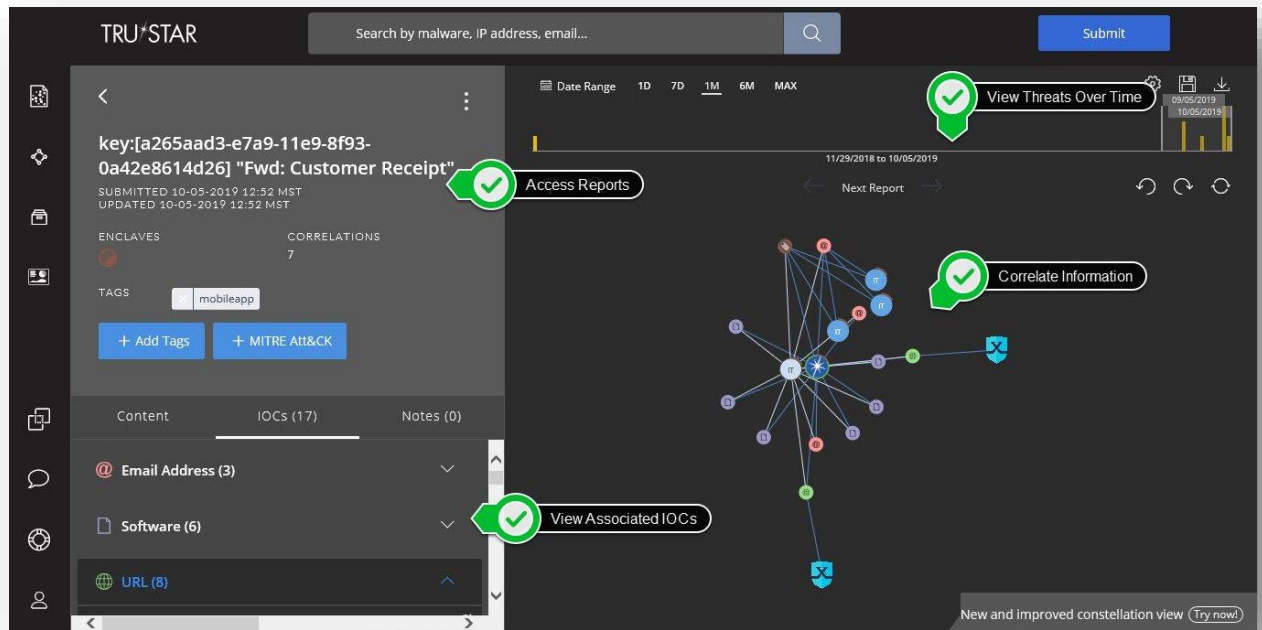
Features of this integration include:

- Allows users to ingest indicators from TruSTAR enclaves of their choice in STIX format into supported tools.
- Users can run discovery service to identify all available services with the TruSTAR TAXII Server.

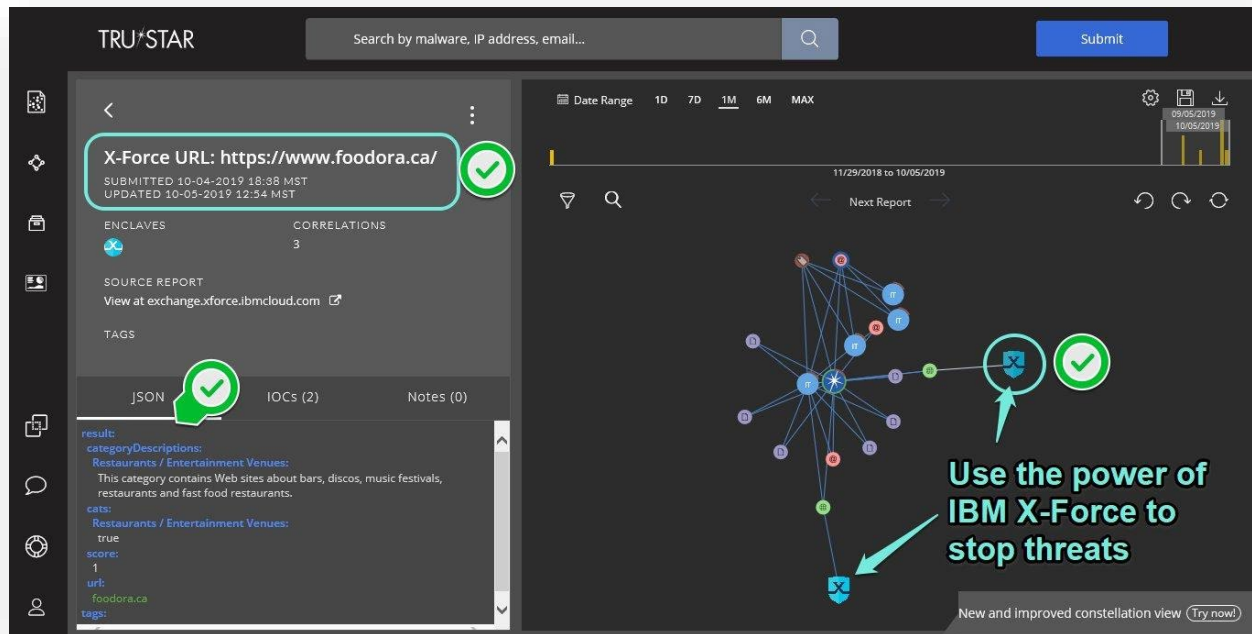
For more information on setting up the Splunk-TruSTAR integration and a current step by step guide to install, setup and troubleshoot that integration, please see:

<https://support.trustar.co/article/r1irw5srpv-server>. More information on STIX/TAXII can be found here: <https://oasis-open.github.io/cti-documentation/>

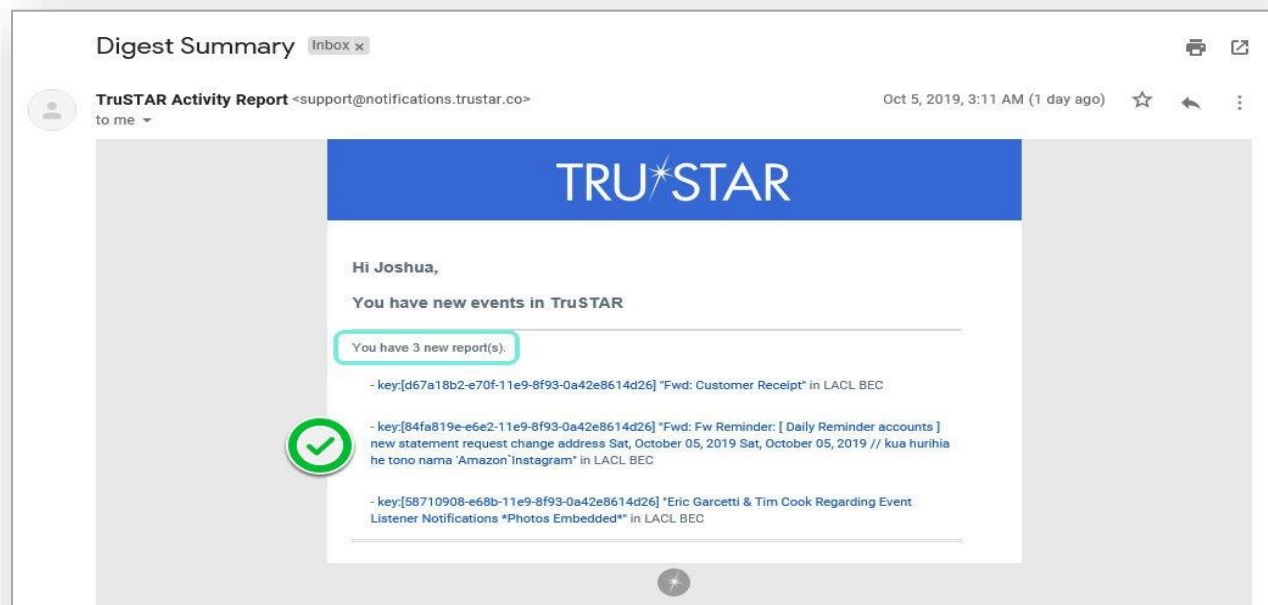
Threat Intelligence Sharing Platform (TISP) Screen Shots



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



The TISP is operational and is constructed with multiple data enclaves. The enclaves are 1) IOCs from partners, 2) business email compromise (aka phishing) and 3) Partner specific (e.g. Public Sector). The phishing IOC enclave is connected to the mobile application. On September 13th, the LACL launched the Los Angeles Cyber Lab mobile app in the Apple store and the following day in the Google play store. The app is free to download and offers users a daily tip, news feeds, trending data from the

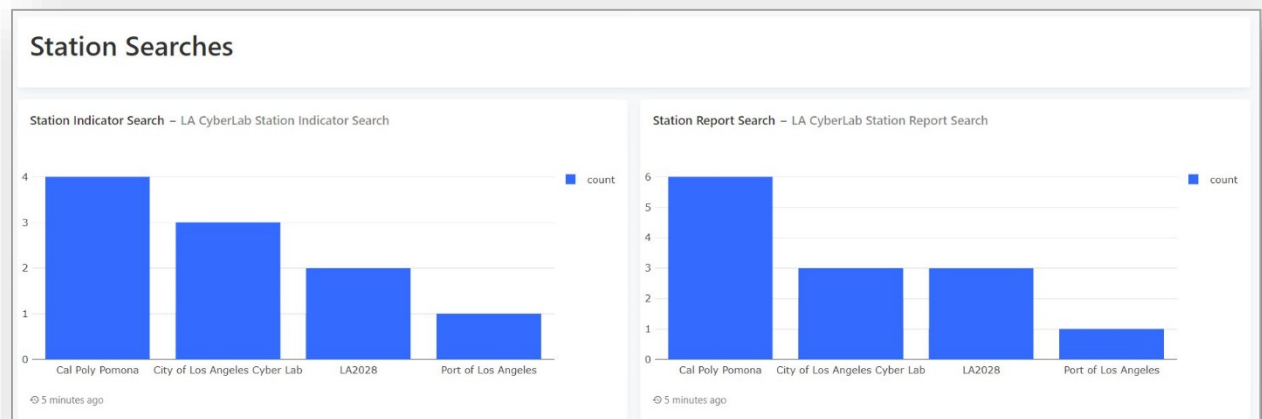


greater Los Angeles region, and has an inbox which provides them notifications about emails they have forwarded to the LACL. Notification responses currently average several hours. When an email is forwarded to the LACL it is ingested with certain selectors being extracted and matched against existing known phishing IOCs. The analysis is being conducted by IBM's X-Force Exchange.

Dashboards

Easy to understand, customized, and shared, dashboards are an assortment of widgets that give you a summary of the reports and metrics you should care about most. Threat intelligence dashboard provides information on threat activities. There are two types of dashboards organization-oriented (internal) and generic (external).

LACL TISP Dashboard



Generic Dashboards

Generic dashboards provide the information about global threat alerts and activities or about the community involvement. LACL uses the generic dashboards to track users with access to the TISP, login frequency, and use.

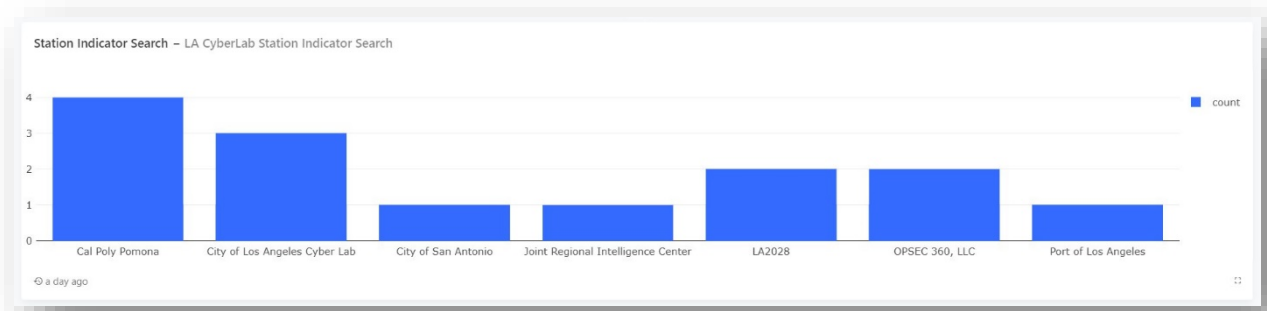
Organization Oriented Dashboard

These dashboards provide information about specific threats and alerts that organizations care about. LACL uses these dashboards to track high search values, import/export of data, and API usage. Knowing who is using the TISP to search for CTI is valuable as the LACL can collaborate with members to create detailed reports for the community.

LACL's information sharing community dashboard example.

Los Angeles Cyber Lab, Inc.

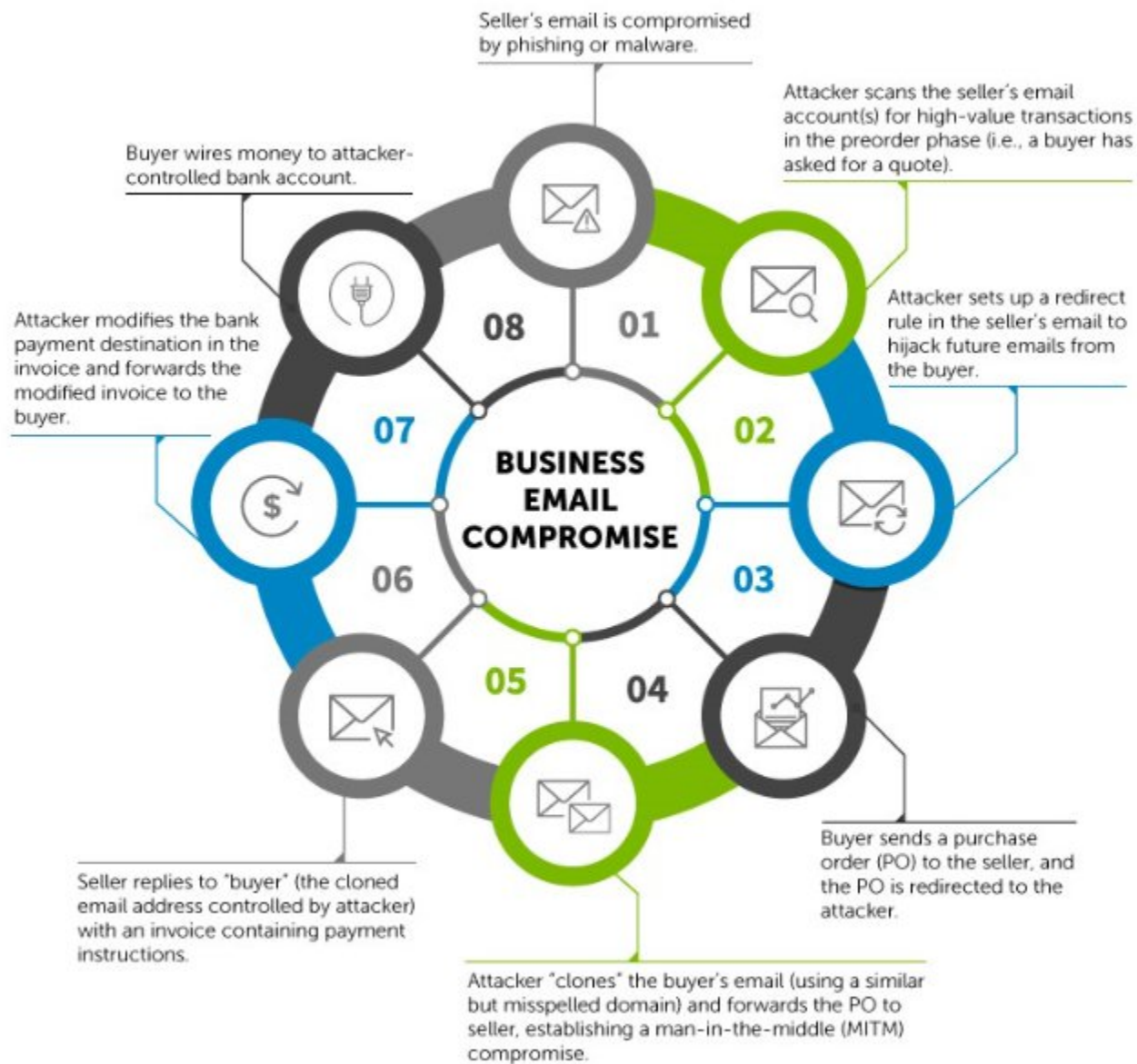
An Internet Security - Information Sharing & Analysis Organization



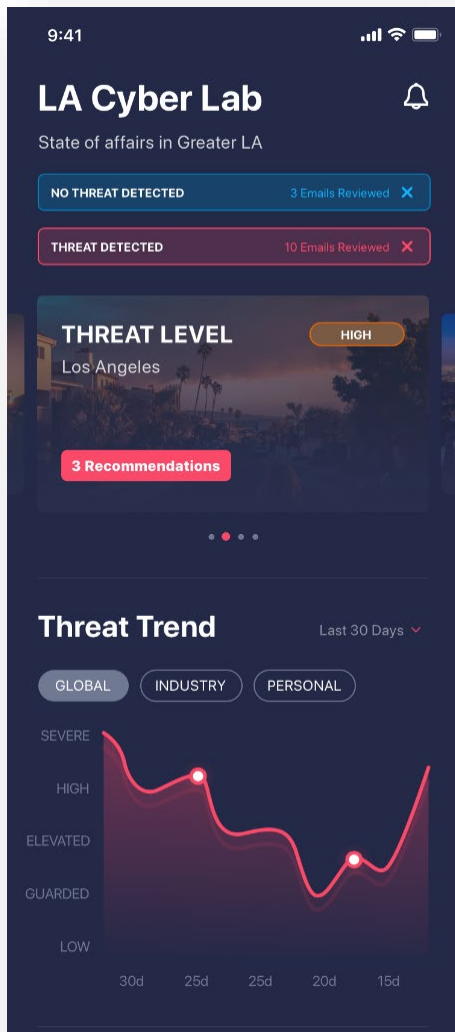
LACL Mobile Application

The LACL Mobile Application was developed in an agile capacity over a 90-day timeline in the summer of 2019. The mobile app was designed, tested, released and beta tested to validate and prove design logic. The application is a light middleware interfacing between the user and the LACL's TISP data lake.

The mobile app is the primary means by which the LACL engages SMBs and individuals. Functionality of the mobile app was designed through a series of small SMB focus groups in conjunction with the LACL team. The app was launched on September 13, 2019 and is available in both Apple App and Google Play stores. The app is free to download and does not have any purchase features.



The concept for the mobile app was created by the LACL to address the gap in SMBs and individuals having access to enterprise CTI. The lowest common denominator among all businesses is *email* and the most common cybersecurity issue associated with email is *business email compromise* (BEC). The LACL defined the scope of the mobile app as follows:



Mobile App Use Case #1) Design and launch a mobile application which connects SMBs and individuals with the LACL TISP.

Mobile App Use Case #2) Leverage the LACL TISP API for a mobile application which can render a score to users about a suspicious email.

Mobile App Use Case #3) Ingest emails, analyze, score, and disseminate the opinion via a mobile application.

Mobile App Use Case #4) Include RSS feeds of relevant cybersecurity news and information for display within the mobile application.

Mobile App Use Case #5) Design and launch a mobile application in both Apple and Google stores simultaneously.

Mobile App Use Case #6) View of a heat map which correlates the geographic location of emails submitted to the LACL.

Mobile App Use Case #7) Provide basic cybersecurity awareness information to users regarding their email submission.

With respect to Mobile Responsiveness Design and Testing, LACL utilized TRG's UX/UI design team, who

focused their approach on implementing an application that renders correctly across different devices, operating systems and screen sizes. TRG implemented the React framework to develop a modular, adaptable and fluid front-end design and user experience. Along with implementing React, The TRG UX/UI design team followed three development principles to ensure a responsive mobile application:

#1) The use of fluid Grids – This approach is based on the percentage of mobile real estate and not the historic pixel-based approach.

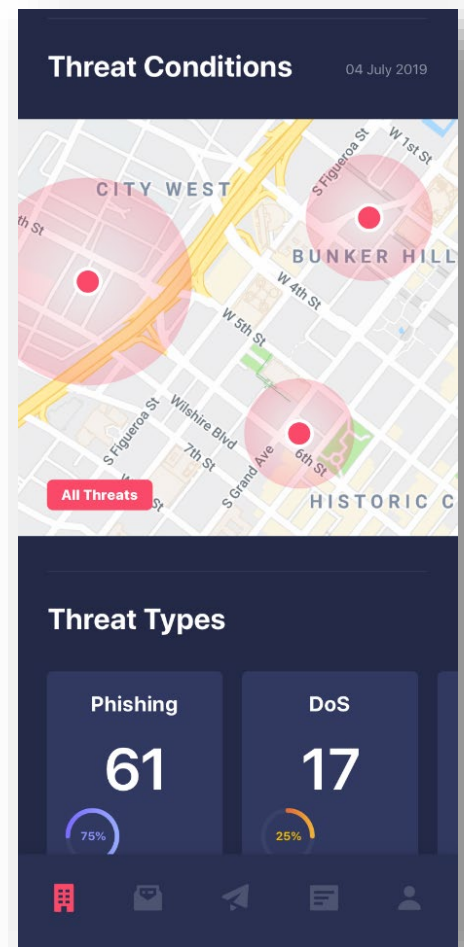
#2) Media Queries – This is used to apply different styles based on the device screen size.

#3) Flexible images and media – This helps to show the images and media differently in different sizes by using scaling or CSS.

Along with the development approach, it is equally important to test the application to ensure it is showing up as expected on all devices. A responsive application needs to give the same experience to the users across mobile operating systems and devices. It needs to be tested for device versions, different screen sizes, modes – landscape or portrait, etc. The content, videos, images, links, etc. all need to be tested for their appearance before releasing the application. For example, plotting on a map may look a little different on Android when compared to iOS. TRG executed the following test cases to ensure responsiveness of the mobile application across a variety of IOS and Android devices:

- 1) Verify whether the content fits on the screen and is not cut out or distorted.
- 2) Verify whether the feeds are loading and do not have broken links in them.
- 3) Verify whether the text color, the font etc, remain the same across devices.
- 4) Verify whether zooming in/out doesn't distort the map.
- 5) Verify whether fast scrolling doesn't distort the content.
- 6) Verify whether the links are working well and if they take the user to the appropriate page.
- 7) Verify whether the application back end calls are not timing out or taking too long to load.
- 8) Verify whether locking of portrait mode so content remains in the most optimum layout.
- 9) Verify whether the images of different types are shown as expected.
- 10) Verify whether navigating between cards in the mobile application doesn't distort the content etc.
- 11) Verify speed and responsiveness to query changes.

With regards to test case 11, TRG UX/UI design team calculated the impact of code and design choices on user experience. For example, typically, people get very frustrated if they have to wait more than one to two seconds for any UI feedback and therefore our mobile design aimed to load data dynamically to reduce the time to content access. For each iteration of the application, TRG measured



timing differentials in already-deployed features so to ensure that future iterations didn't impact performance expectations.

Understanding The Risk Score

The LACL Mobile Application utilizes the IBM's XFE which is aligns the risk score range with the Common Vulnerability Scoring System (CVSS), see <https://www.first.org/cvss/specification-document#5-Qualitative-Severity-Rating-Scale>.

LACL Mobile Application Risk Rating Matrix

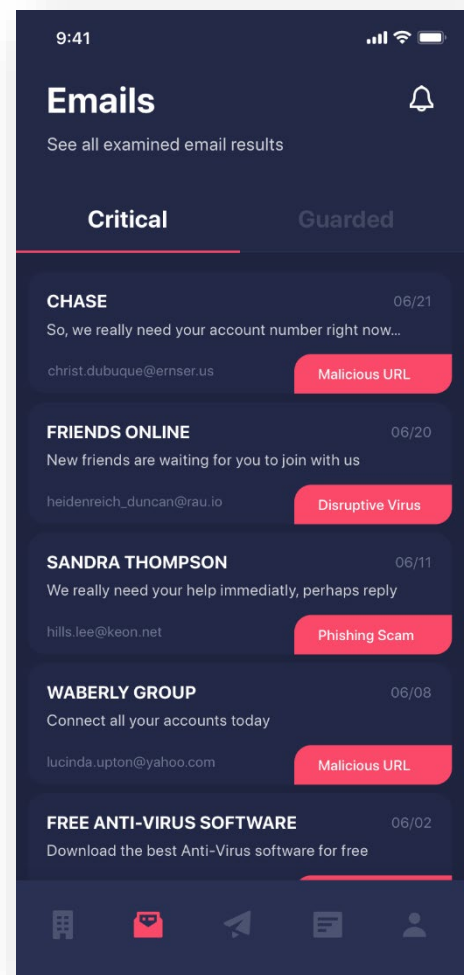
Score	Rating	Risk
0	Unknown (Not previously seen)	Guarded
1 - 3	Low - Medium	Guarded
4 - 10	Medium - High*	Critical

*Unlike CVSS, the Mobile App does not distinguish between High and Critical

Potential Issues and Limitations

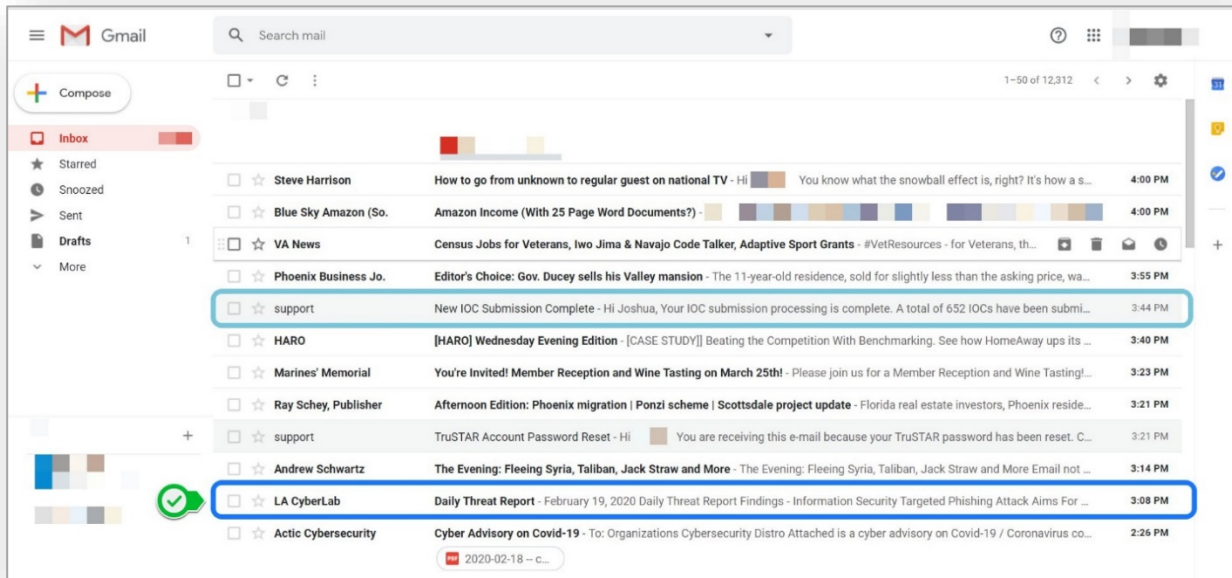
The LACL Mobile App proved to be successful for email providers such as *Hotmail, AOL, Yahoo, and Office 365*. The mobile application provided little value for those organizations utilizing Gmail since this service does a superb job eliminating phishing emails before they reach the user. The mobile application was downloaded over 230 times since its launch. Limitations of the mobile application include:

- False Negative #1: The email submissions are logically analyzed for known malicious IOCs; if a zero day or an IOC which is not within the LACL TISP data lake exists, it will not be positively identified.
- False Negative #2: The email submissions are not reviewed by a human or AI technology which reads the email, therefore, the message may in fact be a phishing attempt but the LACL Mobile App will not recognize it as such because only known indicators are triggering a positive result.
- The mobile app has limitations on the number of submissions which can be used to *call* the API in a 60 second window. While this limitation is not an immediate issue, if the adoption of the mobile app was significant to the point that thousands of submissions were simultaneously sent the result would be delayed responses.



Products and Services

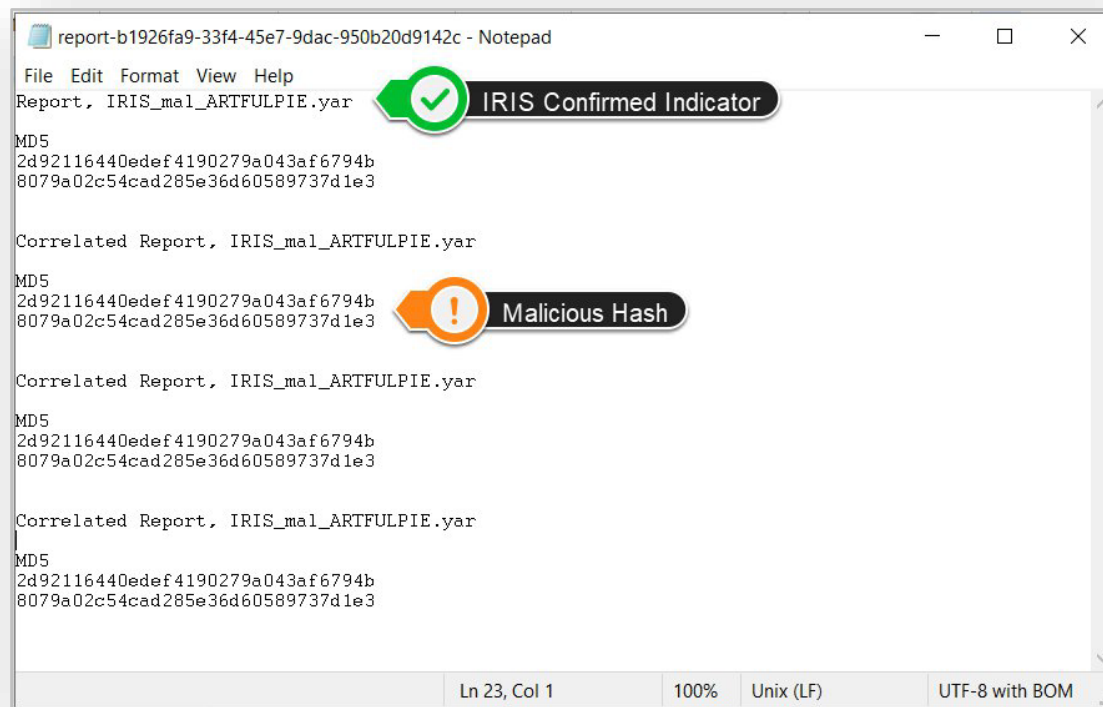
The LACL has created a series of products which are available to anyone, at no charge, and are designed to engage the community in a variety of forms. Connecting the Community, the LACL



designed these offerings to reach targeted audiences and to help educate recipients, grow the LACL brand, and to facilitate partnerships across the region. Below is a list of LACL products and services.

LACL Services

- Anti-Phishing Analysis and Cybersecurity Threat News via the *LACL* mobile app.
- Threat Intelligence via the LACL TISP through either an API or STIX/TAXII feed available to members.
- Threat Intelligence & Reports via the LACL TISP for partners & members with access to the platform; analysts are able to submit or work with data to create cases for IOCs; analysts can provide feedback to the community about ongoing threats and request assistance through the platform.



LACL Products

- **Daily Threat Report:** a daily emailed list of information and physical security events in the news. The communication is sent Monday-Friday excluding holidays.
- **Daily IOC Report:** a daily emailed link to two CSV documents, one including threat data and one including City of Los Angeles threat data. Examples of IOC consist of malicious hashes, URLs, IP addresses and websites. The communication is sent Monday-Friday excluding holidays.
- **Weekly Threat Report:** a weekly emailed list of security events in the news covering agriculture, defense, energy, financial, insurance, healthcare, legal, litigation, regulatory risk, operational risk, pharmaceutical, reputational risk, retail and technology sectors.
- **Ad-Hoc & Special Report:** ad-hoc emails are sent only when a specific information security risk is identified, typically this communication contains immediate/near real-time threat information and actions which businesses should consider; special reports are an emailed PDF attachment containing information about either major events or significant information security issues.

Example from the Daily Threat Report

New and Updated Information on North Korean Malicious Cyber Activity

Created: Friday, February 14, 2020 - 09:58

Categories: Cyber Security

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the Department of Defense have provided new and updated information on malicious cyber activity by the North Korean government. In six new Malware Analysis Reports (MARs), these agencies discuss and provide technical information for Trojan malware variants used by the North Korean government. The new Trojan malware variants include BISTROMATH, SLICKSHOES, HOTCROISSANT, ARTFULPIE, BUFFETLINE, and CROWDEDFLOUNDER. There is also an updated MAR for HOPLIGHT, which was initially reported on last year. In addition to malware descriptions related to HIDDEN COBRA, the MARs contain suggested response actions and recommended mitigation techniques. The MARs encourage users or administrators to flag and report activity they describe to CISA ([online reporting form](#), CISAservicedesk@cisa.dhs.gov, or 1-888-282-0870) or the FBI CyWatch (cywatch@fbi.gov or 1-855-292-3937), and give the activity the highest priority for enhanced mitigation. *[Read the MARs at CISA.](#)*

Identify Barriers to Information Sharing

Identify barriers to cyber information sharing in CISA’s AIS and how do we incentivize SLTT to share both with the government and one another to improve the collective defense posture of the nation and key private sector entities?

LACL Overview and Progress

The LACL has made significant progress towards the information sharing initiative grant objectives. During the past 18 months the LACL has grown 48 percent, reaching hundreds of businesses and SLTT organizations in the region. The efforts of the LACL have focused on establishing a TISP, a mobile application, and significant outreach. The LACL has worked steadily to establish a credible brand whereby organizations within the region can trust the LACL and will want to do business with us. As of March 31, 2020, there were seven TISP partners sharing data. The reason for the slow pace of onboarding are numerous and complex. This request details the systemic, technical, and organizational obstacles encountered.

LACL has identified four systemic issues that exacerbate eight specific technical and organizational obstacles. An extension will allow LACL to continue to identify, document, and solve or mitigate these barriers. The matrix below provides an overview of the systemic issues and specific technical and organizational obstacles LACL has identified.

Barriers to Information Sharing Matrix

Systemic Issues	← Unique Organizations →	
	← Competing Priorities & Lack of Resources →	
	← Time →	
	← Trust →	
Obstacles	I. Technical	II. Organizational
Specific Obstacles	A. Version Control	A. Segmented Organizations
	B. Decentralized IT/Security	B. Risk Aversion
	C. Data Ingestion	C. Awareness
	D. Security Maturity/Technical Infrastructure	
	E. Marketplace	

II. SYSTEMIC ISSUES

LACL has four identified three systemic issues that impact several specific technical and organizational information sharing obstacles. The LACL has had interactions with over 1,000 public and private sector organizations. The interactions with these organizations have allowed the LACL to identify these issues and obstacles.

The systemic issues identified are:

- A. **Unique Organizations:** The LACL sharing partners are diverse, complex, and dynamic organizations with varying security maturities. These organizations have different structures, authorities, and individuals in control of policies and technical security tools. For example, a CISO does not always have the same authority in every organization (*Case- County of Los Angeles 3*). Some organizations are risk averse to the concept of “sharing data” (*Case -City of Santa Monica*). This problem extends to the technical domain, each organization uses different technical tools, configurations, and versions which requires LACL to work closely with each partner, learning about their specific obstacles. **Exploring technical configurations is a case by case approach which is time and resource intensive.**

Mitigation: LACL continues to learn, adjust, and document solutions for the range of onboarding organizations. **Future attempts in CTI sharing require a deep understanding of the partner in order to effectively engage organizations, understand unique challenges, and further develop the onboarding process.** Specifically, the extension will allow for two things:

- 1) Feedback received will inform how LACL refines the TISP and develops streamlined and adaptable onboarding processes and procedures.
- 2) LACL is building a solution catalog, documenting solutions to specific problems.

The combination of a streamlined and adaptable onboarding process, with a solutions catalog will allow LACL to quickly onboard a diverse group of organizations.

- B. **Competing Priorities/Lack of Resources:** The TISP and onboarding support is provided to partners at no financial cost. However, the onboarding process requires partner staff participation with LACL. Competing priorities and lack of resources are a significant onboarding issue. The national cybersecurity workforce shortage further exacerbates this issue within the Los Angeles region; security teams are already understaffed and unable to fill technical positions. Even the LACL experienced difficulty hiring a competent cybersecurity analyst. The LACL onboarding team often waits for partners to provide information or make technical

“People do not understand the term ‘information sharing’ – they think, ‘Oh! I’m sending my personal information to the LA Cyber Lab.’”

– Chris Covino, City of Los Angeles

adjustments. For example, it took one partner three weeks to create a technical security rule to allow information sharing (*Case-Creating a Security Rule*).

Mitigation: LACL has identified a key migration strategy: clearly provide partners with the value of joining the TISP. Currently, LACL is working on a value proposition document that shows the cost benefits of the TISP platform. When potential sharing partners better understand the value of the TISP, they will be more likely to prioritize its implementation. It is important to provide partners information in understandable contexts for executive level decision makers and technical implementers. LACL continues to refine the TISP and develop the onboarding procedures and a streamlined process.

- C. **Time: *The greatest obstacle to CTI sharing is time because it is a requirement of all parties involved.*** The investment of time is something which cannot be quantified owing to the many unknowns both technical and non-technical within each relationship. The average time for an ISAO to begin receiving CTI from a partner is 14 months. The LACL was able to dramatically shorten this timeline for several instances but has discovered that CTI sharing takes months to align people, technology, and coordination, all of which are required to complete the CTI sharing circle.

Mitigation: LACL created the “LACL+1” concept which is the method highlighting the importance of one-on-one relationships with members and partners. Building relationships with the private sector differs greatly from those with the public sector. Each has different objectives, needs, and reasons for participating.

- 1) Public Sector: Is best engaged by leading local municipalities; LACL utilized representatives from the City of Los Angeles to successfully engage other cities & counties leveraging clearly demonstrated common goals.
 - a. Common Goal 1) **Necessity:** Cities need to work together to protect themselves; beyond CTI sharing, public organizations have many other reasons to work together, but few have found a viable way to collaborate on cyber threats – until now.
 - b. Common Goal 2) **Trust:** Public organizations can easily sell their partnership with the City of Los Angeles with limited or no obstacles to share information; contrastingly, when requesting to share with private organizations, public sector officials often had many more questions and were reluctant to move forward without assurances related to privacy and access.
 - c. Common Goal 3) **Public Service:** the City of Los Angeles offered assistance in the form of the LACL to other public organizations as a public service to their fledgling security programs.
- 2) Private Sector: LACL found that in some cases private organizations wanted a relationship with the City of Los Angeles for publicity, positive marketing, and for future sales leads. However, the primary motivation for private organizations was their interest in obtaining access to information previously unavailable to them.

- a. **Social Responsibility:** The LACL has developed a narrative for larger organizations to begin CTI sharing as a part of their social responsibility.
- D. **Trust:** Creating a community in which disparate organizations are willing to provide their CTI is a challenging task. There are several stages in which the LACL gained participation in the TISP: 1) establishing contact – identifying the right person to speak with; 2) building rapport and relationships; 3) establishing value; 4) learning motivations; 5) make natural connections about the CTI sharing framework; 6) invite the organization to share; 7) coach individuals as needed about the ways and means of sharing; 8) provide honest feedback about what works and what doesn't; 9) re-enforce the altruistic and practical necessity of CTI sharing; 10) reward participation.
- a. LACL anticipated that many organizations would require a formal sharing agreement because of data sharing concerns. However, of 45 organizations, only one requested a memorandum of agreement (MOA).
 - b. Some SLTT desired to have a dedicated enclave within the TISP for city/county members only based in some type of fear that their data would be shared with the private sector.
- E. **Mitigation:** Inherent to the TISP are a series of configurations which allow organizations to control (manage) the CTI they want to contribute to the LACL community. The TISP allows for redaction and provides the ability to tag data as desired prior to sharing. These features were sufficient for each organization to have a basic level of confidence and trust in the LACL's TISP. Sharing starts with people and ends with people; relationships are the basis of all trust and the technology is the secondary means. With technology meeting industry requirements, the LACL focused on building relationships. Regarding the segregation of SLTT data, the LACL created a dedicated enclave to encourage CTI sharing but maintains that too many enclaves will further dilute the intentions of CTI sharing. Therefore, the LACL limits the creation of additional enclaves to specific use cases and pushes partners to share to a single enclave. The results have been positive in the majority of cases.

III. TECHNICAL OBSTACLES

- A. **Version Control:** The current version of the LACL TISP (TruSTAR platform) is not compatible with all software. This has slowed the onboarding process and required both LACL and partners to commit more resources towards technical troubleshooting in order to identify the unique organizational issue.

Specific Cases include:

- o *Case- Q-Radar Integration:* One partner attempted to connect with their Q-Radar tool. Organizations utilizing Q-Radar must have a version 7.3.2 or newer to connect with the LACL. Older versions will not integrate.
- o *Case- Splunk Integration:* The LACL TISP has a native integration with Splunk, a well-known and highly utilized security information management tool. However, the TISP

integration is not designed for every version of Splunk. Splunk cloud-based versions require additional configuration and setup in order to connect. Specifically, in both cases the Partner had to whitelist TruSTAR, an IP address, and set their tool to allow for the connection. Each case is different and has required time and multiple dialogs to resolve.

Solutions Moving Forward: The LACL continues to document these lessons learned and catalog them for future onboarding. Specific actions LACL will take include documenting basic configuration requirements. The basic configuration requirements depending upon the tools being used will dictate the onboarding process and reduce time, energy and confusion.

- B. Decentralized IT/Security:** Partner's struggle with internal stakeholder support & approval because there multi-layered approvals which operate on a slow timeline.
- *Case -County of Los Angeles (1):* County of Los Angeles departments provide their own IT services or contract out to the County's Internal Services Division (ISD). County ISD provides some or all IT services depending on the department request. This decentralized approach extends to security, and there is no centralized security operations center that collects data and arrogates IOCs from all County departments. The County can only arrogate IOC's from departments that choose to use ISD's services and the County cannot provide an IOC feed from the entire County. To further complicate this issue, the County CISO is within the Chief Executive Office and does not have direct control over ISD.

Solutions Moving Forward: Rather than working with a central IT security agency, LACL must work with both ISD and individual departments. While LACL is pursuing this approach, individual department bureaucracy and security maturity then become issues. LACL will continue to work with the County CISO's to prioritize and strategize. Involving ISD is the first priority. **The LACL spent several months engaging the County of LA before these issues was identified.**

- *Case- Local Cities:* Initially, LACL expected smaller cities to have a more unified IT and cybersecurity. In reaching out to other cities, this assumption proved to be untrue and typically cybersecurity and IT functions have been placed under the individual department in both funding and responsibility. In one case, we observed the police department's cyber-crimes team and the city's IT to be separate and distinct organizations with completely different capabilities.

Solutions Moving Forward: LACL had to rethink its approach to SLTT as a result and has begun engaging. The LACL may need to engage individual departments rather than a centralized IT agency. However, this must happen with the help of City CIO/CISOs.

C. Data Ingestion: LACL was under the impression that organizations were already prepared to share automated threat data. Therefore, we were not anticipating many issues in the onboarding process.

- *Case -City of Los Angeles:* There has been a variety of issues while attempting to ingest City of LA data into the TISP. LACL attempted to ingest City data directly via CSV file and discovered that the City had not properly configured the data to be exported. LACL helped the City make adjustments to the naming of their exported IOCs. The idea was to ensure the information was parsed correctly once ingested. The API could only handle 500 items in a single line or 10k IOCs in a single push of data, this was discovered through trial and error. These particular API limits cannot be adjusted for ingestion purposes. Several other methods were attempted including the use of Splunk to ingest information. The City uses Splunk cloud-based version which was not directly compatible with the TISP's marketplace Splunk native integration. Adjustments to the Splunk cloud configuration and its information is flowing from the LACL to the City of LA. Currently, the City provides data via an email-based push. However, in order to automate the data flow through STIX/TAXII, a script needs to be created by the City and a stash needs to be established by the LACL to parse their data as it ingests through the API even though it will be sent in a STIX compliant format. The City doesn't have the internal capability to write the script.

Solutions Moving Forward: LACL is working with IBM to create the script to parse the data for the City of Los Angeles. However, other organizations plan to utilize Splunk and a STIX compliant format to connect with the LACL.

- **Executive Dashboards:** Partners have expressed a desire to have executive level dashboards. However, executive level dashboards are not available yet because the TruStar platform requires a minimum flow of data over approximately 90 days. LACL and TruStar also need to assess the functionality and fine tune the dashboards for partners.

Solution Moving Forward: Data began to flow into the TISP on October 2019, therefore by January 2020 the minimum data/time threshold will be met. The LACL established dashboards in February 2020 which provide details into which organizations are sharing information, how the information is being shared, and what information is being contributed and consumed.

- **Automation:** Although many of the marketing materials we have refer to a "system" that "automates" the secure sharing of Cyber Threat Intelligence, there are still a number of processes that, from my perspective, are either manual – or the Partner must complete key steps before sending the data to the TISP. For example:
 - i. Identifying data for sharing

- ii. Anonymizing data
- iii. Assigning TLPs

D. Security Infrastructure & Maturity: Many Organizations do not have the tools, processes, and staff in place to share information.

- *Case -County of Los Angeles(2):* The County CISO's have informed LACL that the County IT provider, the Internal Services Division (ISD), may lack the required security infrastructure to adequately arrogate, analyze and share the IOC's to the TISP.
- *Case -Cities of LA County:* This summer, over 85 municipalities (local cities) were invited to join the TISP. Of the five that responded, **none were technically capable of providing threat data to the LACL.**

Solutions Moving Forward: The concern is that LACL will work with Partners through Phase 0 (exploratory) and Phase I (discussion), but in Phase II (Technical onboarding) realize the partner is technically unable or limited. While LACL is actively pursuing additional partners, **time is needed to develop a clearer vetting process.** LACL is still figuring out what questions need to be asked in Phase 0 and I. The extension will allow LACL to engage with more partners and fine tune the vetting component of the onboarding Processes.

E. Marketplace: TruSTAR offers a marketplace of apps which are a list of existing integrations. The marketplace apps include a variety of IOC feeds which are available through the use of an API. The feeds are either no-cost or paid. The particular issue with these integrations is that certain apps such as Splunk, require staff time set up these to connect.

- *Case-Creating a Security Rule:* A partner's internal security measures blocked marketplace integration, this required the partner to create a new security rule. **It took three weeks for the partner to resolve the issues, causing a significant delay in the onboarding.** Although LACL is unsure of the reason for the delay, this was probably due to internal priorities, an example of the systemic issues previously mentioned impeding the onboarding process.

Solutions Moving Forward: As mentioned in the mitigation of *Systemic Issues#2 Competing Priorities/Resources-* LACL must continue to show partners the sharing value, so they are more inclined to prioritize TISP onboarding. Second, it is important to catalog solutions to quickly and clearly provide partners with solutions.

IV. ORGANIZATIONAL OBSTACLES

A. Segmented Organizations & Security Authority: LACL has encountered issues with larger organizations that lack centralized authority over cybersecurity. This issue has been seen in larger public sector SLTT and the impact to sharing equals a longer timeline.

- *Case- County of Los Angeles (3):* The County of Los Angeles CISO is within the County Chief Executive Office, this position provides strategic and policy guidance but does not have direct control over day to day security operations. The County's Internal Services Division (ISD) is a separate operational County division that acts as an internal managed services provider. The County's CISO and Deputy CISO have been in ongoing discussions with LACL and want the County to become a LACL sharing partner but they must work internally to bring ISD onboard, then ISD must work directly with LACL to work on the technical onboarding. This has significantly slowed onboarding.

Solutions Moving Forward: LACL continues to work closely with the County CISO to develop an internal value proposition to pitch to ISD. LACL is learning from this process and is prioritizing the creation of documentation that potential partners can use to build support internally. This case highlights *Systemic Issues#1-Unique organizations*, and the need to understand organizations to streamline the onboarding process. LACL considers a best practice to onboarding is to work closely with organizations to understand their issues. **LACL is working to streamline the approach by working closely with partners and expanding brand recognition.**

B. Organizational Risk Aversion: Some potential partners have expressed discomfort with the idea of sharing any data. During Phase I and II meetings, there is often a natural knee jerk reaction to the idea of sharing data. While third party risk is a significant issue, but information shared to the TISP is not and should not be sensitive information.

- *Case -City of Santa Monica:* The CISO for the City of Santa Monica has expressed concern about sharing data with unknown partners (i.e. LACL/TruStar). Understandably, the CISO is concerned about unvetted third parties. The CISO said they were more comfortable working directly with the City of Los Angeles.

Solutions Moving Forward: LACL has identified two strategies to mitigate these issues:

- 1) Clearly inform potential partners of the type of data that is shared into the TISP. LACL only requests IOC's, nothing that would include sensitive data. LACL needs to make it clear to partners that they decide what to share based on their risk tolerance. *Understanding the technical skill level of the partner is difficult to determine initially and at times has required extensive discussion (e.g. teaching).*

2) Leverage existing Partners to help. Work closely with the City of Los Angeles to assuage fears and provide alternative sharing solutions. For example, the City's Cybersecurity Policy Director is now working directly with Santa Monica to address sharing concerns. If a partner is still not comfortable sharing with LACL, alternative sharing options with the City are available. Information shared with the City will then become part of a larger City threat feed into the TISP.

- C. Awareness:** Even in the absence of other obstacles, the LACL discovered that information sharing was vastly more successful when organizations became aware of the LACL's mission organically. In several instances, attendees to the LACL Security Summit returned to their offices and discussed the TISP resulting in their immediate membership. Organizations which self-identify typically contact the LACL through one of their security engineers or architects.
- LACL was not contacted by a cybersecurity analyst or researcher for TISP membership during the pilot project. LACL assesses that the media and marketing campaigns did not connect with professionals in a position to either recognize the benefits of the TISP or were not in a decision-making role to request inclusion.
 - Many people were unclear about what *information sharing* meant. Further, once explained it became obvious that in many conversations the LACL was not reaching the proper individuals to engage which lengthened the process of gaining success in information sharing efforts.

V. OTHER INITIATIVES

Technical Methods / limitations

Mobile application scoring of phishing data: the construction of the light middleware application which feeds to the TISP functions as designed; a better investment in funds and future efforts could be to increase either the enclaves within the TISP or to increase the phishing specific data feeds to the BEC enclave within TruStar.

Dashboards were provided within the TISP. However, they were insufficient for the desired use cases of C-Suite and security leaders. The existing dashboards are designed for analysts which is the core function of the TISP. Executive dashboards are required to help present the information to non-technical audiences and to create business dialogs about threat intelligence and the values of the TISP.

We need to push "protection through partnership" and "how do we work together?" We work together by sharing information. Not any information but specific information.

TISP Management Best Practices

Sharing Concerns

RH-ISAC for example, two analysts on staff to review submitted data for vetted intelligence which they pull insights out. Intelligence is then shared to another enclave which is subscribed to.

Ingestion:

A community of trust in which members share information of which the value is undetermined. LACL requests all members to provide quality data which they believe to be high confidence intelligence.

Policy and Management: provide best practices of tagging and labeling data prior to sending in IOCs. LACL can mature the program by enforcing submission best practices.

Subscriptions:

Establish a new enclave which can be shared at a later date. As membership grows, LACL can provide a new feed which it rolls out later with vetted intelligence.

Create enclaves for members who were owned by malware and offer it to other members.

LACL has not established a direct feed for members but instead uses the ingestion tool as the exportation location.

SOC best practices: a SOC manager may assign a higher confidence to a vetted source despite subscribing the LACL general feed.

Recommendation #1: CISA is requested to confer with LACL about previous/past successes and failures utilizing API & STIX/TAXII protocols for bidirectional machine to machine data sharing. Specifically, any preexisting use cases which could be relevant to the LACL's efforts would be appreciated as it begins the RFP cycle.

Conclusion #1: Feedback from Dollar Shave Club security team was: provide automation on shared IOCs in the form of ingestions rules. When a STIX pull is initiated by the ISAO member IOCs with rules will automatically *"block at firewall & flag for review"* – The LACL is incorporating this request into the scope of work for the project.

Conclusion #3: Members are looking for changes in the current daily threat report which provides infosec news. The LACL is creating a Special Alert Report which will provide members the ability to receive timely notice of LA specific threat intelligence. The special report will focus on one subject with a brief description of the issue and actions available via embedded links. Additional functionality to the existing reports will give the members the ability to select the frequency of how often they receive reports (e.g. daily, weekly, special, etc.)

Conclusion #4: Private sector companies want more data enrichment on IOCs being shared from the LACL. The most likely way to do this is in the analysis phase of the CONOPS. Additional

information is needed to define what type of data enrichment the LACL might be able to provide. *This information is consistent with conclusion #1.*

Conclusion #5: One obstacle to information sharing is the perception that sharing information which is not actionable is viewed by some as “providing more noise.” Specifically, POLA has defined a narrow space within which they want to share threat information but the use of the LACL as their portal is likely not the best strategy because they view the LACL portal as *too much information* for their niche group of partners.

Conclusion #6: The National Homeland Security conference event could have more cyber sharing-centric focused tracks for ISAO/ISACs; the MS-ISAC conference was a good event for networking and for promotion of the LACL.

Conclusion #7: Members sharing information to the LACL via the threat intelligence sharing portal might be limited by the software version of their existing tools. The LACL is identifying which tools and versions are compatible.

Conclusion #8: Partners will share information on their own timeline. There is virtually no incentive to motivate partners to share before they are ready. LACL has attempted to motivate partners with very limited success despite employing the standard methods of engagement.

Conclusion #9: Most SLTT members were not in a position to take advantage of the Cyber Lab’s free threat intelligence. We found that the majority of attendees were outsourcing their IT and cybersecurity. We also discovered that the key to making connections with the tribal organizations was to attend their meetings in person versus electronic or telephonic communications.

Conclusion #10: SMB has traditionally been a difficult group to engage through information sharing. The mobile app is creating a new means of interacting with these businesses. Adoption of the app and usage will be the keys to future success.

Impacts of the Pilot Project

What is the impact of the project? How has it contributed?

The pilot project is providing a nexus for SLTT and business to communicate. Further outreach is required to broaden the impact of this grant funded opportunity.

SMB has traditionally been a difficult group to engage through information sharing. The mobile app is creating a new means of interacting with these businesses. Adoption of the app and usage will be the keys to future success. Currently there are 219 authenticated downloads of the mobile app. The mobile app has become a great conversation starter with people at all levels of business and often leads to a deeper conversation of the TISP.

What is the impact on the development of the principal discipline(s) of the project?

No other convergence of technology currently exists. This is the first time an enterprise tool is being used to facilitate sharing to a community level. Existing solutions and tools provide threat intelligence to mature security organizations and teams.

The mobile phishing app wraps around the TruSTAR API and pulls IBM IRIS results for emails being ingested through the app. This effort is pioneering the future of threat information sharing and aggregation.

What is the impact on other disciplines?

Data from the pilot project may become useful for researchers looking to discover trends and analysis of indications of compromise in the region.

What is the impact on the development of human resources?

None, this project does not substantially change the process or fundamentals utilized by cybersecurity analysts. The impact to cyber threat analysts' being informed and able to work with and collaborate with other analysts is improved through this pilot project.

What is the impact on physical, institutional, and information resources that form infrastructure?

None, the pilot project is a cloud-based architecture and does not create additional infrastructure physically or institutionally.

What is the impact on technology transfer?

None, this pilot project had no impact on technology transfer.

What is the impact on society beyond science and technology?

The LACL's mobile app could prove to be a vital connection between SMB and the greater Los Angeles business community; this is the first time where enterprise level CTI has been used as a data source linking SMBs. Managed security services provide some access to SMBs but no direct link or access to higher level CTI.

What dollar amount of the award's budget is being spent in foreign country(ies)?

None of the grant funds were spent with foreign countries or outside of the United States of America.

Develop Documentation

Develop documentation including design, policies and procedures, CONOPS, and operations manual(s).

Policies, Procedures, Techniques

The LACL created the following documentation during the pilot project to guide

Policies

- LACL Acceptable Use Policy
- LACL Access Control Policy
- LACL AWS Database Credentials Policy
- LACL Frequently Asked Questions (FAQs)
- LACL IBM Policy Guidance
- LACL Intellectual Property
- LACL ISAO Framework
- LACL Mobile App Security Policy
- LACL Mobile App User Manual
- LACL Mobile Application Responsiveness Policy
- LACL Payment Process
- LACL Privacy Policy
- LACL Systems and Infrastructure
- LACL Threat Sharing Capability
- LACL TISP Support & Maintenance Procedures
- LACL Travel Policy
- Threat Intelligence Sharing RFP Diagram (CONOPS)
- TruSTAR Support & User Manual

Procedures

- LACL Change Request Form
- LACL Configuration Management Policy
- LACL Information Protection Security Change Management Policy
- LACL Information Protection Security Password Policy
- LACL Partner Sharing Policy
- LACL Data Retention Policy
- LACL TISP Partner Onboarding Policy

Techniques

- Analysis Methodology
- Feed Overlap Analysis Matrix

- IOC Use Cases (MISP)
- LACL IBM X-Force Exchange Risk Scoring
- LACL Middleware Email Scoring
- LACL Mobile App Final Wording for Threat Levels
- LACL Threat Data Sources
- LACL TISP Dashboards
- LACL TISP Middleware Cloud Architecture
- LACL TISP Reports
- LACL TISP Admin Instructions
- LACL Mobile Application Test Scrips Execution
- LACL Unit Tests Execution Consolidated Feedback and Issues

LACL TISP Maturity Model

Threat Intelligence Sharing Platform (TISP) Maturity Model			
	Basic <-----> Advanced		
Level	Access	Integration	Sharing
What	Access to threat intelligence data through the TISP (TruSTAR platform web application).	TISP access and threat intelligence data integrating with security tools	Full security tool integration, including aggregating and sharing IOC to the TISP
	Indicators of Compromise (IOC)	IOCs & Research Enrichment	IOC Reports & Case Enrichment
Benefit	Provides additional security insight. Users can see shared threat data, perform research, see trends etc.	Integrated threat data to make analysts and tools more accurate and efficient.	IOC's from the TISP are integrated into security tools, organizations share IOC into the TISP.
	Benefit to Member	Benefit to Community	Benefit to All
Sharing	Can manually upload reports (e.g. CSV)	Can manually upload reports. Limited Automated Sharing with existing integrations.	Automated Sharing between tools and TISP via API or STIX/TAXII
Who	Smaller organizations that lack the infrastructure for integration of sharing.	Medium organization with some security tools and limited staff.	Organizations with dedicated security staff and mature security infrastructure.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Role	Researcher, Analysts, Engineers, Investigators		
		Security Engineers	
Requirements	TISP account and web browser	TISP account & Tools capable of ingesting threat intelligence	Organizational capability to identify suspicious and malicious traffic and the ability to share data

Social Media Outreach

The Facebook groups LACL engaged included communities of information security professionals, IT professionals, programmers, computer scientists/engineers as well as women groups wanting to explore the cyber field. The primary mission of these groups is to advance women in cybersecurity by providing programs and partnerships that promote networking, education, mentoring, resource-sharing and opportunities. Most LACL followers are interested in LACL TISP, training programs, networking and job searches.

- Women in Cybersecurity (WiCyS)**most interested in LACL*
- Women’s Cyber Jjutsu
- Los Angeles Business Group
- Cybersecurity Professionals
- Cybersecurity Jobs
- Cybersecurity Lounge

LACL maintains the following social media accounts used to interact with the community:

Facebook	Los Angeles Cyber Lab	Created July 2, 2019 with no presence or followers; currently has 147 followers
Twitter	@LACyberLab1	Created in 2017 – Posting tweets regularly
Instagram	CyberLabLA	Created in 2018 – Limited Use
LinkedIn	Los Angeles Cyber Lab	Created September 2019 – abandoning the LACL account
YouTube	Los Angeles Cyber Lab	Created August 2017 - 7 videos

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



Conclusions

More interest and followers could be gained with providing academic cybersecurity training programs, job placement/opportunities and networking events.

Work with Academic Partners

Work with academic partners who will utilize the IS-ISAO operation center to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology.

The LACL engaged the academic institutions in a variety of ways to explore information sharing opportunities. Academic institutions each have their own niche within the cybersecurity education continuum. As the LACL worked with each organization it identified the unique assets, potential for collaboration and audience these groups served. Larger academic institutions have multiple departments and organizations within the overarching structure and are largely siloed both in terms of budget and information. Effectively engaging these organizations requires a deep understanding of their capabilities and interests. The LACL explored creating courses in cybersecurity, certificate programs, undergraduate and graduate level research projects, and leadership seminars. Ultimately, the LACL was abandoned creating courses and certificate programs because of time and resource constraints. The LACL lacked substantial data to propose a meaningful research program and decided to re-engage in those conversations at a later date. Success was achieved with academic partners in two ways: participating in business school cybersecurity seminars and in supporting student learning through hands on access to CTI via the LACL TISP.

University of Southern California (USC) Information Sciences Institute (ISI), a leading graduate research university within Los Angeles, California, has been a member of the LACL Advisory Board since its inception. USC-ISI provided some initial thoughts and posed questions to the LACL during its creation of the TISP concept of operations. USC-ISI expressed desire to further discuss potential research opportunities with its engineering students but was unable to provide the LACL with any ideas, research proposals or concepts. The LACL database of IOCs was too small for USC-ISI to work with during the pilot period. As LACL IOC data grows through contributions of its members, USC-ISI and LACL will revisit the topic and determine what contributions can be made to the community through academic research.

USC Policy Program Initiative:

The USC, in partnership with the Office of Los Angeles Mayor Eric Garcetti is planning an interdisciplinary Cyber Policy Initiative. This joint initiative will include USC's schools of Public Policy, engineering, law, business administration, communication, the Mayor's Office of Public Safety, and the Los Angeles Cyber Lab. Strategic Direction would come from an interdisciplinary advisory board. The objective of the initiative is to produce interdisciplinary policy, people, and programs to address the growing cyber challenges. To achieve this, the initiative will 1) *Develop a Cyber Policy Master and certificate programs* 2) *Produce cyber policy-relevant research focused on interdisciplinary*

understanding and solutions 3) Create real word opportunities for students and practitioners 4) Host events to promote the USC's Cyber policy initiatives and other national cyber policy initiatives.

I. Developing a Cyber Policy Master's and certificate programs

- Create integrated cyber policy degree and certification program options for students in the Policy, Engineering, Law, Business, and communications schools.
- Explore other interdisciplinary cyber degree programs

II. Produce cyber policy-relevant research focused on interdisciplinary understanding and solutions to cyber issues - possible areas of research:

- Providing cybersecurity as a public service
- Economic, social, and physical cyber resilience
- Public - Private information sharing challenges
- Public - Private Partnerships
- Cyber risk perception and translating risk to decision makers and the public
- Entertainment and media cyber/tech perception

III. Create real word opportunities for students and practitioners

- City of Los Angeles Mayor's Office, Cyber Policy Fellowship (govt focused)
- Los Angeles Cyber Lab, Cyber Policy Fellowships (public-private focused)
- Capstone and practicum cyber projects
- Workshops for the community
- Local government workshops and table tops
- Partnerships with LA's entertainment and media industry

IV. Host events to promote the USC's Cyber policy initiatives and other national cyber policy initiatives.

- Co- host an annual summit with the City of Los Angeles focused on Cyber policy and collaboration
- Host National workshops/events for highlighting specific policy issues (ex. elections, risk perception, information sharing, translating etc.)

University of California at Los Angeles (UCLA) Extension is a non-degree conferring organization offering courses for those seeking to learn without gaining credit hours or participating in a formal degree earning program. UCLA Extension is a popular way for professionals to gain knowledge without the rigors and commitment of advanced academic programs. The courses are open to all levels of learners. LACL engaged UCLA Extension to discuss the creation of cybersecurity programs and courses. UCLA Extension was open to discussing the creation of courses if the LACL had content and course

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

curriculums to propose. UCLA Extension is interested in helping fill the skills gap among the cybersecurity workforce. The timeline for UCLA Extension to move through the course creation and certification is about 18 months. LACL did not have content or the capacity to develop courses within the pilot period. LACL abandoned this effort since many other cybersecurity higher education programs exist both within the greater Los Angeles area and online. Our efforts and resources were better spent on developing the TISP.

On **July 24th**, the Outreach Director spoke about the LACL and the Security Summit at the UCLA Bruins Alumni Professional Organization.

LACL cohosted a community event in partnership with the University of California Los Angeles (UCLA) Burkle Center for International Relations; *“How Hackers, Laws, Cybersecurity and Regulators Connect in a Connected World”*.

The LACL sought to engage academic partners in a variety of ways. The Executive provided thoughtful and engaging discussion on the collective cyber defense of our community and nation. The event had over 100 attendees and was held in conjunction with the University of California Irvine Cybersecurity Policy & Research Institute.

Pepperdine University - Graziadio Business School (GBS) is an emerging leader among business schools in California. GBS hosted the LACL as part of the 2019 Cybersecure SoCal event in October 2019. During this event the LACL discovered that business graduate school students and alumni represent a unique subgroup of the business community, with their own networks and events catered to meeting their business needs. LACL presented to the group and posted information from the event via linked-in which saw the greatest number of interactions for any LACL related post during the pilot period. LACL concluded that previous efforts to connect with academic partners in engineering, information, and computer science departments while important, left out a major portion of business professionals from the business schools and other programs such as public policy and criminal justice. From this event, the LACL gained support from the Pepperdine University CISO and added the university to its Advisory Board.

LACL presented at the Pepperdine University, Graziadio Business School event in association with SecureTheVillage; the event connected with CISOs and tech professionals during Cybersecurity Awareness Month. *Pepperdine was added to the LACL’s Advisory Board expanding its partnership with the ISAO.*

California State Polytechnic University, Pomona (Cal Poly) is an undergraduate university focused on hands-on learning. The unique focus of Cal Poly led to the LACL’s discovery of their student led security operations center (SOC). The Student SOC is part of the university’s College of Sciences and is in its infancy and was initially funded by Northrop Gruman. LACL attended the school’s technology fair and offered the TISP to the Student SOC at no cost, in order to fill a gap in their security tool set. Cal Poly gained access to the TISP four months later. Currently, the LACL is partnering with their faculty to identify opportunities to promote their Student SOC program. LACL intends to help Cal Poly establish a

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

cadre of cyber analyst students who will interact with TISP data and provide reports back to the LACL TISP community based upon the members shared information. Cal Poly is one of the newest members of the LACL Advisory Board.

Cyber Work Force Development

Develop hands-on cyber work force development programs in collaboration with academia.

Trainings – Types

The LACL Program Director led the fellowship program; they reviewed over 60 resumes and offered eight interviews of which four were accepted. Two interviewees were selected to replace the existing fellows and will begin in August and September; the fellowships are sponsored by City National Bank.

Outreach for the LACL was significant during the month of August 2019. The LACL spoke at local business leader forums and conferences, held an SLTT meeting, hosted several speaker series discussions, and hosted a hands-on analyst training with the National Cyber Forensics Training Agency (NCFTA). These events were successful in bringing many new connections to the LACL. The intent was to drive interest towards the Security Summit in September and increase information sharing through our daily threat report.

The darkweb training event received positive feedback and interest. LACL raised its social media profile through this event because the training was free to the public. The training increased participant's knowledge and awareness of threats. The LACL was able to connect with Sony threat researchers and build a dialog for future potential collaboration. The training had 33 registrants and 20 attendees for the 2.5-day sessions. These training sessions are a positive way of engaging the community because it allows peers to meet, learn, and interact with the LACL.

LACL held 4 one-hour training sessions throughout the two-day event and received the greatest interest, at least two sessions were standing room only. The training sessions were included in the event at no additional cost; training topics included 1) Wireshark, 2) Cyber Analyst Incident/Information management, 3) Data breach incident tabletop exercise, 4) Red Team Hacking

and one other additional analyst focused topic. ISSA offered CPEs for attending the summit.

Connecting The Community

September 17-18, 2019 - Training Agenda

Time	Training Topic	Presenter
9/17 - 2:00 Santa Monica D	Deep Packet Analysis with Wireshark and Tshark Part #1	Candan Bolukbas, NormShield In this meetup we used Wireshark to decrypt HTTPS streams, reconstruct audio streams and analyze sophisticated attacks. We also used tshark to analyze pcap file and extract field to process with command line tools. Please make sure that you have Wireshark and Tshark installed.
9/17 - 3:00 Santa Monica D	IT Risk in Motion Tabletop Exercise	Robert Kang, Loyola University & Special Guests Crisis response in a major cyber breach takes planning and training; get the full effect of what are the best practices and also the things not to do during this role-playing session.
9/18 - 10:00 Santa Monica D	Red Team Hacking	Dioly Alexandre, BlackShield The most successful teams have to know how they are being attacked. Thinking like a hacker is only half of the equation; learn the general methodology and explore concepts in tools which make your job easier.
9/18 - 2:00 Santa Monica D	Operationalizing Intelligence from Sharing Communities	Patrick Coughlin, TruStar Sharing communities like the LA Cyber Lab provide critical connective tissue for exchanging intelligence across enterprises. But they come in many different forms and the data is often unstructured and orthogonal to existing security workflows. In this session, we'll present the common challenges associated with operationalizing intelligence from different types of sharing communities and we'll share some technical tools and tips for how to make the most of your sharing community intelligence.

The Cyber Lab hosted a day long training with CISCO Security for students, analysts, researchers, and cybersecurity professionals. There were 28 attendees who learned about network security and participated in a capture the flag event. Both SLTT and private sectors were among the attendees.

Partners – STV, CISCO, NormShield, BlackShield, etc.

Speakers Series, Summit, Hands-on

LACL Sustainability & Future Recommendations

REGIONAL CYBER ISAO PILOT PROGRAM

CISA have identified threat sharing as essential to protecting critical infrastructure and furthering national cybersecurity. Federal agencies and national sector-based information sharing centers have led threat sharing efforts through a top down approach for years. However, the Ransomware epidemic highlights the need for a new level of threat sharing between federal, state, and local governments, as well as the private sector. The LACL and City of Los Angeles are now advocating for state and local governments to lead local efforts to complement existing federal and national threat sharing by establishing regional interconnected ISAO.

This pilot program lays the foundation for a nationwide and locally implemented threat sharing network by establishing 3-4 regional Information Sharing Analysis Organizations (ISAO). Specifically, the pilot will export the LACL ISAO model and leverage the LACL's TISP to connect regions. Many regions are working towards a coordinated approach, and this will build on those efforts, promote local innovation, and ensure national interoperability. To implement this, LACL will provide pilots sites with a regional coordinator, a sharing platform, and ongoing support.

Connecting the Community

Through the *Connecting the Community* initiative LACL has become a foundational member of the Los Angeles cybersecurity ecosystem. The LACL advisory board includes over 30 private sector partners and the County of Los Angeles. In January 2020, the City of Los Angeles, LACL, and the other local municipalities partner to establish the Regional Cyber Coordination Group (RCCG). The RCCG provides local governments with cybersecurity resources, knowledge, and works towards future collaboration.

Joint Cyber Intelligence Integration Task Force



In February 2020, the LACL and the Joint Regional Intelligence Center partnered to form the Joint Cyber Intelligence Integration Task Force (JCIITF). The JCIITF's innovative approach brings together the Greater Los Angeles Region's intelligence partners to integrate and improve cyber threat analysis and information sharing. The JCIITF works closely with the RCCG, California Cybersecurity Integration Center (CAL-CSIC), CISA, and the FBI.

CONTINUING THE PARTNERSHIP AND EXPANDING THE MODEL

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

The LACL now seeks to continue its partnerships with CISA to build on these successes and further develop the LACL as model IS-ISAO. Specifically, funding will allow LACL to stay a key player in the region's security by continuing to expand private sector TISP participation, workforce development, and be active in the RCCG and JCIITF. Further, funding will allow LACL to support the City of Los Angeles as it establishes threat sharing partnerships with other major metropolitan cities.

In addition to regional initiatives, LACL is also looking to export the ISAO model and lay foundation for a national threat sharing network by establishing 3-4 regional ISAO. The pilot program will promote local relationships, regional innovation, and ensure national interoperability. Specifically, LACL will provide pilot sites with a regional coordinator, 15-30 sharing platform accounts, and ongoing support. Cities of San Antonio, San Francisco, and the Cyber Resilient Massachusetts Working Group have all expressed interest in becoming pilot sites.

LACL suggests sustainment funding for one year: \$1.1M; two years: \$2.1M.

Funding to the LACL will support existing and expanding capabilities. A high-level overview of LACL:

Threat Intelligence Sharing Platform (TISP)

- Expand participation and continue to provide the service free for the private and public sectors.
- Threat Analyst team to analyze and refine TISP partner data to produce improve TISP data and produce in depth intelligence products and timely advisories.
- Additional licenses for new TISP members

Regional ISAO Pilots - Extending the Cyber Lab Network

- Establish pilot program to build a nationwide threat sharing network by establishing 3-4 regional ISAO.
- Provide pilots sites with a regional coordinator, sharing platform accounts, and ongoing support.

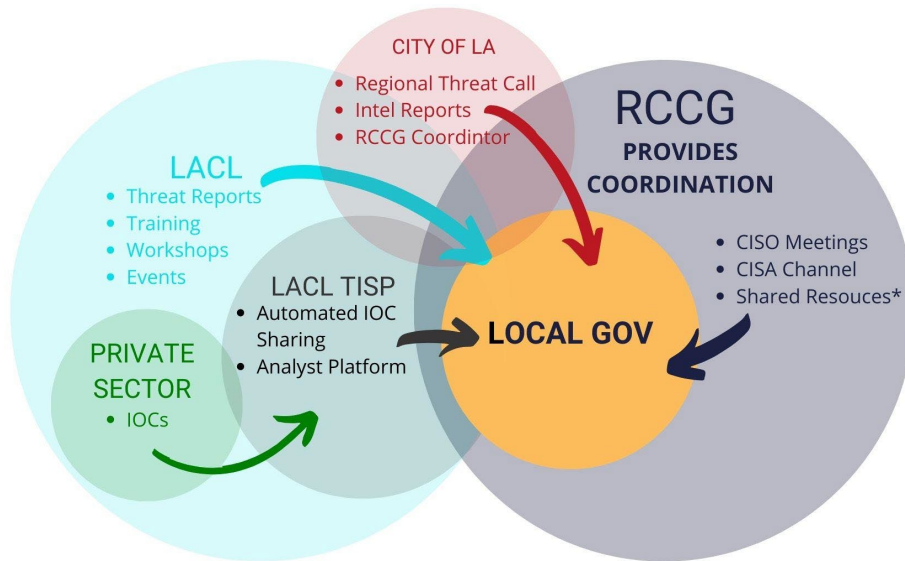
Workforce Development, Education, and Events

- LACL Academy - provide advanced training opportunities to tech professionals
- Expand training opportunities - connect tech community and underserved workforce populations in the region
- Workshops for small and medium business - town hall style meet-ups which provide practical application of security

Regional and National Cybersecurity

- Continue to be a key member in the RCCG and JCIITF, supporting the regions SLTT community with threat sharing, training, and other support.

- Build joint threat sharing partnerships with the City of Los Angeles and major US cities



Center of Cyber Excellence for Information Sharing

- Establish a Center of Cyber Excellence with Academic partners
- Study and analyze information sharing to understand barriers, benefits, and best practices.
- Make policy recommendations to local, state, and federal lawmakers to improve private and public sector information sharing

Regional ISAO Pilot Overview

LACL and the City of Los Angeles are now looking to export this model and connect regions through a single sharing platform. LACL will provide¹⁷ 3-4 sites with:

- The Threat Intelligence Sharing Platform
- Regional Coordinator/Analyst
- Regional advising, support, and assistance

Regional ISAO Objectives

Establishment

- Establish a regional ISAO by integrating the function into an existing organization or establishing a new organization
- Integrate the ISAO into existing threat sharing and regional cybersecurity efforts

¹⁷ Depends on federal funding

Threat Sharing

- Provide public and private sector partners with timely and relevant cyber threat information through the TISP, briefings, advisories, and reports
- Build local relationships and capacity to facilitate threat sharing with the public and private partners
- Identify threat sharing barriers and best practices
- Share threat information with LACL, other pilot ISAOs, and federal partners through the TISP, briefings, and reports.

Regional Cyber Support

- Assist SLTT governments
- Other innovative initiatives as decided by pilot sites

Pilot Principles

- **Local Implementation:** Locally implemented ISAOs are in the best position to build trust and relationships that are necessary for threat sharing. Furthermore, local authorities will know the best way to integrate ISAOs into the existing cybersecurity ecosystems. For example, the ISAO function could be integrated into an existing SLTT organization, such as a major city, fusion center, state agency, or a nonprofit. Alternatively, pilot partners could follow the LACL approach and create a public-private partnership.
- **Regional Innovation:** Pilot sites would be regional experiments in ISAO integration, relationship building, partnership collaboration, threat sharing and new initiatives. Success and failure can be documented, and best practices can be developed. Cyber threat sharing is still in its infancy, and experimentation and innovation will drive progress.
- **National Network:** Pilot sites would be directly connected to LACL through the TISP. The goal is a national network of ISAOs, allowing for rapid threat sharing. This regional ISAO will also provide federal partners with an established network.



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- **Long Term Interoperability:** IASOs will facilitate technical connections and formal relationships between major metropolitan areas. Building these connections and relationships now will ensure long term threat sharing interoperability. As regions improve their ability and infrastructure to identify and share indicators of compromise, its important regions use common methods and tools for communicating

LACL Conclusions

The LACL has made great progress in the fulfillment of its Mission and Vision. However, much work remains, and it is critical to the continued success of the LACL to have a fully engaged team of staff, volunteers, Advisory Board Members and the business community that are willing to creatively engage the private sector and dedicate the needed time and resources. The threat of Cyber-attacks is all too real and becomes more lethal every day making the Mission of the LACL truly important to a free society and the maintenance of our way of life.

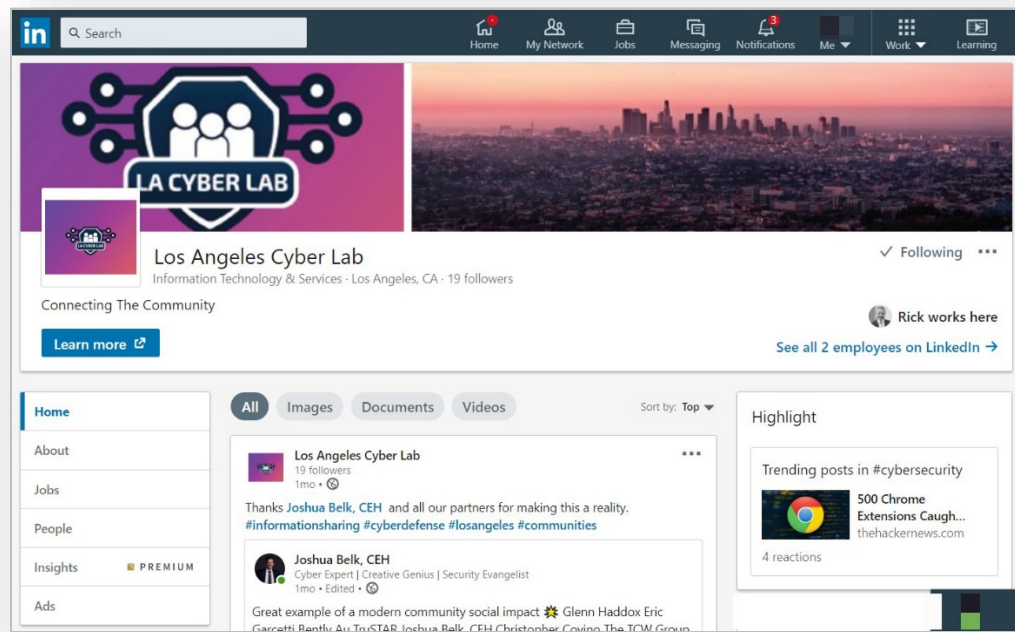
Future sustainability of the LACL

The project is tied too close to the City of Los Angeles in that when people hear about the LACL, they think this is a city managed initiative. The City of Los Angeles is a municipality and doesn't treat the LACL as a non-profit business which has had a negative impact on relationships with the private sector. The perception by businesses is that the LACL is part of the City which implies they are being requested to share information with a local government.

Businesses do not prioritize the LACL and therefore while they have expressed interest in sharing they move slowly, often requiring months of engagement before moving forward with real threat intelligence sharing.

Participating in the LACL is not properly incentivized. Businesses and local governments do not perceive a real value from their participation. Despite LACL efforts to explain and express the benefits of sharing information the businesses struggle to define the benefit they might derive from participation. Participating to benefit the community is altruistic and does not necessarily resonate as a motivation for businesses to allocate resources to provide information to the LACL when resources are already limited.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Appendix A – Financial Accounting

A detailed listing of the financial activities of the pilot project are recorded via FFR submissions to GrantSolutions.Gov. LACL maintains accounting records for the pilot project which have been provided to CISA and are available upon request. Below is a high-level spending breakdown of the pilot project.

Annual Budget Internet - Security Information Sharing and Analysis Organization (IS-ISAO) Pilot <i>Project Period: 10/1/2018-3/31/2020</i>				
APPR CODE	Cost Category <i>Select from Dropdown</i>	IS ISAO Grant Objective(s) <i>Select from Dropdown</i>	Item	Total Budgeted Cost
ISAO-C-0001	Travel	Bi-Lateral Cybersecurity Information Sharing	MS-ISAC Annual Meeting - 28 April - 1 May Denver, CO	\$ 3,420.82
ISAO-C-0002	Travel	Bi-Lateral Cybersecurity Information Sharing	ISAO Standards Organization International Information Sharing Conference (IISC) - 20-23 August, 2019, San Antonio, TX	\$ 2,464.08
ISAO-C-0003	Travel	Bi-Lateral Cybersecurity Information Sharing	National Homeland Security Conference - June 17-20, 2019, Phoenix, AZ	\$ 2,636.31
ISAO-C-0004	Travel	Bi-Lateral Cybersecurity Information Sharing	ISSA CISO Forum and Women in Cyber Conference	\$ 1,956.54
ISAO-C-0005	Travel	Bi-Lateral Cybersecurity Information Sharing	FEMA Region IX Cyber Workshop Series - July 9, 2019, Mountain View, CA	\$ 306.84
ISAO-C-0006	Travel	Identify Barriers to Information Sharing	LACL Security Summit 2019; Sept 17-18, 2019, Los Angeles, CA	\$ 2,565.41
ISAO-C-0007	Travel	Bi-Lateral Cybersecurity Information Sharing	RSACON 2020, Feb 24-28, 2020, San Francisco, CA	\$ 8,000.00
Total				\$ 21,350.00
ISAO-D-0001	Equipment	Establish Fully Functional IS-ISAO	Smart Board Screens or Situational Awareness Monitors (x2)	\$ 23,000.00
ISAO-D-0002	Equipment	Establish Fully Functional IS-ISAO	Other Situational Awareness Equipment	\$ -
ISAO-D-0003	Equipment	Develop Documentation	Laptop or Desktop Computer Suite (x4)	\$ 12,000.00
ISAO-D-0004	Equipment	Establish Fully Functional IS-ISAO	Office Furniture	\$ 12,242.66
Total				\$ 47,242.66
ISAO-E-0001	Supplies	Establish Fully Functional IS-ISAO	Office Supplies	\$ 2,000.00
Total				\$ 2,000.00
ISAO-F-0001	Contractual	Bi-Lateral Cybersecurity Information Sharing	Threat Intelligence, Analysis, and Sharing Platform (TIASP) - Hardware, Software, Labor, Etc.	\$ 1,200,000.00
ISAO-F-0002	Contractual	Bi-Lateral Cybersecurity Information Sharing	Threat Intelligence, Analysis, and Sharing Platform (TIASP) - Support & Maintenance	\$ 634,290.00
ISAO-F-0003	Contractual	Establish Fully Functional IS-ISAO	Executive Director (ED) / Chief Development Officer (CDO)	\$ 173,838.28

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

ISAO-F-0004	Contractual	Identify Barriers to Information Sharing	Policy Director	\$	36,000.00
ISAO-F-0005	Contractual	Identify Barriers to Information Sharing	Program Director	\$	91,400.00
ISAO-F-0006	Contractual	Cyber Work Force Development	Outreach Director	\$	26,710.00
ISAO-F-0007	Contractual	Establish Fully Functional IS-ISAO	Cyber Threat Analyst	\$	247,987.06
ISAO-F-0008	Contractual	Establish Fully Functional IS-ISAO	Data Scientist / Visualization Analyst	\$	39,045.00
ISAO-F-0009	Contractual	Establish Fully Functional IS-ISAO	Grant Management & Administration	\$	150,000.00
Total				\$	2,599,270.34
ISAO-H-0001	Other Direct Costs	Establish Fully Functional IS-ISAO	LACL Website	\$	18,944.67
ISAO-H-0002	Other Direct Costs	Bi-Lateral Cybersecurity Information Sharing	Situational Awareness Room Events	\$	19,000.00
ISAO-H-0003	Other Direct Costs	Bi-Lateral Cybersecurity Information Sharing	LACL Summit	\$	147,230.33
ISAO-H-0004	Other Direct Costs	Work with Academic Partners	Conference/Outreach Events	\$	30,000.00
ISAO-H-0005	Other Direct Costs	Establish Fully Functional IS-ISAO	Media Production (Photo/Video)	\$	56,825.00
ISAO-H-0006	Other Direct Costs	Establish Fully Functional IS-ISAO	Marketing - LACL Continual	\$	21,000.00
ISAO-H-0007	Other Direct Costs	Cyber Work Force Development	Marketing - Events, Outreach, and Conferences	\$	30,000.00
Total				\$	323,000.00
Grand Total				\$	2,992,863.00

Appendix B – Outreach Activities

The following is a list of the outreach activities conducted during the pilot project.

Training

Oct 2018

Nov 2018

Dec 2018

Jan

Feb

Mar

Apr – MS-ISAC

May

On **May 30th**, the Outreach Director participated in the SecureTheVillage Leadership Council, attended by 41 local professionals, where he discussed the LACL key initiatives, the current status of the threat sharing portal and upcoming events.

On **June 4th**, the Executive Director and Mr. Jacob Finn attended the Southern California CISO Summit. The two engaged attendees and participated in various presentations obtaining several new commitments from SLTT and private sector organizations to become members of the LACL with the potential for partnership inclusion in the current bidirectional information sharing initiative.

On **June 6th**, **June 9th**, **June 11th**, and **June 14th**, the Outreach Director participated in networking events and attended two webinars to evaluate current trends in the security industry and to identify potential subjects for future LACL events.

On **June 13th**, the LACL staff completed a web application bootcamp with The Rosslyn Group. The teams explored the user experience of the mobile application and developed the framework for the user interface. The mobile app will be the primary means of interaction with SMB and the community.

On **June 17th**, the LACL attended the National Homeland Security Conference, Phoenix, AZ to facilitate further adoption and increased participation amongst SLTT.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

On **July 24th**, the Outreach Director spoke about the LACL and the Security Summit at the UCLA Bruins Alumni Professional Organization.

On **July 31st**, the LALC is hosted a Situational Awareness briefing for members to update them on the pending launch of the mobile phishing application and the threat intelligence sharing platform. There were 27 attendees and from the group breakout sessions the following feedback was provided by the members: 1) LACL TISP data should be non-attributable; 2) Security Summit outreach should include connections with the LA Chamber of Commerce and upcoming SLTT events.

On **August 7th**, the LACL hosted an SLTT event at the City of LA EOC to discuss participation as part of the LACL threat sharing initiative. The cities of Burbank, Lynwood, and Monrovia were represented. Each of these cities expressed interest in membership but none were in a position to become sharing partners.

On **August 7th**, the LACL co-hosted a speaker's series panel discussion *Cyber Risk: The Cyber Security and Cyber Privacy Threat Landscape*. Over 28 professionals attended the event.

On **August 9th**, the LACL Executive Director spoke at the SecureTheVillage monthly leaders in security business breakfast.

On **August 21st & 22nd**, the LACL Executive Director presented *Anatomy of an IOC and Information Sharing Changes* at the annual Information Sharing Conference for ISAOs.

On **August 22nd**, the LACL co-hosted a cyber resiliency speaker's discussion with Homeland Security Advisors Council (HSAC), an Advisory Board member of the LACL, which was attended by 95 public sector and non-profit professional.

On **August 27-28th**, the LALC is hosted a hands-on analyst training workshop *Accessing The Darkweb* with NCFTA.

On **August 28th**, the LACL is cohosted a speaker's series panel discussion *Securing The Human: Growing the Community*.

On **September 16th**, LACL hosted CISA for a site visit.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

On **September 17th & 18th**, LACL Security Summit 2019: LACL launched the TISP and mobile app to increase information sharing and public-private sector partnerships on 9/17 & 9/18; over 350 attendees from SLTT, academia, and business communities participated. There were 527 registered attendees, we have confirmed 40 speakers, 5 moderators and Mayor of Los Angeles, Eric Garcetti provided the welcome address and keynote. Themes for the event include the following categories: aviation security panel, privacy and law discussions, space security panel, cybersecurity risk and best practices along with at least one panel focused on women in tech. CISA Region 9 representative moderated several panels and the LACL Executive Director provided multiple presentations all focused on information sharing via the TISP or mobile app. The overall event was very successful as it greatly increased the awareness of the LACL in the community and provided a positive experience for all. The event began late on the first day due to street closures and traffic associated with a POTUS visit at a nearby venue.



On **October 17th**, the LACL presented at the Pepperdine Cybersecure SoCal 2019 conference.

On **October 23rd**, the LACL presented to local SLTT leaders at the 2019 Maritime Cybersecurity Symposium.

On **October 30th**, the LACL attended a local Small Business conference to engage companies in information sharing.

On **November 21st**, the LACL cohosted a community event "How Hackers, Laws, Cybersecurity and Regulators Connect in a Connected World".

On **December 4th**, the LACL participated in the Media-Entertainment ISAC Summit.

On **December 6th**, the LACL participated in the Southern California ISACA/CSA Holiday Mixer.

On **December 11th**, the LACL participated in the Southern California CISO Executive Summit.

On **January 15th**, the LACL

Webinars:

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- Hosted Technical Information Sharing & Challenges Webinar
- Participated in 2019 LA City Club Tech Conference
- Participated in the Cyber Risk Management Forum
- Attended The California Consumer Privacy Act Webinar (CCPA)
- Attended The Power of AI to Disrupt Security Ops
- Attended the CISA Infrastructure Security and Resilience Forum in Irwindale, CA
- Attended Cyber Risk Management

Events:

- LACL Security Summit 2019 – Connecting the Community – GO LOUD event for the launch of the mobile app and information sharing community related event
- Hosted hands-on analyst training workshop *Accessing The Darkweb*
- Hosted Cybersecurity and Cyber Privacy Legal Threat Landscape
- Hosted *Cyber Risk: The Cyber Security and Cyber Privacy Threat Landscape*
- Cohosting a speaker's series panel discussion *Securing The Human: Growing the Community*
- Cohosting a Cybersecurity Leaders Forum with HSA Council
- Presented *Anatomy of an IOC* at the annual Information Sharing Conference for ISAOs
- Presented *LACL Mobile Phishing App* at the annual Information Sharing Conference for ISAOs
- Presented at the UCLA Alumni - Silicon Beach Chapter
- Presented at the Business Leaders in Security
- Presented at the Tripartite Security Forum in Auckland, New Zealand
- Presented at the SecureTheVillage Leadership Council
- Presented at the Content Privacy Summit
- Participated at Cybersecure LA 2018
- Participated in DataConLA 2019
- Attended MS-ISAC Conference
- Attended National Homeland Security Conference
- Attended ISSA CISO Conference & Cyber Security Woman of the Year 2019 Awards
- Attended InfraGuard Pacific Region Information Sharing Initiative (ISI)
- Attended the Managed Security Services Forum

Ongoing Outreach Efforts

- American Business Bank
- Bogaard International Group
- British-American Business Council
- California State University, Dominguez Hills
- California State University, Polytech Pomona
- Citadel Group
- Crucyble

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

- Cybertegic
- DataConLA
- FBI Science and Technology
- First Republic Bank
- Forcepoint
- GM, Ecosystem Strategy & Business Development,
- Herbalife
- Intel
- ISSA
- JASK
- LA Chamber of Commerce
- LBW Insurance & Financial Services, Inc
- Obsidian Security
- Pacific City Bank
- Polsinelli Law Firm, Century City
- Resecurity
- Response Software
- San Bernardino County
- SkylinkTV
- TruStar
- UC Berkeley
- UCLA Extension
- USC Information Science Institute

Appendix C – Pilot Project Participants

This section documents support from both organizations and individuals who contributed to the LACL. The following is a list of the key participants who worked on the pilot project.

Name	Project Role	Contributions to Project
Joshua Belk	Executive Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led LACL daily efforts and pilot platform project. He provided overall management and direction to the information sharing initiative.
Christopher Covino	Project Lead & Grant Representative; Mayor's Office of Public Safety, City of Los Angeles	Managed the grant, was a public advocate for the LACL pilot platform and information sharing.
Magdalena Kenon	Program Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led business operations and finance for the grant.
Daniel Lee	Senior Cyber Analyst, Los Angeles Cyber Lab, Inc.	Collaborated with the City of Los Angeles analysts in threat intelligence information sharing.
Kian Rahimnejad	Fellow, Los Angeles Cyber Lab, Inc.	Researched information used in promotional materials and created content to support the pilot project.
Jasmine Vu	Fellow, Los Angeles Cyber Lab, Inc.	Facilitated membership meetings and coordinated events in support of the pilot project.
Ariana Kim	Fellow, Los Angeles Cyber Lab, Inc.	Researched information used in promotional materials and created content to support the pilot project.
Jens Bechmann	Outreach Director, Los Angeles Cyber Lab, Inc. (Independent Contractor)	Led outreach to community and business partners for grant initiatives.
Robert Velsaco	Policy Director, Los Angeles Cyber Lab, Inc. (OPSEC360, LLC)	Led technical teams and managed vendors to provide information sharing products supporting the grant.
Haroon Azar	The Rosslyn Group	Led mobile phishing app coordination and strategic engagement for the LACL's business email compromise initiatives.
Imran Chaudhari	The Rosslyn Group	Technical lead for development of the mobile phishing application (aka LACL app).
Ahmed Salem	The Rosslyn Group	Technical engineer of the mobile phishing app and API integration.
Kevin Albano	IBM	IRIS and analytics point of contact for threat analysis for IBM.
Patrick Coughlin	TruSTAR	Cofounder of TruSTAR, led project development and integration with LACL.
Chris Godfrey	TruSTAR	Primary client engagement for the threat intelligence platform to the LACL. Facilitates all requirements for the TruSTAR API and platform.
Eve LaDue	Mayor's Office of Public Safety, City of Los Angeles	Procurement and contract specialist for LACL's cyber threat information sharing RFP.
Carlos Carrillo	IBM	IBM point of contact, coordinates and manages IBM and TruSTAR teams. Is the primary point of contact for threat sharing for the LACL.
Stan Stahl	SecureTheVillage; Los Angeles Cyber Lab, Inc. Advisory Board Member	Participated in outreach efforts, marketing, and facilitated community involvement.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Ara Aslanian	InverseLogic; Los Angeles Cyber Lab, Inc. Advisory Board Member	Participated in outreach efforts, marketing, and facilitated community involvement.
Jayson Gibson	Phoenix Online Media (POM)	Owner of POM. Primary for the LACL's website and establishment of social media.
Michael Estrella	Avelane Road	Owner of Avelane Road, primary consultant for video and multimedia production of LACL video series.
Jayson Garcia	TruSTAR	Primary client engagement for the threat intelligence platform to the LACL. Facilitates all requirements for the TruSTAR API and platform.
Lena Hwang	Mayor's Office of Public Safety, City of Los Angeles	Accounting and finance approver.
Miho Yoshimura	Mayor's Office of Public Safety, City of Los Angeles	Accounting and finance reviewer.
Neeraj Bhatnagar	Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Reuben Wilson	Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Jeffrey Gorell	Deputy Mayor for Homeland Security and Public Safety – Mayor's Office of Public Safety, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Timothy Lee	Chief Information Security Officer, City of Los Angeles	Los Angeles Cyber Lab Board of Directors
Ahmad Ishaq	ByteCubed	Los Angeles Cyber Lab Board of Directors
Rick Orloff	CSO Advisors	Los Angeles Cyber Lab Board of Directors
Bently Au	Chief Information Security Officer, AEG	Los Angeles Cyber Lab Board of Directors
Glenn Haddox	President, Los Angeles Cyber Lab, Inc.; Chief Information Security Officer, Southern California Edison	Provided thought leadership to the Executive Director.
Karl Mattson	President, Los Angeles Cyber Lab, Inc.; Chief Information Security Officer, City National Bank	Provided thought leadership to the Executive Director.
Jacob Finn	Project Lead & Grant Representative; Mayor's Office of Public Safety, City of Los Angeles	Managed the grant, was a public advocate for the LACL pilot platform and information sharing.

The following is a list of organizations who provided support to the LACL during the pilot project.

Organization Name:	City of Los Angeles, local municipal government, is a member of the cyber lab advisory board.
Location of Organization:	https://www.lacity.org/
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided office space and logistics for LACL staff to conduct business.
X Facilities	Provided office space and conference rooms for meetings.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

X	Collaborative research	Conducted joint analyst research of indications of compromise and threat intelligence.
X	Personnel exchanges	Provided two part-time resources to facilitate LACL daily threat report activities, web support, and platform discussion.
Organization Name:		City National Bank, a Los Angeles based regional financial institution, is a member of the cyber lab advisory board.
Location of Organization:		https://cnbbank.bank
Partner's contribution to the project (identify one or more)		
X	Financial support	Provided \$10,00.00 in sponsorship for the Security Summit 2019.
X	In-kind support	Funded two part-time fellowship positions beginning February 2019 for one year.
X	Facilities	Provided conference rooms for board meetings and fellowship interviews.
	Collaborative research	
	Personnel exchanges	
Organization Name:		CISCO Systems, a Fortune 500 technology corporation, is a member of the cyber lab advisory board.
Location of Organization:		https://www.cisco.com/
Partner's contribution to the project (identify one or more)		
	Financial support	
X	In-kind support	Co-sponsored and provided two cyber defense hands-on training March 1 st , 2019 & January 28, 2020.
	Facilities	
	Collaborative research	
	Personnel exchanges	
Organization Name:		Resecurity, Inc., a cybersecurity solutions company providing darkweb monitoring.
Location of Organization:		
Partner's contribution to the project (identify one or more)		
X	Financial support	Provided \$6,000.00 in sponsorship at the Security Summit 2019.
	In-kind support	
	Facilities	
	Collaborative research	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Personnel exchanges	
Organization Name:	NormShield, Inc., a third party vendor security company providing security risk scorecards.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided cybersecurity training at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Silent Sector, a security consulting firm.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$500.00 in sponsorship at the Security Summit 2019.
In-kind support	
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Silent Storm Security, a security consulting firm.
Location of Organization:	
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$500.00 in sponsorship at the Security Summit 2019.
In-kind support	
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Working Scholars, a workforce development organization.
Location of Organization:	www.study.com
Partner's contribution to the project (identify one or more)	
X Financial support	Provided \$4,000.00 in sponsorship at the Security Summit 2019.
In-kind support	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	Fioressence, a beauty and wellness company.
Location of Organization:	www.fioressence.com
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided free products for attendees as a sponsor at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	
Organization Name:	OPSEC360, LLC, a security consulting firm, is a member of the cyber lab advisory board.
Location of Organization:	www.opsec360.com
Partner's contribution to the project (identify one or more)	
Financial support	
X In-kind support	Provided artwork and graphic design as a sponsor at the Security Summit 2019.
Facilities	
Collaborative research	
Personnel exchanges	

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Appendix D – CTI Sharing Partners

The following tables are the status of the public and private sector engagement for TISP CTI sharing.

Contact	DISCUSSION	ACCESS	SHARING
PHASE 0	PHASE I	PHASE II	PHASE III
<i>CAL OES (Cal-CSIC)</i>	<i>Cedar-Sinai Hospitals</i>	<i>AEG</i>	<i>Avery Dennison</i>
<i>Fox</i>	<i>City of San Diego</i>	<i>City National Bank</i>	<i>City of Los Angeles</i>
<i>City of Beverly Hills</i>	<i>County of Los Angeles</i>	<i>City of Atlanta</i>	<i>IBM</i>
<i>City of Phoenix</i>	<i>Dollar Shave Club</i>	<i>City of Boston</i>	<i>ME-ISAC</i>
<i>City of San Diego</i>	<i>Port of Long Beach</i>	<i>City of Burbank - DWP</i>	<i>InverseLogic</i>
<i>County of San Bernardino</i>	<i>Shepard-Mullin</i>	<i>City of Glendale</i>	
<i>JRIC Phoenix</i>	<i>Southern California Edison</i>	<i>City of Long Beach</i>	
<i>KPMG</i>		<i>City of Pasadena</i>	
<i>NASA JPL</i>		<i>City of Pasadena - DWP</i>	
<i>American Airlines</i>		<i>City of Riverside</i>	
<i>Riot Games</i>		<i>City of San Antonio</i>	
		<i>City of San Fernando</i>	
		<i>City of San Francisco</i>	
		<i>City of Santa Monica</i>	
		<i>City of Torrance</i>	
		<i>County of Los Angeles</i>	
		<i>FBI Cyberhood Watch LA</i>	
		<i>Hulu</i>	
		<i>iHerb LLC</i>	
		<i>OPSEC360</i>	
		<i>JRIC Los Angeles</i>	
		<i>Cal Poly Pomona</i>	

Phase	Organization	Notes	Industry	Initial Contact
PHASE 0 -	<i>CAL OES (Cal-CSIC)</i>	<i>Unknown</i>	<i>State</i>	<i>February</i>

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Contact				2019
PHASE 0 - Contact	Cal Poly Pomona	On Hold – February	Academia	April 2019
PHASE 0 - Contact	City of Beverly Hills	No Response Yet	Gov -Local	December 2019
PHASE 0 - Contact	City of Phoenix	Reconnect Jan 2020	Gov -Local	November 2019
PHASE 0 - Contact	City of San Diego	Pending Call 2nd call	Gov -Local	November 2019
PHASE 0 - Contact	County of San Bernardino	No Response	Gov - Local	August 2019
PHASE 0 - Contact	JRIC Phoenix	On Hold – February	Fusion	November 2019
PHASE 0 - Contact	KPMG	Pending Follow Up	Consulting	September 2019
PHASE 0 - Contact	NASA JPL	No Response Yet		December 2019
PHASE 0 - Contact	Riot Games	No Response Yet	Tech	June 2019
PHASE 0 - Contact	American Airlines	Initial Contact	Aerospace	February 2020
PHASE I - Discussion	Cedar-Sinai Hospitals	Pending Follow Up Call	Healthcare	March 2019
PHASE I - Discussion	City of San Diego	Follow up Required		December 2019
PHASE I - Discussion	County of Los Angeles	Pending Follow Up	Gov - Local	August 2019
PHASE I - Discussion	Dollar Shave Club	Pending Follow Up Call	Beauty	February 2019
PHASE I - Discussion	Port of Long Beach	Pending Follow Up	Transportation	June 2019
PHASE I - Discussion	Shepard-Mullin	Pending Technical Call	Law	July 2019
PHASE I - Discussion	Southern California Edison	On Hold Until 2020	Energy	March 2019
PHASE II Access	AEG	Pending Follow Up	Entertainment	February 2019
PHASE II Access	City National Bank	Pending Partner Update	Finance	February 2019
PHASE II	City of Atlanta	Phase III pending Tech	Gov - Local	December

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Access				2019
PHASE II Access	City of Boston	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of Burbank - DWP	Access Only - Tech Limitations	Energy	December 2019
PHASE II Access	City of Glendale	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of Long Beach	Access Only - Tech Limitations	Gov - Local	January 2020
PHASE II Access	City of Pasadena	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of Pasadena - DWP	Access Only - Tech Limitations	Energy	December 2019
PHASE II Access	City of Riverside	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	City of San Antonio	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of San Fernando	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of San Francisco	Phase III pending Tech	Gov - Local	January 2020
PHASE II Access	City of Santa Monica	On Hold Until 2020	Gov - Local	June 2019
PHASE II Access	City of Torrance	Access Only - Tech Limitations	Gov - Local	December 2019
PHASE II Access	County of Los Angeles	Phase III pending Tech	Gov - Local	December 2019
PHASE II Access	FBI Cyberhood Watch LA	For Intel	Gov - Federal	December 2019
PHASE II Access	Hulu	Pending Technical Call	Tech/Entertainment	July 2019
PHASE II Access	iHerb LLC	Call Scheduled	Food	November 2019
PHASE II Access	JRIC Los Angeles	For Intel only	Fusion	October 2019
PHASE II Access	LA 2028 -Olympic Organizer	Phase III pending Tech	non profit	January 2020
PHASE II Access	LA Community College District	Phase III pending Tech	Education	January 2020
PHASE II Access	LA Metro	Phase III pending	Transportatio	December

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Access			<i>n</i>	<i>2019</i>
PHASE II Access	<i>LA Unified School District</i>	<i>Pending Technical Call</i>	<i>Gov - Local</i>	<i>November 2019</i>
PHASE II Access	<i>Quibi</i>	<i>Verify Technology</i>	<i>Tech</i>	<i>December 2019</i>
PHASE II Access	<i>TCW</i>	<i>Tech Follow Up</i>	<i>Tech</i>	<i>October 2019</i>
PHASE II Access	<i>OPSEC360</i>	<i>Tech Follow Up</i>	<i>Tech</i>	<i>January 2020</i>
PHASE II Access	<i>USCG Sector Los Angeles/Long Beach</i>	<i>For Intel only</i>		
PHASE III Sharing	<i>InverseLogic</i>	<i>Verify Technology</i>	<i>Tech</i>	<i>December 2019</i>
PHASE III Sharing	<i>Avery Dennison</i>	<i>Complete</i>	<i>Manufacturing</i>	<i>November 2019</i>
PHASE III Sharing	<i>City of Los Angeles</i>	<i>Complete - Includes LAWA, PoLA, LADWP</i>	<i>Gov -Local</i>	<i>February 2019</i>
PHASE III Sharing	<i>IBM</i>	<i>Complete</i>	<i>Tech</i>	<i>June 2019</i>
PHASE III Sharing	<i>ME-ISAC</i>	<i>Complete</i>	<i>ISAC</i>	<i>February 2019</i>
PHASE X	<i>CISCO</i>	<i>Not Interested</i>	<i>Tech</i>	<i>March 2019</i>

Appendix E – TISP Value Proposition

Threat Intelligence Sharing Platform (TISP) Value Proposition

CISA made a \$3M investment in the LACL pilot project to increase information sharing among the public and private sectors. Through the grant the LACL established a mechanism to enable organizations to easily share threat intelligence through crowdsourcing indicators of compromise (IOC) in a TISP. The TISP is intended to augment and not replace any existing TIP. The LACL utilizes the TruSTAR platform for its TISP; TruSTAR provides the aggregation of IOCs and related threat intelligence information which is shared within the community. Furthermore, the TISP provides users an easy to use interface (API access also) for enriching and analyzing threat information. The LACL threat sharing model comprises of the following components:

- A threat intelligence sharing platform (TruSTAR)
- Existing LACL IOC data
- OSINT data feeds
- Analytics
- Reports
- Partner IOC data
- Business Email Compromise data

The value of these individual components are outlined in the table below as well as the advantages to becoming a partner and sharing information to with the LACL community.

Partners: Are those entities (academic, public or private sectors) which share threat intelligence to the LACL TISP.

Members: Are those entities or individuals who receive (consume) threat intelligence from the LACL.

Threat Intelligence: Partners have access to 57 threat feeds; Members may receive 32 threat feeds.

LACL TISP saves organizations on average \$570K by providing access to an enterprise level tool and analyst vetted CTI.

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Product	Value	Cost	Partner	Member
TISP (TruStar)	TISP	\$200K	✓	
Existing LACL IOC Data	Over 24 months of vetted IOC data with contextualized information	\$250K	✓	
OSINT Data Feeds	<p>Consisting of 16 feeds which are analyzed, arranged, and ingested into the existing LACL IOC data feed; analysts work through these feeds to provide high fidelity IOCs with further enriching existing data (<i>partial list</i>):</p> <ul style="list-style-type: none"> • Abuse Ransomware • Abuse SSL IP Blacklist • Bambenek • Broadanalysis • CISA - AIS • EU-Cert • H-ISAC • Hail A TAXII • Hybrid Analysis Public • Infosecislands • Internet Storm Center • Malware bytes • NIST NVD • Packetstorm • Unit 42 • US-Cert 	\$320K	✓	✓
Analytics	IBM Incident Response Information System (IRIS) analysis of IOC data	\$100K	✓	
Reports	<p>IRIS Monthly Reports:</p> <p>Threat Activity (10)</p> <p>Malware Analysis (5)</p> <p>Threat Group (1)</p>	\$100K	✓	✓
Partner Data (IOC Enclave)	High fidelity IOCs contributed by partners into a single enclave.	\$250K	✓	✓

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Phishing Data (BEC Enclave)	Community provided data about potential phishing IOCs	\$75K		
Total Value of the LACL Information Sharing Model		\$1.295M	\$1.22M	\$570K

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Partner Received Threat Intelligence Feeds Included:

Feed Name	Enclave_id
a_de_pasquale	649b15c1-dfb8-408d-b359-0cd1411d14ef
Abuse Ransomware	170c3077-f502-4b1a-b8f7-7538f83a66c1
Abuse SSL IP Blacklist	00cbe17f-8d3c-4dd8-84ac-3c0c4e6a7c02
anand_himanshu	751511a8-3499-42b5-a6e5-acfece24bd33
asset_island_	34908b5d-2d3d-4582-8a42-aa6d4b2f003d
atindermann08	bef7dc37-8e50-498b-baea-1043585c74d1
Avman1995	0199dd32-575d-4361-8c14-d1c468816381
Bambenek	ed9d7459-dd90-414f-96ee-5e37f232cd18
Bauldini	9bfa800b-4a74-4be7-a09b-5724fb71ec5f
Broadanalysis	0e4443fc-2b50-4756-b5e0-4ea30030bcb3
Community	28177710-9cb8-aa2f-29e8-135c14365e80
DecayPotato	f83278e1-4f41-4602-8d3b-1e35d18f07b6
CISA-AIS	cabbfa67-afd7-4a0c-a20f-e51e25923629
Diemiurgo	63a16f2e-e163-456b-99dc-4b12ac1cd755
Dodge This Security	87753c77-44e8-4786-bc46-01608dc23a77
EU-CERT	e7f4907a-2909-48e8-9c2d-74ffc4b22e8c
FewAtoms	4a9891a5-0e65-41df-a0d1-9c77f17cd6ff
H-ISAC TLP Green & White Alerts	5392b0a7-32fb-4825-aac7-1e6c6d437de3
h3x2b	9b116216-a46b-472a-af44-c5b16ac4c9a8
Hail A TAXII	7819c8d1-2b7b-48ac-b127-c71d8e7de612
HazMalware	e6e48dcb-51cb-4911-9343-11f02ffe2bad
Hybrid Analysis Public Feed	2ecccdd-c740-4ad9-aa5c-82744cd1f6aa
IBM X-Force	c13392e3-8d5c-49bb-8a5b-bb55b41eb3b7
Infosecisland	eec779f5-7abc-48ea-ad19-4c5a5f8f5822
Internet Storm Center	eecdff2d-22ae-4e4a-b924-42da4e7ccd4b
issuemakerslab	d13bf951-6071-4ca3-811a-89378decff3f
James_inthe_box	5fefc6f4-57f4-47a6-8f23-b97ce83d2c32
JanOfficial	4355d90d-bd77-4612-9073-012b11a56e98
JROdriguezB	9adb22a9-417a-472f-9650-ba8f1f3a2849
JRoosen	645717ce-6c43-49b4-aaaa-b1cc642f764b
justmlwhunting	279f247e-39f7-4911-a2d3-a545095d1d7d
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb
LACL TISP	a28684aa-d047-4770-bac7-1c5a67f7dacb
MaelSecurity	9dcbb428-52d5-400c-bc62-cfba02376018
Mak Wana	c10226c8-21dd-463c-b4cd-b8e14983d248
malhunters	09a1512e-581c-4e02-abce-97ecf5469f13
Malware Traffic Analysis	e13e0b52-0977-4cf6-be37-3445865c9e8a
Malwarebytes	5d5d1eee-f65f-4fd9-a14b-43c597d9af9e
My Online Security	752d5f90-3281-455d-8162-d629db21f37e
NeonPrimetime	3a8c95e0-6689-4142-b3ab-2900e59429d7
NIST NVD	d2eec321-34bc-4db6-aa20-2ad0a52135fc
Packetstorm	d2cf82f0-5aba-4cf4-ba3b-fc990829b663

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

pancak3lullz	89eb5207-0965-4400-bb83-f5c3d6e2f881
PolarToffee	7504840b-79c9-4fa3-812c-026bc7068393
pollo290987 _(@_@)_/	74f32d63-33c6-4edb-8cb9-c3c2a86b80d1
ps66uk	f6205545-3c00-490e-bf77-cbae6afc997c
Racco42	ad45e7fe-db06-4628-809f-dded2e65344b
RealRalf9000	0978b56c-fdc7-4aaa-8d3a-2367196a144f
Ring0x0	1474353b-cbf8-450c-8c6b-e5973e073ab2
SaurabhSha15	588ca83f-91d4-462d-b781-f7a4505a619e
scsinusy	b5fe326e-1b9c-4cc1-9726-070b83c6acba
Sohn von Erde	9feb9831-2867-4d36-a7ad-466108affa65
Techhelplist	42eed79a-5a4e-48da-a412-190bf4a3acbc
Unit 42	11125bbd-ca70-4f16-bce2-7e361693ceb2
US-CERT	919879d7-88b3-4605-9464-b2a8fca5473a
VK_Intel	9d21c878-b914-41d3-9ad2-47a7c430fd9a
Zerophage	e83a4fa6-af05-417d-b13a-b18a5fc9b426

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Member Received Threat Intelligence Feeds Included:

Feed Name	Enclave_id
a_de_pasquale	649b15c1-dfb8-408d-b359-0cd1411d14ef
Abuse Ransomware	170c3077-f502-4b1a-b8f7-7538f83a66c1
Abuse SSL IP Blacklist	00cbe17f-8d3c-4dd8-84ac-3c0c4e6a7c02
Avman1995	0199dd32-575d-4361-8c14-d1c468816381
Bambenek	ed9d7459-dd90-414f-96ee-5e37f232cd18
Broadanalysis	0e4443fc-2b50-4756-b5e0-4ea30030bcb3
Community	28177710-9cb8-aa2f-29e8-135c14365e80
CISA-AIS	cabbfa67-afd7-4a0c-a20f-e51e25923629
EU-CERT	e7f4907a-2909-48e8-9c2d-74ffc4b22e8c
H-ISAC TLP Green & White Alerts	5392b0a7-32fb-4825-aac7-1e6c6d437de3
HazMalware	e6e48dcb-51cb-4911-9343-11f02ffe2bad
IBM X-Force	c13392e3-8d5c-49bb-8a5b-bb55b41eb3b7
Infosecisland	eec779f5-7abc-48ea-ad19-4c5a5f8f5822
Internet Storm Center	eecdff2d-22ae-4e4a-b924-42da4e7ccd4b
James_inthe_box	5fetc6f4-57f4-47a6-8f23-b97ce83d2c32
JanOfficial	4355d90d-bd77-4612-9073-012b11a56e98
JRoosen	645717ce-6c43-49b4-aaaa-b1cc642f764b
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb
LACL TISP	a28684aa-d047-4770-bac7-1c5a67f7dacb
Mak Wana	c10226c8-21dd-463c-b4cd-b8e14983d248
Malware Traffic Analysis	e13e0b52-0977-4cf6-be37-3445865c9e8a
Malwarebytes	5d5d1eee-f65f-4fd9-a14b-43c597d9af9e
NeonPrimetime	3a8c95e0-6689-4142-b3ab-2900e59429d7
pancak3lullz	89eb5207-0965-4400-bb83-f5c3d6e2f881
pollo290987 _(@_@)_/	74f32d63-33c6-4edb-8cb9-c3c2a86b80d1
ps66uk	f6205545-3c00-490e-bf77-cbae6afc997c
Ring0x0	1474353b-cbf8-450c-8c6b-e5973e073ab2
SaurabhSha15	588ca83f-91d4-462d-b781-f7a4505a619e
Techhelplist	42eed79a-5a4e-48da-a412-190bf4a3acbc
Unit 42	11125bbd-ca70-4f16-bce2-7e361693ceb2
US-CERT	919879d7-88b3-4605-9464-b2a8fca5473a
Zerophage	e83a4fa6-af05-417d-b13a-b18a5fc9b426

Appendix F – LACL In Publications & Media

Published Articles

- Ars Technica, [Los Angeles partnership launches platform to help people catch phishes](#) [Sean Gallagher] September 18, 2019
- Government Technology, [L.A., IBM Launch Threat Intelligence Platform for Businesses](#) [Lucas Ropek] September 18, 2019
- Inside Cybersecurity, [LACL set to unveil threat app aimed at bolstering small business cybersecurity](#) [Charlie Mitchell] September 17, 2019
- StateScoop, [LA Cyber Lab launches threat platform, mobile app for local businesses](#) [Ryan Johnston] September 17, 2019
- Politico, [Morning Cybersecurity 9/17/19](#) [Tim Starks] September 17, 2019

Self-Published Videos

Cyber Lab: Don't Get Phished, <https://www.youtube.com/watch?v=lr--tDWs2pc>, February 22, 2020; Protect yourself and your business from phishing attacks, download the LACL app today for the latest in protection from the those trying to steal your data and money. Don't become a victim, after downloading the app you will be able to forward suspicious emails to the LACL for review. You'll shortly receive a response indicating if your email was truly malicious or not. Some phishing emails don't contain malware but ask you to provide personal information in response...don't be fooled. Read carefully and follow your instincts.

LACL TISP Threat Sharing, <https://www.youtube.com/watch?v=Aplm5-04qZI>, January 15, 2020; The LACL Threat Intelligence Sharing Platform (TISP) allows members to collaborate by sharing threat intelligence to defend our community "Protection Through Partnership" The TISP is a free service available to public and private sector organizations who want to gain greater insight into their network environments.

Connecting The Community, <https://www.youtube.com/watch?v=5Krd6LkPuP4>, December 4, 2019; LACL Security Summit 2019 - Connecting The Community - helped usher in a new age in information sharing and partnerships between public and private sectors. LACL launched a mobile app and a Threat Intelligence Sharing Platform which connects businesses creating a collective cyber defense for the community. We become part of the change in the cyber ecosystem! Information is available at www.lacyberlab.org/toolsforlabusinesses.

LACL: About US, <https://www.youtube.com/watch?v=9cU4QdF4OZc>, October 28, 2019; Welcome to LACL! Learn about the latest in threat intelligence as we evolve the cyber ecosystem in the LA business community. Protection through Partnership.

Cyber Lab Mobile App: Protect Against Phishing, <https://www.youtube.com/watch?v=SfNKgsV0xY0>, October 3, 2019; Follow a local business owner as she protects herself and her business against phishing attacks. Download the LACL app today!

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

LACL Security Summit 2019, <https://www.youtube.com/watch?v=Q1CM24FFFjY>, July 17, 2019;
REGISTRATION IS OPEN FOR THE LACL SECURITY SUMMIT 2019!!! Join business leaders and security professionals in the Los Angeles greater area and beyond...See the latest trends in tech, engage with industry leaders, and be a part of the cyber ecosystem changes in phishing and information sharing from the LACL.

Appendix G – List of Known ISAOs/ISACs

ISAO/ISAC	Web Address
Advanced Cyber Security Center	www.acscenter.org
Arizona Cyber Threat Response Alliance	azinfragard.org/actra
Automotive ISAC	automotiveisac.com
Aviation ISAC	a-isac.com
California Cybersecurity Information Sharing Organization	https://www.californiatechnology.org/calciso
Center for Model Based Regulation	www.cmbreg.org
Columbus Collaboratory	ColumbusCollaboratory.com
Communications ISAC	https://www.cisa.gov/national-coordinating-center-communications
Cyber Houston	cyberhouston.org
Cyber Information Sharing and Collaboration Program	dhs.gov/ciscp
Cyber Resilience Institute	www.cyberresilienceinstitute.org
Cyber Threat Alliance	www.cyberthreatalliance.org
Cyber Warfare Range	azcwr.org
CyberHawaii	CyberHawaii.org
Cybersecurity Collaborative	cyberleadersunite.com
CyberUSA	cyberusa.us
CyberWyoming	www.madesafeinwyoming.org
Defense Industrial Base ISAC	www.dibisac.net
Defense Security Information Exchange	www.dsie.org
Downstream Natural Gas ISAC	dngisac.com
Electricity ISAC	eisac.com
Emergency Management and Response ISAC	www.usfa.fema.gov/operations/ops_cip_emr-isac.html
Energy Analytic Security Exchange	grfederation.org/ease
EnergySec	www.energysec.org
Faith-Based ISAO	faithbased-isao.org
Financial Services ISAC	fsisac.com
Fortify 24x7	www.fortify24x7.com
Geographically-Based Community ISAOs	gbcisaos.org
GICSR Global Situational Awareness Center	www.gicsr.org
Global Directors & Officers ISAO	global-do.org
Global Resilience Federation	www.GRFederation.org
Global Trafficking ISAO	TraffickingISAO.org
Health ISAC	h-isac.org
Healthcare Ready	www.healthcareready.org
HITRUST	hitrustalliance.net
Hospitality Technology Next Generation	www.htng.org

Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

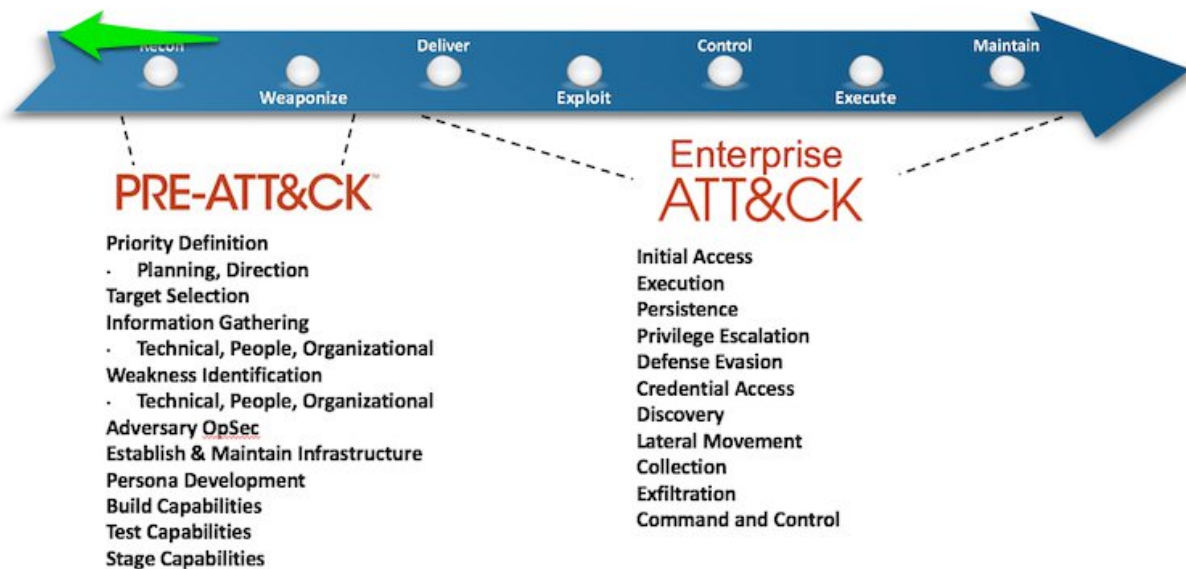
Houston Banking ISAO	HouBankISAO.org
Indiana ISAC	www.in.gov/isac
Information Technoogy ISAC	www.it-isac.org
InfraGard	www.infragardnational.org
InsuraShield	InsuraShield.net
International Association of Certified ISAOs	www.certifiedisao.org
IoT ISAO	iot-isao.org
Legal Services ISAO	https://grfederation.org/lis-isao
Los Angeles Cyber Lab	LACyberLab.org
Louisiana Business Emergency Operations Center	LABEOC.org
Maritime and Port Security ISAO	portsecure.org/about/
Maritime ISAC	www.maritimesecurity.org
Maryland ISAO	www.mdisao.org
Medical Device ISAO	www.medisao.com
Mid-Atlantic Cyber center	macc-isao.mitre.org
Multi-State ISAC	www.cisecurity.org/ms-isac/
National Council of ISACs	www.nationalisacs.org
National Credit Union ISAO	ncuisao.org
National Cybersecurity Society	http://www.nationalcybersecuritysociety.org/
National Defense ISAC	ndisac.org
Northeast Ohio CyberConsortium	www.neocc.us
NRF Cyber Risk Exchange	NRF.com/nrf-cyber-risk-exchange
Oil and Natural Gas ISAC	www.ongisac.org
Political Campaign ISAO	USCyberdome.com
Real Estate ISAC	www.reisac.org
Regional Information Sharing Systems	www.riss.net/
Research and Education Network ISAC	www.ren-isac.net
Retail and Hospitality ISAC	https://rhisac.org
Sensato ISAO	sensato.co
Small and Mid-Sized Business ISAO	smbisao.com
Small Business Suply Chain ISAO	https://stc-ntc-lsu.org
Southern California ISAO	www.socalisao.com
Sports ISAO	sports-isao.org/site
Surface Transportation, Public Transportation, and Over-The-Road Bus ISACs	www.surfacetransportationisac.org
Texas CISO Council	www.texascisocouncil.org
Trustworthy Accountability Group	www.tagtoday.net
Water ISAC	WaterISAC.org

Analysis Methodology

Data in the form of standard indications of compromise (IOCs) are received either through push or pull configurations utilizing a STIX / TAXII protocol. The LACL cloud-based server collects the data from partners whereby data is ingested for analysis and utilization.

HOW ATT&CK FACILITATES MACHINE LEARNING:

MITRE's ATT&CK framework holds great promise in labeling events. The 11 categories were identified based on the later stages (exploit, control, maintain, execute) of a seven-stage Cyber Attack Lifecycle first articulated by Lockheed Martin as the cyber kill chain². For example, under the ATT&CK framework, a certain collection of IOCs could be tagged "domain fronting" under Command and Control (C2) in the matrix. Once this C2 tag is applied, using machine learning the same set of IOCs can be automatically labeled C2 elsewhere within a broader data store. When this system is adopted on a broader collaborative platform, its power will be immense as the function of IOC sets will be far more quickly identified expediting investigation and preemptively applied to prevent attacks.



<https://attack.mitre.org/resources/enterprise-introduction/>

Cyber Kill Chain / Cyber ATT&CK Lifecycle



Sample IOCs for Analysis

**Source: TruSTAR 2019 - [TruSTAR sample IOCs](#)

=== **Ursnif/Gozi** ===

SHA256

29D355127B54288F1CAE45EA3FF6A59C3BEF1995ACA15AD538679E48FC9F58EE

SHA1 E49AE7F11255D5C4CA42A38AEAA70D738F8CB59

MD5 6D245368F247897B930BB5F597B08ABC

15743d098267ce48e934ed0910bc299292754d02432ea775957c631170778d71
 070d70d39f310d7b8842f645d3ba2d44b2f6a3d7347a95b3a47d34c8e955885d
 31835c6350177eff88265e81335a50fcbe0dc46771bf031c836947851dcebb4f
 bd23a2eec4f94c07f4083455f022e4d58de0c2863fa6fa19d8f65bfe16fa19aa
 407a6c99581f428634f9d3b9ec4b79f79c29c79fdea5ea5e97ab3d280b2481a1
 75f31c9015e0f03f24808dca12dd90f4dfbbbd7e0a5626971c4056a07ea1b2b9

DNS requests

DOMAIN saintsandsinnersbar.com

DOMAIN itschoolegz.com

Connections

IP 8.250.159.254

IP 94.23.14.191

IP 46.17.45.108

IP 192.35.177.64

151.106.27.208

185.139.69.88

185.204.2.165

185.204.2.252

93.170.123.201

91.240.87.19

37.230.112.226

Dropping URLs:

[http://b9nicktof280.com/skoex/po2.php?l=deof\[1-12\].fgs](http://b9nicktof280.com/skoex/po2.php?l=deof[1-12].fgs)

[http://dwillow100bc.com/skoex/po2.php?l=deof\[1-11\].fgs](http://dwillow100bc.com/skoex/po2.php?l=deof[1-11].fgs)

[http://ljeffery54ae.top/skoex/po2.php?l=cupk\[1-11\].fgs](http://ljeffery54ae.top/skoex/po2.php?l=cupk[1-11].fgs)

[http://s1ldorothea4176.com/skoex/po2.php?l=cupk\[1-13\].fgs](http://s1ldorothea4176.com/skoex/po2.php?l=cupk[1-13].fgs)

http://151.106.27.208/client[.]rar

C2 domains:

ptl8sb.xyz
fooopzrp80yy.info
ksoniay95ee.info
lusgiuea.info
m6692vj7052.com
valphonsosry.info
zindv.club

=== **Emotet** ===

2eeb8c0911166e330d80e6e3038ef643
9c7f93cacede78e46b9be41af6804061
30a3d136f09554b4f6579e0ff59ee532
b43c4c2ab3d672f7b3a3a9be1764da04
6a576ce1ddd64fc6f173d7b7f1ebf1ec
6312930a139fa3ed22b87abb75c16afa
5017ececeb4d4f7c8483dd8178df693760ad227e94053b560ac60cd81870b199
308E12124421
9952bc89f8c70d198731ca6749228995fcc95073fa4225a793166a1870d4a7ea
6a7686d975d462332996c2098109d9e7
720065a4ac290f49f1be3f6f51d2270685d927a67746d2d0fecdec3138602190
73ddc47fc5ee06bddd987ce92107f85e364332e0aa8bbfbfbef52672c60dc3b01
7b48023defa745e7f48178be81a5db0636e6bd2e3adc0007b6631f9a148cdfae
808e007d456c663f6d4acbc8d55bc4e9c4336c0f2ad396f8f36f626cd063b7bf
923946a9a088ac8e71399b0f37702db4f25bad05
9952bc89f8c70d198731ca6749228995fcc95073fa4225a793166a1870d4a7ea
9adcfc8bc122edba857723599495eeb220ec19c9215f9fb5777ecc9c79dd055a
9c7f93cacede78e46b9be41af6804061
a065ed6ac5b3e96fe199b3ce0c300824661930438f55f7db134bb4b2ad2e78a6
aaf356d6973d26431167239fa14eeb4786c630e379dfdd232fac262d007868e0
ae80b79971917a7f7c6a66be17ccbe615ad2df2a4838cdecblreddfdfl1ea81f1a
b1b191abdaf11e9dd31ded27e6bf8c81
b2d5e936e3619763edaef00f7c098562bcf1057845058aa75e5bbd97bc7fc1c8
b893b1cb23670ab6caf21fb585804fd06e65e2b3537aa8d62648bfe4a141f6f8
ba8c9520beab21228251c92052271702
be1d878cca7ee7f93ab86a9d3e95623a
c546488c5f0a56ea6063a375ef7ea194df3020e92b724ac5f1bc14e7ea4ed9a5
c6ca1d78722cb6d53ecc97f4131912bd1fdafd0ee6d2646a808679f4eb3c6f51
c7e79a8af1da1a83dc1f4895c2f2046237c78641
c8e45939bfade8368a44b42c340676f5379776d71ef9db2f367d19c72bec8715
dd0697a8af0ba3d38f96e6bc8cc6e9548a8765f2
e493d0d3f17e7da7d604e688b9a3b6cbceade48d02385d5a4ad77c5852ff0f1f
e60f06d9dbea477fc46bad3183b4ade030477a8d9ddd13701a0b3078b98c302f
ee334c17eb80ac984491d82a253a5ab8
f6b1b401c0488fa97b0ef24d0b334a0f96a9ff73a4f4659a1adec03b044aa105

51.255.50.164
138.201.140.110
144.76.117.247
167.114.210.191
178.62.37.188
181.140.37.228
184.161.177.223
186.177.30.6
186.23.186.99
189.208.239.98
190.156.169.212
190.171.105.158
192.155.90.90
209.217.209.214
210.2.86.72
217.13.106.160
41.60.202.26
47.204.55.229
62.75.187.192
64.46.91.165
66.209.69.165
71.41.68.158
81.134.59.36
92.48.118.27
96.20.172.107
96.20.94.194

=== **Kovter** ===

4b37261d195927e8eb8e7720b06d81ebb396d167bddfc47c5bf3299c16e3143e
4b52a132ef1ee73716d4b48600528b7f39637f8a685a25dc39cc387d5471fcb4
4c2c1c4f83f5c7b159a0c6df1b9826aa1941f042c884d175490886a8efb12a3c
503fea24e4f82da1708bfa67ec9becd83aa8802e
5126b0b6f0e6ead2f61ae912dde98516
5163ea4e9eead143b523214942f01b0d67e823eb735d92c7d7f26110d951d052
51f1558fed8a5843c135268255194122a6c584d46afcc0c619c281de3b4ea1b5
548acca21065fd1e890272b1d44390c973aee9f61594157786ae546ed1a5527c
586639a9c9cd792e258cf4dbfad7770ea4bcd85a
5b36d98f475a35d6e8dc98be54494c39ddfbc95c44ea8da759a41cb1372b549d
5b6482ce2d13985bf2539c7605f84079c77a8ebb
5dea213a4b0cec84403759bac7063d64f733c18579039f0d48cd8c78625d16ec
60186bad9ec6d3eb4a488ed0ee21eda5f414e53f
615f9a5b4465303ed7428b68c15819ae19b42ff85e12eea09ab787c684e22637
6584b6eabe5e0f2e21fa0ebc0b0304d13888fdfd447bd9fa48605d06aed984ef
68dbd7180475a82c392d52bb1b5025f30c31c1a173fe5ee764e8ac2c59ff7255
691d9714c0e7f5f666b2f5642ef9829c3bd2fbb842916f92cd7869d5420e5767
6b8089434623a9d01c112b859f04306e96ccdf5c8e1c05422d100b22bd2aaffb
6efdfa35b2b067cd9a1e0218d3a83af6

7116288a94d93137fa8a6a1af047c2d20bc74d77afd8e91667e954b2eaf372cf
771d4c236064d3a25a94d92c26cc562d85ca3920
79999f384d313b5cbca5cd9d0943f590fd14b8b04ac69618912b7853e3d9a1de
7a5d5c109bbde92cdc3d50295cc7268b0944158d1030df675ca7381525164313
7c448193352445896ec2f8cc7e3c4d26
7caaf55ff9c5f7947d3036ac46b78f33
812bd973092832e762f1bb024f2635fa18a922648ecec3ea9771bf15adcb5451
824cebf9f50a6f6dfc8cc4b10aa5f72ad9c00a6133a0940c9e5f03f30e198aed
836fe7e940b19459041084612f966a53f981dbd8
849c70fb58fef4c58a31e7b72bebe6fba11932a4b277fe9976ca8db7d014e1d6
8707f964c96588201f8fb90112a4c10ea5cdfab931ce2e47fb82d5b28d7a5bf
8afa3ff6f56f87d2012f64fc0b3492b193c2060e715893ffc3574488d03d10f7
8e0f8d07202ecaeda8b3452ef1267777f404ca7b331f443e0d430552f6253e0d
8fe7b977aea19e4db1c3d0846d85ed875d37c6fa5423545644335afbf6f2e444
9a2811da41435c5f35d63dbc9ecdbd7c8c7670073c762567a4b7f3a0eef6c730
9dc2c6f5c307b13839567cb756b51c20
a2c41b4868c2e1638318a52d1dfb5c9c
a641a7e71af1d177209b7c0a1d2c9039b2b66c19e32d54a3d08e1e434f33e1c2
ae0d06b1ffbd3ee83448b4f490bb52307069bafb
b0a235141adc6e78ce9973c69e052de32d70e63908c7dec393b201ba5f5aa196
b0ddb4be0ca32c61fb3ff98870b7b68d85752729
b1303a17658fdece726c9420a5916d01
b535168617f6d63fd1d5aca1e8f051985754a11d0b7632bac1474e317d9b9c93
b717dc25bdf3df0257a51a13b5febd1288e07257c9865d1c7d32e97deb9e2f5f
b7f3de17c908167042b53a2f812e75ff2993d940d71e7e7191c25fa845b1b608
ba0d72bdd59a92b6dd23356ade735149841912429a6a757a5cfd656358a59864
ba4d067e6caf43a76324bb52b1c3d821aa4d3ccd
bb6217ff048221fdbddf877c1982b2dc4f77213a18473db59006dabccba42a2a
be3f53f548267c1c92b7267e93668b53
c5460f6612228a86fe14115263fa37b1f277ed45f14a68e316de4fe7eeaa17d1
c6e6a8351b541df3b5765f5768a01215
ca18b1c51b0bd9e17c3828a83d550de1416e6f01bbcfce63ffb41d405cdd783d
cc49ddaac45786c4ba29e9da01cedcb16d2cd2a5f9b30407a81b7727b64588c3
cf82d275b3010d511f8ed700d42365f176d71edad50585a4ea4cbc65748d32b7
d12fb1fcb3c131caed92087423201981a7403361
d3443c21a8fbec2dff05d45565a84c572be0dadf
d688b224fd591c9160ce0af399d60c8eed3f8d72374dbcee87db2515e06b9890
d6934912c1183b06fce2840a6a13a76e6cc3598f971ca1aa4c6085655812adc7
da211a8ae0c54341ce11a67ccf3f4981b17e2bddd5dc1af3138abe40cc93dedd
dd5cb09c15067cb011cc823f0ebb82d8f5999b91e11941f9fa59dd4ea1d1bdf8
e098de1c0c68772538a58f26858bc053
e6e8b85b28d435bd76f8bf3ddfa99689aa699de8
e8e58d0c40cf5687974051fdc2225bf48190d5adffed5ff7f6051033021e68b0
e95d648019601e6c8a592d58248d69d4971cf0a5b94efacc4f1bc331ca6fd04c
e9c30d85d085a180bff76033e43ff46cdecc9333
ed7ed26843158a156621f592e6f6df00ce5fbe2c7c9e1925acf78f40d7ad3311
ede72eb9d0683fe4e69a4e4fdd73dd16bb9b54d7eac34809212cb4c594c44fb2
ee0e059e5abe79cb502ad83856ea6151b3c9d2e2e20f30db6a4632ee540ac405
eed32cf7aece25f6fdeb7f6bfa6124f

f2a227665a634ab63eb5dfdbbcd62cb247c1e2b9048e6a178f092f30ad85f50f
f6a8f4f76e9f1c20df0c8888125482a95a2efddd2fa2986b928b7095f076b783
faf844001c2bd57c4bb2e64ba050e4d6
fc6a5a9e90966b4d83e338955353a5defbe08faa0cdb8e60db5dd4c2beeeddee

Purpose

ATT&CK for Enterprise is a constantly growing common reference for adversary behavior that brings greater awareness of what actions may be seen during an enterprise network intrusion. It enables a comprehensive evaluation of computer network defense (CND) technologies, processes, and policies against a common enterprise adversary model. We do not claim that it is a comprehensive list of techniques, only an approximation of what is publicly known; therefore, it is also an invitation for the community to contribute additional details and information to continue developing the body of knowledge. Contributions could include new techniques, categories of actions, clarifying information, examples, other platforms or environments, methods of detection or mitigation, and data sources. See the [Contribute](#) page for instructions on how to get involved.

The result will help focus community efforts on areas that are not well understood or covered by current defensive technologies and best practices. Developers of current defensive tools and policies can identify where their value and strengths are in relation to the ATT&CK for Enterprise adversary model. Likewise, cyber security research can use ATT&CK for Enterprise as a grounded reference point to drive future investigation.

ATT&CK for Enterprise Use Cases

- Prioritize development and/or acquisition efforts for CND capabilities
- Conduct analyses of alternatives between CND capabilities
- Determine “coverage” of a set of CND capabilities
- Describe an intrusion chain of events based on the technique used from start to finish with a common reference
- Identify commonalities between adversary tradecraft, as well as distinguishing characteristics
- Connect mitigations, weaknesses, and adversaries

Enterprise Techniques

Enterprise Techniques: 244

ID	Name	Description
T1156	.bash_profile and .bashrc	~/.bash_profile and ~/.bashrc are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. ~/.bash_profile is executed for login shells and ~/.bashrc is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), ~/.bash_profile is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, ~/.bashrc is executed. This allows users more fine grained control over when they want certain commands executed.
T1134	Access Token Manipulation	Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command <code>runas</code> .
T1015	Accessibility Features	Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.
T1087	Account Discovery	Adversaries may attempt to get a listing of local system or domain accounts.
T1098	Account Manipulation	Account manipulation may aid adversaries in maintaining access to credentials and certain permission levels within an environment. Manipulation could consist of modifying permissions, modifying credentials, adding or changing permission groups, modifying account settings, or modifying how authentication is performed. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to subvert password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain.
T1182	AppCert DLLs	Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> are loaded into every process that calls the ubiquitously used application programming interface (API)

ID	Name	Description
		functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec.
T1103	Applnit DLLs	Dynamic-link libraries (DLLs) that are specified in the Applnit_DLLs value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. Similar to Process Injection , these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.
T1155	AppleScript	macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the <code>osalang</code> program.
T1017	Application Deployment Software	Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.
T1138	Application Shimming	The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses Hooking to redirect the code as necessary in order to communicate with the OS.

ID	Name	Description
T1010	Application Window Discovery	Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.
T1123	Audio Capture	An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.
T1131	Authentication Package	Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.
T1119	Automated Collection	Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of Scripting to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. This functionality could also be built into remote access tools.
T1020	Automated Exfiltration	Data, such as sensitive documents, may be exfiltrated through the use of automated processing or Scripting after being gathered during Collection.
T1139	Bash History	Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code> . Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials.
T1009	Binary Padding	Some security tools inspect files with static signatures to determine if they are known malicious. Adversaries may add data to files to increase the size beyond what security tools are capable of handling or to change the file hash to avoid hash-based blacklists.
T1197	BITS Jobs	Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

ID	Name	Description
T1067	Bootkit	A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR).
T1217	Browser Bookmark Discovery	Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.
T1176	Browser Extensions	Browser extensions or plugins are small programs that can add functionality and customize aspects of internet browsers. They can be installed directly or through a browser's app store. Extensions generally have access and permissions to everything that the browser can access.
T1110	Brute Force	Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.
T1088	Bypass User Account Control	Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
T1042	Change Default File Association	When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility. Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.
T1146	Clear Command History	macOS and Linux both keep track of the commands users type in their terminal so that users can easily remember what they've done. These logs can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable HISTFILE. When a user logs off a system, this information is flushed to a file in the user's home directory called ~/.bash_history. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Since everything typed on the command-line is saved, passwords passed in on the command line are also saved.

ID	Name	Description
		Adversaries can abuse this by searching these files for cleartext passwords. Additionally, adversaries can use a variety of methods to prevent their own commands from appear in these logs such as <code>unset HISTFILE, export HISTFILESIZE=0, history -c, rm ~/.bash_history</code> .
T1115	Clipboard Data	Adversaries may collect data stored in the Windows clipboard from users copying information within or between applications.
T1191	CMSTP	The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.
T1116	Code Signing	Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries . The certificates used during an operation may be created, forged, or stolen by the adversary.
T1059	Command-Line Interface	Command-line interfaces provide a way of interacting with computer systems and is a common feature across many types of operating system platforms. One example command-line interface on Windows systems is cmd , which can be used to perform a number of tasks including execution of other software. Command-line interfaces can be interacted with locally or remotely via a remote desktop application, reverse shell session, etc. Commands that are executed run with the current permission level of the command-line interface process unless the command includes process invocation that changes permissions context for that execution (e.g. Scheduled Task).
T1043	Commonly Used Port	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as
T1092	Communication Through Removable Media	Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by Replication Through Removable Media . Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

ID	Name	Description
T1500	Compile After Delivery	Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Similar to Obfuscated Files or Information , text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as csc.exe or GCC/MinGW.
T1223	Compiled HTML File	Compiled HTML files (.chm) are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such as VBA, JScript, Java, and ActiveX. CHM content is displayed using underlying components of the Internet Explorer browser loaded by the HTML Help executable program (hh.exe).
T1109	Component Firmware	Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to System Firmware but conducted upon other system components that may not have the same capability or level of integrity checking. Malicious device firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.
T1122	Component Object Model Hijacking	The Component Object Model (COM) is a system within Windows to enable interaction between software components through the operating system. Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.
T1090	Connection Proxy	A connection proxy is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN , ZXProxy, and ZXPortMap.

ID	Name	Description
T1196	Control Panel Items	Windows Control Panel items are utilities that allow users to view and adjust computer settings. Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a CPlApplet function. Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file.
T1136	Create Account	Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.
T1003	Credential Dumping	Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
T1081	Credentials in Files	Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.
T1214	Credentials in Registry	The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.
T1094	Custom Command and Control Protocol	Adversaries may communicate using a custom command and control protocol instead of encapsulating commands/data in an existing Standard Application Layer Protocol . Implementations include mimicking well-known protocols or developing custom protocols (including raw sockets) on top of fundamental protocols provided by TCP/IP/another standard network stack.
T1024	Custom Cryptographic Protocol	Adversaries may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.
T1002	Data Compressed	An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the

ID	Name	Description
		network. The compression is done separately from the exfiltration channel and is performed using a custom program or algorithm, or a more common compression library or utility such as 7zip, RAR, ZIP, or zlib.
T1485	Data Destruction	Adversaries may destroy data data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as <code>del</code> and <code>rm</code> often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.
T1132	Data Encoding	Command and control (C2) information is encoded using a standard data encoding system. Use of data encoding may be to adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, UTF-8, or other binary-to-text and character encoding systems. Some data encoding systems may also result in data compression, such as gzip.
T1022	Data Encrypted	Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip.
T1486	Data Encrypted for Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

ID	Name	Description
T1213	Data from Information Repositories	Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information.
T1005	Data from Local System	Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system prior to Exfiltration.
T1039	Data from Network Shared Drive	Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration.
T1025	Data from Removable Media	Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration.
T1001	Data Obfuscation	Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, commingling legitimate traffic with C2 communications traffic, or using a non-standard data encoding system, such as a modified Base64 encoding for the message body of an HTTP request.
T1074	Data Staged	Collected data is staged in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Data Compressed or Data Encrypted .
T1030	Data Transfer Size Limits	An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.
T1207	DCShadow	DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a Domain Controller (DC). Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

ID	Name	Description
T1491	Defacement	Adversaries may modify visual content available internally or externally to an enterprise network. Reasons for Defacement include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion.
T1140	Deobfuscate/Decode Files or Information	Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware, Scripting , PowerShell , or by using utilities present on the system.
T1089	Disabling Security Tools	Adversaries may disable security tools to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security scanning or event reporting.
T1488	Disk Content Wipe	Adversaries may erase the contents of storage devices on specific systems as well as large numbers of systems in a network to interrupt availability to system and network resources.
T1487	Disk Structure Wipe	Adversaries may corrupt or wipe the disk data structures on hard drive necessary to boot systems; targeting specific critical systems as well as a large number of systems in a network to interrupt availability to system and network resources.
T1175	Distributed Component Object Model	Windows Distributed Component Object Model (DCOM) is transparent middleware that extends the functionality of Component Object Model (COM) beyond a local computer using remote procedure call (RPC) technology. COM is a component of the Windows application programming interface (API) that enables interaction between software objects. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).
T1038	DLL Search Order Hijacking	Windows systems use a common method to look for required DLLs to load into a program. Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.
T1073	DLL Side-Loading	Programs may specify DLLs that are loaded at runtime. Programs that improperly or vaguely specify a required DLL may be open to a vulnerability in which an unintended DLL is loaded. Side-loading vulnerabilities specifically occur when Windows Side-by-Side (WinSxS) manifests are not explicit enough about characteristics of the DLL to be loaded. Adversaries

ID	Name	Description
		may take advantage of a legitimate program that is vulnerable to side-loading to load a malicious DLL.
T1172	Domain Fronting	Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).
T1483	Domain Generation Algorithms	Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.
T1482	Domain Trust Discovery	Adversaries may attempt to gather information on domain trust relationships that may be used to identify Lateral Movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain. Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct SID-History Injection , Pass the Ticket , and Kerberoasting . Domain trusts can be enumerated using the DSEnumerateDomainTrusts() Win32 API call, .NET methods, and LDAP. The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts.
T1189	Drive-by Compromise	A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation.
T1157	Dylib Hijacking	macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries can take advantage of ambiguous paths to plant dylibs to gain privilege escalation or persistence.

ID	Name	Description
T1173	Dynamic Data Exchange	Windows Dynamic Data Exchange (DDE) is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.
T1114	Email Collection	Adversaries may target user email to collect sensitive information from a target.
T1499	Endpoint Denial of Service	Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.
T1480	Execution Guardrails	Execution guardrails constrain execution or actions based on adversary supplied environment specific conditions that are expected to be present on the target.
T1106	Execution through API	Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.
T1129	Execution through Module Load	The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows Native API which is called from functions like CreateProcess(), LoadLibrary(), etc. of the Win32 API.
T1048	Exfiltration Over Alternative Protocol	Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.
T1041	Exfiltration Over Command and Control Channel	Data exfiltration is performed over the Command and Control channel. Data is encoded into the normal communications channel using the same protocol as command and control communications.

ID	Name	Description
T1011	Exfiltration Over Other Network Medium	Exfiltration could occur over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries could choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.
T1052	Exfiltration Over Physical Medium	In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.
T1190	Exploit Public-Facing Application	The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL) , standard services (like SMB or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion .
T1203	Exploitation for Client Execution	Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.
T1212	Exploitation for Credential Access	Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems. One example of this is

ID	Name	Description
		MS14-068, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions. Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.
T1211	Exploitation for Defense Evasion	Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.
T1068	Exploitation for Privilege Escalation	Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform Privilege Escalation to include use of software exploitation to circumvent those restrictions.
T1210	Exploitation of Remote Services	Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.
T1133	External Remote Services	Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.
T1181	Extra Window Memory Injection	Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data). Registration of new windows classes can include a request for up to 40 bytes of extra window memory (EWM) to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value.

ID	Name	Description
T1008	Fallback Channels	Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.
T1083	File and Directory Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
T1107	File Deletion	Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces behind as to what was done within a network and how. Adversaries may remove these files over the course of an intrusion to keep their footprint low or remove them at the end as part of the post-intrusion cleanup process.
T1222	File Permissions Modification	File permissions are commonly managed by discretionary access control lists (DACLS) specified by the file owner. File DACL implementation may vary by platform, but generally explicitly designate which users/groups can perform which actions (ex: read, write, execute, etc.).
T1006	File System Logical Offsets	Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.
T1044	File System Permissions Weakness	Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.
T1495	Firmware Corruption	Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot. Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices could include the motherboard, hard drive, or video cards.

ID	Name	Description
T1187	Forced Authentication	The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443.
T1144	Gatekeeper Bypass	In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called <code>com.apple.quarantine</code> . This attribute is read by Apple's Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.
T1061	Graphical User Interface	The Graphical User Interfaces (GUI) is a common way to interact with an operating system. Adversaries may use a system's GUI during an operation, commonly through a remote interactive session such as Remote Desktop Protocol , instead of through a Command-Line Interface , to search for information and execute files via mouse double-click events, the Windows Run command , or other potentially difficult to monitor interactions.
T1484	Group Policy Modification	Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain.
T1200	Hardware Additions	Computer accessories, computers, or networking hardware may be introduced into a system as a vector to gain execution. While public references of usage by APT groups are scarce, many penetration testers leverage hardware additions for initial access. Commercial and open source products are leveraged with capabilities such as passive network tapping , man-in-the-middle encryption breaking , keystroke injection , kernel memory reading via DMA , adding new wireless access to an existing network , and others.
T1158	Hidden Files and Directories	To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a 'hidden' file. These files don't show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI)

ID	Name	Description
		prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls -a</code> for Linux and macOS).
T1147	Hidden Users	Every user account in macOS has a userID associated with it. When creating a user, you can specify the userID for that account. There is a property value in <code>/Library/Preferences/com.apple.loginwindow</code> called <code>Hide500Users</code> that prevents users with userIDs 500 and lower from appearing at the login screen. By using the Create Account technique with a userID under 500 and enabling this property (setting it to Yes), an adversary can hide their user accounts much more easily: <code>sudo dscl . -create /Users/username UniqueID 401 .</code>
T1143	Hidden Window	The configurations for how applications run on macOS and OS X are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code> , which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window .
T1148	HISTCONTROL	The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. This setting can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that " ls" will not be saved, but "ls" would be saved by history. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. Adversaries can use this to operate without leaving traces by simply prepending a space to all of their terminal commands.
T1179	Hooking	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.
T1062	Hypervisor	A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware. It presents a virtual running environment to an operating system. An example of a common hypervisor is Xen. A type-1 hypervisor operates at a level below the operating system and could be designed with Rootkit functionality to hide its existence from

ID	Name	Description
		the guest operating system. A malicious hypervisor of this nature could be used to persist on systems through interruption.
T1183	Image File Execution Options Injection	Image File Execution Options (IFEO) enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., "C:\dbg\ntsd.exe -g notepad.exe").
T1054	Indicator Blocking	An adversary may attempt to block indicators or events typically captured by sensors from being gathered and analyzed. This could include modifying sensor settings stored in configuration files and/or Registry keys to disable or maliciously redirect event telemetry.
T1066	Indicator Removal from Tools	If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.
T1070	Indicator Removal on Host	Adversaries may delete or alter generated artifacts on a host system, including logs and potentially captured files such as quarantined malware. Locations and format of logs will vary, but typical organic system logs are captured as Windows events or Linux/macOS files such as Bash History and /var/log/* .
T1202	Indirect Command Execution	Various Windows utilities may be used to execute commands, possibly without invoking <code>cmd</code> . For example, Forfiles , the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a Command-Line Interface , Run window, or via scripts.
T1490	Inhibit System Recovery	Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of Data Destruction and Data Encrypted for Impact .
T1056	Input Capture	Adversaries can use methods of capturing user input for obtaining credentials for Valid Accounts and information Collection that include keylogging and user input field interception.

ID	Name	Description
T1141	Input Prompt	When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: Bypass User Account Control).
T1130	Install Root Certificate	Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate. Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.
T1118	InstallUtil	InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. InstallUtil is located in the .NET directories on a Windows system: C:\Windows\Microsoft.NET\Framework\v\InstallUtil.exe and C:\Windows\Microsoft.NET\Framework64\v\InstallUtil.exe. InstallUtil.exe is digitally signed by Microsoft.
T1208	Kerberoasting	Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service).
T1215	Kernel Modules and Extensions	Loadable Kernel Modules (or LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system. When used maliciously, Loadable Kernel Modules (LKMs) can be a type of kernel-mode Rootkit that run with the highest operating system privilege (Ring 0). Adversaries can use loadable kernel modules to covertly persist on a system and evade defenses. Examples have been found in the wild and there are some open source projects.
T1142	Keychain	Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and Kerberos. Keychain files are located in ~/Library/Keychains/, /Library/Keychains/, and /Network/Library/Keychains/. The security command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

ID	Name	Description
T1159	Launch Agent	Per Apple's developer documentation, when a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (plist) files found in <code>/System/Library/LaunchAgents</code> , <code>/Library/LaunchAgents</code> , and <code>\$HOME/Library/LaunchAgents</code> . These launch agents have property list files which point to the executables that will be launched.
T1160	Launch Daemon	Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> . These LaunchDaemons have property list files which point to the executables that will be launched.
T1152	Launchctl	Launchctl controls the macOS launchd process which handles things like launch agents and launch daemons, but can execute other commands or programs itself. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input. By loading or reloading launch agents or launch daemons, adversaries can install persistence or execute changes they made. Running a command from launchctl is as simple as <code>launchctl submit -l -- /Path/to/thing/to/execute "arg" "arg" "arg"</code> . Loading, unloading, or reloading launch agents or launch daemons can require elevated privileges.
T1161	LC_LOAD_DYLIB Addition	Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The <code>LC_LOAD_DYLIB</code> header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long adjustments are made to the rest of the fields and dependencies. There are tools available to perform these changes. Any changes will invalidate digital signatures on binaries because the binary is being modified. Adversaries can remediate this issue by simply removing the <code>LC_CODE_SIGNATURE</code> command from the binary so that the signature isn't checked at load time.
T1149	LC_MAIN Hijacking	As of OS X 10.8, mach-O binaries introduced a new header called <code>LC_MAIN</code> that points to the binary's entry point for execution. Previously, there were two headers to achieve this same effect: <code>LC_THREAD</code> and <code>LC_UNIXTHREAD</code> . The entry point for a binary can be hijacked so that initial execution flows to a malicious addition (either another section or a code cave) and then goes back to the initial entry point so that the victim doesn't know anything was different.

ID	Name	Description
		By modifying a binary in this way, application whitelisting can be bypassed because the file name or application path is still the same.
T1171	LLMNR/NBT-NS Poisoning and Relay	Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name.
T1168	Local Job Scheduling	On Linux and macOS systems, multiple methods are supported for creating pre-scheduled and periodic background jobs: cron, at, and launchd. Unlike Scheduled Task on Windows systems, job scheduling on Linux-based systems cannot be done remotely unless used in conjunction within an established remote session, like secure shell (SSH).
T1162	Login Item	MacOS provides the option to list specific applications to run when a user logs in. These applications run under the logged in user's context, and will be started every time the user logs in. Login items installed using the Service Management Framework are not visible in the System Preferences and can only be removed by the application that created them . Users have direct control over login items installed using a shared file list which are also visible in System Preferences . These login items are stored in the user's <code>~/Library/Preferences/</code> directory in a plist file called <code>com.apple.loginitems.plist</code> . Some of these applications can open visible dialogs to the user, but they don't all have to since there is an option to 'Hide' the window. If an adversary can register their own login item or modified an existing one, then they can use it to execute their code for a persistence mechanism each time the user logs in . The API method <code>SMLoginItemSetEnabled</code> can be used to set Login Items, but scripting languages like AppleScript can do this as well .
T1037	Logon Scripts	Windows allows logon scripts to be run whenever a specific user or group of users log into a system. The scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server.
T1177	LSASS Driver	The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) <code>lsass.exe</code> process.

ID	Name	Description
T1185	Man in the Browser	Adversaries can take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify behavior, and intercept information as part of various man in the browser techniques.
T1036	Masquerading	Masquerading occurs when the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. Several different variations of this technique have been observed.
T1031	Modify Existing Service	Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and Reg .
T1112	Modify Registry	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in Persistence and Execution.
T1170	Mshta	Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension .hta. HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser.
T1188	Multi-hop Proxy	To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.
T1104	Multi-Stage Channels	Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.
T1026	Multiband Communication	Some adversaries may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

ID	Name	Description
T1079	Multilayer Encryption	An adversary performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.
T1128	Netsh Helper DLL	Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility. The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code> .
T1498	Network Denial of Service	Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.
T1046	Network Service Scanning	Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans using tools that are brought onto a system.
T1126	Network Share Connection Removal	Windows shared drive and Windows Admin Shares connections can be removed when no longer needed. Net is an example utility that can be used to remove network share connections with the <code>net use \system\share /delete</code> command.
T1135	Network Share Discovery	Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.
T1040	Network Sniffing	Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.
T1050	New Service	When operating systems boot up, they can start programs or applications called services that perform background system functions. A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.
T1096	NTFS File Attributes	Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. Within MFT entries are

ID	Name	Description
		file attributes, such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files).
T1027	Obfuscated Files or Information	Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.
T1137	Office Application Startup	Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started.
T1075	Pass the Hash	Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.
T1097	Pass the Ticket	Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.
T1174	Password Filter DLL	Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as dynamic link libraries (DLLs) containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts.
T1201	Password Policy Discovery	Password policies for networks are a way to enforce complex passwords that are difficult to guess or crack through Brute Force . An adversary may attempt to access detailed information about the password policy used within an enterprise network. This would help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying

ID	Name	Description
		passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).
T1034	Path Interception	Path interception occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. One example of this was the use of a copy of <code>cmd</code> in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function.
T1120	Peripheral Device Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.
T1069	Permission Groups Discovery	Adversaries may attempt to find local system or domain-level groups and permissions settings.
T1150	Plist Modification	Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. These files are UTF-8 encoded and formatted like XML documents via a series of keys surrounded by < >. They detail when programs should execute, file paths to the executables, program arguments, required OS permissions, and many others. plists are located in certain locations depending on their purpose such as <code>/Library/Preferences</code> (which execute with elevated privileges) and <code>~/Library/Preferences</code> (which execute with a user's privileges).
T1205	Port Knocking	Port Knocking is a well-established method used by both defenders and adversaries to hide open ports from access. To enable a port, an adversary sends a series of packets with certain characteristics before the port will be opened. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports, but can involve unusual flags, specific strings or other unique characteristics. After the sequence is completed, opening a port is often accomplished by the host based firewall, but could also be implemented by custom software.
T1013	Port Monitors	A port monitor can be set through the API call to set a DLL to be loaded at startup. This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, <code>spoolsv.exe</code> , on boot. The <code>spoolsv.exe</code> process also runs under SYSTEM level permissions. Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code> .

ID	Name	Description
T1086	PowerShell	PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.
T1145	Private Keys	Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.
T1057	Process Discovery	Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.
T1186	Process Doppelgänger	Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction.
T1093	Process Hollowing	Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to Process Injection , execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis.
T1055	Process Injection	Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.
T1012	Query Registry	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.
T1163	Rc.common	During the boot process, macOS executes <code>source /etc/rc.common</code> , which is a shell script containing various utility functions. This file also defines routines for processing command-line arguments and for gathering system settings, and is thus recommended to include in the start

ID	Name	Description
		of Startup Item Scripts . In macOS and OS X, this is now a deprecated technique in favor of launch agents and launch daemons, but is currently still used.
T1164	Re-opened Applications	Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine. While this is usually done via a Graphical User Interface (GUI) on an app-by-app basis, there are property list files (plist) that contain this information as well located at <code>~/Library/Preferences/com.apple.loginwindow.plist</code> and <code>~/Library/Preferences/ByHost/com.apple.loginwindow.*.plist</code> .
T1108	Redundant Access	Adversaries may use more than one remote access tool with varying command and control protocols as a hedge against detection. If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary's tools and access, then the adversary will be able to retain access to the network. Adversaries may also attempt to gain access to Valid Accounts to use External Remote Services such as external VPNs as a way to maintain access despite interruptions to remote access tools deployed within a target network.
T1060	Registry Run Keys / Startup Folder	Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
T1121	Regsvcs/Regasm	Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally signed by Microsoft.
T1117	Regsvr32	Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries.
T1219	Remote Access Tools	An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be whitelisted within a target environment. Remote access tools like VNC, Ammy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries.

ID	Name	Description
T1076	Remote Desktop Protocol	Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). There are other implementations and third-party tools that provide graphical access Remote Services similar to RDS.
T1105	Remote File Copy	Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Files may be copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP . Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.
T1021	Remote Services	An adversary may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.
T1018	Remote System Discovery	Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used. Adversaries may also use local host files in order to discover the hostname to IP address mappings of remote systems.
T1091	Replication Through Removable Media	Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.
T1496	Resource Hijacking	Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems which may impact system and/or hosted service availability.
T1014	Rootkit	Rootkits are programs that hide the existence of malware by intercepting (i.e., Hooking) and modifying operating system API calls that supply system information. Rootkits or rootkit

ID	Name	Description
		enabling functionality may reside at the user or kernel level in the operating system or lower, to include a Hypervisor , Master Boot Record, or the System Firmware .
T1085	Rundll32	The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.
T1494	Runtime Data Manipulation	Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user. By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
T1053	Scheduled Task	Utilities such as at and schtasks , along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.
T1029	Scheduled Transfer	Data exfiltration may be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.
T1113	Screen Capture	Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations.
T1180	Screensaver	Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension. The Windows screensaver application scrnsave.scr is located in <code>c:\Windows\System32\</code> , and <code>c:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.
T1064	Scripting	Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and PowerShell but could also be in the form of command-line batch scripts.

ID	Name	Description
T1063	Security Software Discovery	Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules and anti-virus. These checks may be built into early-stage remote access tools.
T1101	Security Support Provider	Windows Security Support Provider (SSP) DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code> . An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the <code>AddSecurityPackage</code> Windows API function is called.
T1167	Securityd Memory	In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords. Apple's securityd utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password.
T1035	Service Execution	Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.
T1058	Service Registry Permissions Weakness	Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code> . The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, <code>sc.exe</code> , PowerShell, or Reg . Access to Registry keys is controlled through Access Control Lists and permissions.
T1489	Service Stop	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.

ID	Name	Description
T1166	Setuid and Setgid	When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively . Normally an application is run in the current user's context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn't need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file's attributes via <code>ls -l</code> . The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code> .
T1051	Shared Webroot	Adversaries may add malicious content to an internally accessible website through an open network file share that contains the website's webroot or Web content directory and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured.
T1023	Shortcut Modification	Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process. Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use Masquerading to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.
T1178	SID-History Injection	The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. An account can hold additional SIDs in the SID-History Active Directory attribute , allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).
T1218	Signed Binary Proxy Execution	Binaries signed with trusted digital certificates can execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files. This behavior may be abused by adversaries to execute malicious files that could bypass application whitelisting and signature

ID	Name	Description
		validation on systems. This technique accounts for proxy execution methods that are not already accounted for within the existing techniques.
T1216	Signed Script Proxy Execution	Scripts signed with trusted certificates can be used to proxy execution of malicious files. This behavior may bypass signature validation restrictions and application whitelisting solutions that do not account for use of these scripts.
T1198	SIP and Trust Provider Hijacking	In user mode, Windows Authenticode digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature.
T1045	Software Packing	Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.
T1153	Source	The <code>source</code> command loads functions into the current shell or executes files in the current context. This built-in command can be run in two different ways <code>source /path/to/filename [arguments]</code> OR <code>./path/to/filename [arguments]</code> . Take note of the space after the ".". Without a space, a new shell is created that runs the program instead of running the program within the current context. This is often used to make certain features or functions available to a shell or to update a specific shell's environment.
T1151	Space after Filename	Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system. For example, if there is a Mach-O executable file called evil.bin, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to evil.txt, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to "evil.txt " (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed .

ID	Name	Description
T1193	Spearphishing Attachment	Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.
T1192	Spearphishing Link	Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.
T1194	Spearphishing via Service	Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.
T1184	SSH Hijacking	Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.
T1071	Standard Application Layer Protocol	Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
T1032	Standard Cryptographic Protocol	Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.
T1095	Standard Non-Application Layer Protocol	Use of a standard non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

ID	Name	Description
T1165	Startup Items	Per Apple's documentation, startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items . This is technically a deprecated version (superseded by Launch Daemons), and thus the appropriate folder, <code>/Library/StartupItems</code> isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code> , reside in the top-level directory.
T1492	Stored Data Manipulation	Adversaries may insert, delete, or manipulate data at rest in order to manipulate external outcomes or hide activity. By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
T1169	Sudo	The sudoers file, <code>/etc/sudoers</code> , describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL .</code>
T1206	Sudo Caching	The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments." Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code> that is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).
T1195	Supply Chain Compromise	Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

ID	Name	Description
T1019	System Firmware	The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer.
T1082	System Information Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.
T1016	System Network Configuration Discovery	Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp , ipconfig/ifconfig , nbtstat , and route .
T1049	System Network Connections Discovery	Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.
T1033	System Owner/User Discovery	Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using Credential Dumping . The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs.
T1007	System Service Discovery	Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist , and "net start" using Net , but adversaries may also use other tools as well.
T1124	System Time Discovery	The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network.
T1501	Systemd Service	Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources. Systemd is the default initialization (init) system on many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems.

ID	Name	Description
T1080	Taint Shared Content	Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.
T1221	Template Injection	Microsoft's Open Office XML (OOXML) specification defines an XML-based format for Office documents (.docx, .xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives comprised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.
T1072	Third-party Software	Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, VNC, HBSS, Altiris, etc.). If an adversary gains access to these systems, then they may be able to execute code.
T1209	Time Providers	The Windows Time service (W32Time) enables time synchronization across and within domains. W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.
T1099	Timestomp	Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name Masquerading to hide malware and tools.
T1493	Transmitted Data Manipulation	Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity. By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.
T1154	Trap	The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code> . Adversaries can use this to register code to be executed when the shell encounters specific interrupts either to gain execution or as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.

ID	Name	Description
T1127	Trusted Developer Utilities	There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application whitelisting defensive solutions.
T1199	Trusted Relationship	Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.
T1111	Two-Factor Authentication Interception	Use of two- or multifactor authentication is recommended and provides a higher level of security than user names and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms. Adversaries may target authentication mechanisms, such as smart cards, to gain access to systems, services, and network resources.
T1065	Uncommonly Used Port	Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.
T1204	User Execution	An adversary may rely upon specific actions by a user in order to gain execution. This may be direct code execution, such as when a user opens a malicious executable delivered via Spearphishing Attachment with the icon and apparent extension of a document file. It also may lead to other execution techniques, such as when a user clicks on a link delivered via Spearphishing Link that leads to exploitation of a browser or application vulnerability via Exploitation for Client Execution . While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it.
T1078	Valid Accounts	Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.
T1125	Video Capture	An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the

ID	Name	Description
		purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.
T1497	Virtualization/Sandbox Evasion	Adversaries may check for the presence of a virtual machine environment (VME) or sandbox to avoid potential detection of tools and activities. If the adversary detects a VME, they may alter their malware to conceal the core functions of the implant or disengage from the victim. They may also search for VME artifacts before dropping secondary or additional payloads.
T1102	Web Service	Adversaries may use an existing, legitimate external Web service as a means for relaying commands to a compromised system.
T1100	Web Shell	A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (see, for example, China Chopper Web shell client).
T1077	Windows Admin Shares	Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include <code>C\$</code> , <code>ADMIN\$</code> , and <code>IPC\$</code> .
T1047	Windows Management Instrumentation	Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135.
T1084	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts. Examples of events that may be subscribed to are the wall clock time or the computer's uptime. Several threat groups have reportedly used this technique to maintain persistence.
T1028	Windows Remote Management	Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify

ID	Name	Description
		the Registry, modify services). It may be called with the <code>winrm</code> command or by any number of programs such as PowerShell.
T1004	Winlogon Helper DLL	Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\SoftwareWow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon.
T1220	XSL Script Processing	Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages.



Los Angeles Cyber Lab, Inc.
 An Internet Security – Information
 Sharing & Analysis Organization (IS-ISAO)
 Supported by the U.S. Department of Homeland Security

Change Request (CR) Form

Project Name:	LA Cyber Lab – [TISP or Mobile App]
CR NUMBER: <COULD BE ASSIGNED AN AUTOMATED SYSTEMS>	COMPLETE PART 1 AND SUBMIT TO LACL POLICY DIRECTOR

PART 1: REQUEST (TO BE COMPLETED BY REQUESTER)	
Title of Change	
Requester	Date MM/DD/YY
Impact of Requested Change	<input type="checkbox"/> Scope <input type="checkbox"/> Schedule <input type="checkbox"/> Resources <input type="checkbox"/> Budget
Change Description	< Describe change and justification >
Change Category	1-Fix, 2-Expedite, 3-Required, 4-Requested
Analysis Category	1-Large (> 40 hours), 2-Medium (20-40 hours), 3-Small (< 20 hours)
Priority Category	1 -Critical, required prior to implementation 2 -Required prior to implementation 3 -Required post implementation 4 -Wanted post implementation
Cost Impact	< \$ >
Schedule Impact	< days >
Required for/by (event / date)	

PART 2: IMPACT ANALYSIS (TO BE COMPLETED BY REQUESTER AND LACL POLICY DIRECTOR)			
Impact to Team or Project Plan	Impact	If Yes, describe impact:	Effort Req'd
< Team or plan task >	Y / N		<Days, Weeks or Months >
< Team or plan task >	Y / N		
< Team or plan task >	Y / N		
< Team or plan task >	Y / N		
Analyzed by		Date	MM/DD/YY

PART 3: APPROVAL (TO BE COMPLETED BY AUTHORIZED STAKEHOLDER AND LACL EXECUTIVE DIRECTOR)				
CR Approved	Y / N	Date:	MM/DD/YY	<Why approved or rejected?>
Priority Assigned	<input checked="" type="checkbox"/>	Low	<input type="checkbox"/>	Medium
			<input type="checkbox"/>	High
Authorized Stakeholder				
Project Manager Signature				

PART 4: IMPLEMENTATION (TO BE COMPLETED BY LACL POLICY DIRECTOR)				
Task ID & Description				
Task Completed	Y / N	Date	MM/DD/YY	<Comments>
Change Request Closed	Y / N	Date	MM/DD/YY	<Comments>
Requester Notified	Y / N	Date	MM/DD/YY	<Comments>



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Los Angeles Cyber Lab Information Sharing Framework

January 3, 2020



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Revision Updates

Item	Version	Description	Date
1	1.0	Initial Publication	January 3, 2020
2	2.0	Minor updates, TISP Maturity Model	January 14, 2020

Table of Contents

1	EXECUTIVE SUMMARY	9
2	INTRODUCTION	9
3	INFORMATION SHARING CONCEPTS	9
3.1	INFORMATION SHARING FRAMEWORK.....	11
3.2	APPLYING SHARED INFORMATION.....	12
3.3	FUNCTIONAL COMPONENT DESCRIPTIONS.....	13
3.4	ESTABLISHING INFORMATION SHARING GOALS.....	16
4	INFORMATION AN ISAO MAY WANT TO SHARE	18
4.1	KEY FACTORS	18
4.2	INDICATORS	19
4.3	VULNERABILITY INFORMATION.....	21
4.4	COURSES OF ACTION	21
4.5	INCIDENTS	22
4.6	THREAT ACTORS	23
4.7	TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)	24
4.8	CAMPAIGNS	25
4.9	ANALYTICAL REPORTS	25
4.10	THREAT INTELLIGENCE REPORTS	26
4.11	SECURITY ADVISORIES AND ALERTS.....	26
4.12	OPERATIONAL PRACTICES	27
5	STEPS TO CONSIDER WHEN SHARING INFORMATION.....	27
6	INFORMATION ANALYSIS.....	29
6.1	ANALYTICAL CONSIDERATIONS	31
6.2	ANALYSIS SERVICES.....	32
7	ARCHITECTURAL CONSIDERATIONS	33
7.1	SHARING MODELS	33
7.1.1	PEER-TO-PEER.....	33
7.1.2	HUB-AND-SPOKE (LACL).....	34
7.1.3	HYBRID APPROACH.....	34
7.2	SHARING METHODS	35
7.2.1	PUBLISH-SUBSCRIBE (LACL).....	35
7.2.2	CROWDSOURCING (LACL).....	36
7.3	SHARING MECHANISMS.....	36
8	OPERATIONAL CONSIDERATIONS.....	38
9	INFORMATION PRIVACY.....	41
9.1	CORE PRINCIPLES.....	42

10	INFORMATION SECURITY	42
	APPENDIX A ADDITIONAL RESOURCES.....	44
	APPENDIX B GLOSSARY	47
	APPENDIX C ACRONYMS.....	51

Figures

Figure 1. Context for Information Sharing.....	11
Figure 2. Conceptual Information Sharing Framework.....	12
Figure 3. Applying Information to Cybersecurity Risks.....	13
Figure 4. Framework for Delivering Intelligence.....	29
Figure 5. Sharing Models.....	33

Tables

Table 1. LACL TISP Maturity Model.....	10
Table 2. Functional Categories and Information Sharing Capabilities.....	14
Table 3. Sharing Mechanisms to Consider	37

1 EXECUTIVE SUMMARY

The purpose of this document is to provide an introduction to Los Angeles Cyber Lab's (LACL) cybersecurity information sharing. The intent is to provide a foundation for information sharing as it relates to Information Sharing and Analysis Organizations (ISAOs). This document describes a conceptual framework for information sharing, information sharing concepts, the types of cybersecurity information an organization may want to share, ways an organization can facilitate information sharing, as well as privacy and security concerns to be considered. This framework is adapted from the ISAO-SO foundational documents.

Throughout the document, the terms *cybersecurity information sharing*, *cyber threat sharing*, and *information sharing* are used interchangeably.

2 INTRODUCTION

Organizations addressing cybersecurity risks can find value by participating in what has generally been characterized as *information sharing*. A benefit of information sharing is the opportunity to leverage knowledge, awareness, understanding and experiences across a broader community.

Participation in information sharing efforts is primarily driven by interest in improving cybersecurity, either personal, organizational, or both. Those responsible for managing cybersecurity risks and taking actions to deal with them may wish to participate in ad hoc, defined, or institutionalized information sharing activities to better understand the environment in which they are operating and to contribute to collective interests.

Information sharing does not solve all cybersecurity challenges an organization faces but can prepare an organization to better understand the threat environment affecting it and others. Learning from others' experiences and understanding what others have found to be effective cybersecurity measures can be an additional benefit as organizations build situational awareness, make decisions, take actions and allocate resources in similar situations.

This document provides an introduction to overall effort of the LACL information sharing initiative with respect to threat intelligence and takes advantage of the ISAO Standards Organization foundational guidance.

3 INFORMATION SHARING CONCEPTS

Public and private organizations manage cyber-related risks based on the technology they employ and the information they protect. Managing risk entails understanding their own internal environment and the environment in which they are operating (situational awareness), determining directions to pursue (decision-making), and detailing efforts (actions) to undertake. These are activities an organization executes daily.

The LACL provides a variety of information to its members in order to help

them manage their cyber-related risk. This information can be logically grouped into two dimensions: **Purpose & Time and Application** of resources.

Purpose covers three areas, namely;

- **Situational Awareness**—information providing an awareness of the broader threat landscape.
- **Decision Making**—information relevant to a particular organization’s needs and enabling more effective security management.
- **Action**—information directly supporting the implementation of a particular measure to improve security.

Time and Application of resources begins with information operationally relevant to security and builds upon it. This dimension covers three areas:

- **Immediate**—information relating to actions to defend against or respond to new threats, vulnerabilities, or incidents.
- **Tactical**—information relating to decisions on how to best deploy an organization’s existing resources against the change in the threat environment.
- **Strategic**—information relating to making plans and decisions on efforts and resources needed to address emerging or future threat environments.

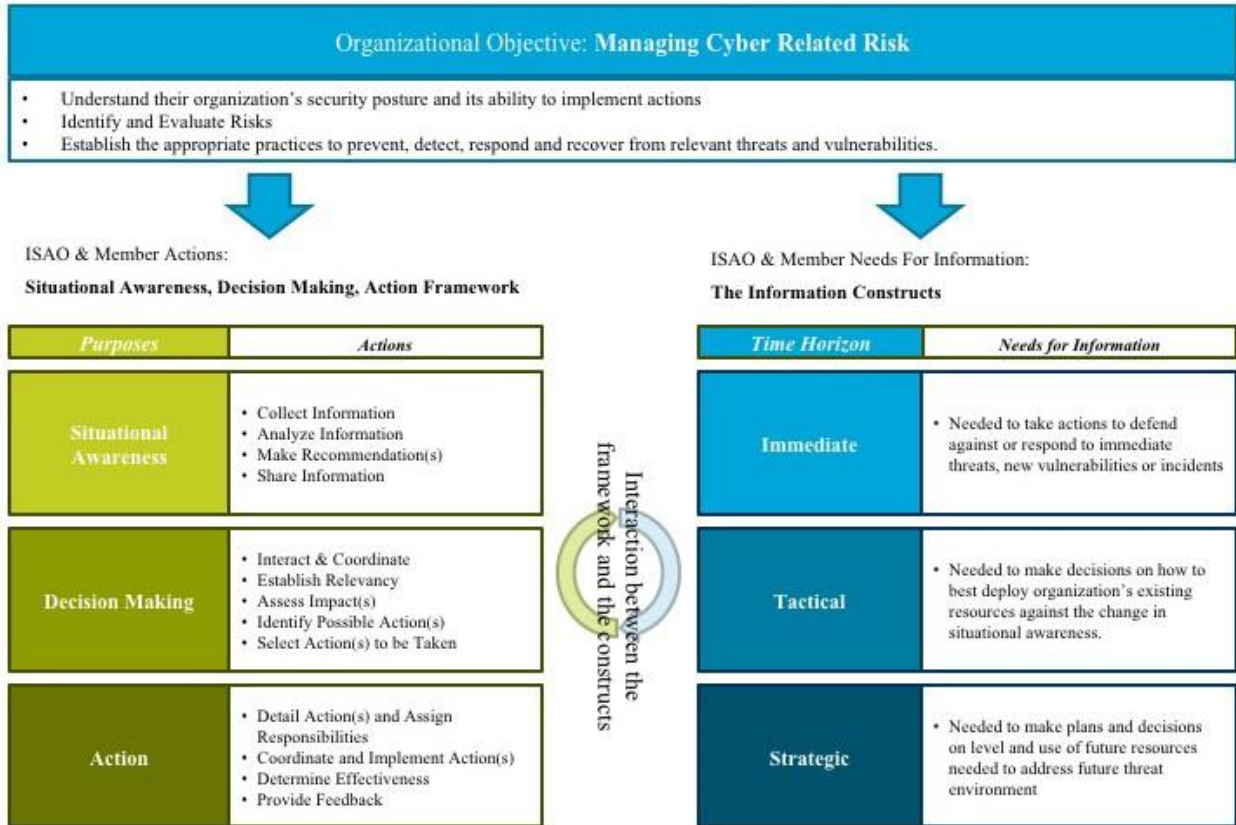
Table 1: LACL TISP Maturity Model

Threat Intelligence Sharing Platform (TISP) Maturity Model			
	Basic <-----> Advanced		
Level	Access	Integration	Sharing
What	Access to threat intelligence data through the TISP (TruSTAR platform web application).	TISP access and threat intelligence data integrating with security tools	Full security tool integration, including aggregating and sharing IOC to the TISP
	Indicators of Compromise (IOC)	IOCs & Research Enrichment	IOC Reports & Case Enrichment
Benefit	Provides additional security insight. Users can see shared threat data, perform research, see trends etc.	Integrated threat data to make analysts and tools more accurate and efficient.	IOC's from the TISP are integrated into security tools, organizations share IOC into the TISP.
	Benefit to Member	Benefit to Community	Benefit to All
Sharing	Can manually upload reports (e.g. CSV)	Can manually upload reports. Limited Automated Sharing with existing integrations.	Automated Sharing between tools and TISP via API or STIX/TAXII
Who	Smaller organizations that lack the infrastructure for integration of sharing.	Medium organization with some security tools and limited staff.	Organizations with dedicated security staff and mature security infrastructure.
Role	Researcher, Analysts, Engineers, Investigators		
		Security Engineers	
Requirements	TISP account and web browser	TISP account & Tools capable of ingesting threat intelligence	Organizational capability to identify suspicious and malicious traffic and the ability to share data

Figure 1 depicts an information construct and a framework for interacting to align the ISAO and member efforts with the information intended to help organizations manage cyber-related risks.

Figure 1. Context for Information Sharing

ISAOs and member organizations operate in overall context of managing cyber risks; taking a risk based approach, where defensives are aligned to the risks the organization faces



3.1 INFORMATION SHARING FRAMEWORK

Using the two dimensions previously discussed, the Information Sharing Framework depicted in Figure 2 presents a context for high-level sharing interactions of the LACL sharing community.

Figure 2. Information Sharing Framework

	Situational Awareness	Decision Making	Action
Immediate <i>(Taking actions against immediate threats/new vulnerabilities/incidents)</i>	ISAO Action: <ul style="list-style-type: none"> •Collect information on threats, vulnerabilities, and incidents •Analyze information and make recommendations •Share information with members Member Org. Action: <ul style="list-style-type: none"> •Collect information and share with ISAO •Receive information from ISAO 	ISAO Action: <ul style="list-style-type: none"> •Assess potential impact for all members •Response to member queries •Coordination between members •Propose/assess possible actions Member Org. Action: <ul style="list-style-type: none"> •Establish relevancy •Assess impact •Review potential actions •Select actions to take 	ISAO Action: <ul style="list-style-type: none"> •Support response to threats •Coordinate joint response •Assess impact of actions Member Org. Action: <ul style="list-style-type: none"> •Respond to shared information
Tactical <i>(Using existing resources to protect against changes in situational awareness)</i>	ISAO Action: <ul style="list-style-type: none"> •Create overall view of current situational awareness and defensive measure practices •Consolidate, enrich, analyze information and make recommendations •Share information with members Member Org. Action: <ul style="list-style-type: none"> •Receive information from ISAO •Interact with other members •Share defensive measures 	ISAO Action: <ul style="list-style-type: none"> •Assess potential impact for all or specific members •Response to member queries •Coordination between members •Propose/assess possible actions Member Org. Action: <ul style="list-style-type: none"> •Establish relevancy •Assess impact of existing defensive measures against threat updates and situational awareness changes •Review potential actions •Select actions to take 	ISAO Action: <ul style="list-style-type: none"> •Support implementation •Coordinate joint actions •Assess impact of actions Member Org. Action: <ul style="list-style-type: none"> •Implement decided course of action •Review and adjust
Strategic <i>(Changing resources based on future threat environment)</i>	ISAO Action: <ul style="list-style-type: none"> •Trend analysis on information •Publish in-depth analysis •Share information with members Member Org. Action: <ul style="list-style-type: none"> •Receive information from ISAO •Interact with other members •Share strategies and plans 	ISAO Action: <ul style="list-style-type: none"> •Response to member queries •Coordination between members •Propose/assess possible actions Member Org. Action: <ul style="list-style-type: none"> •Assess existing resources against future threat environment •Benchmark against peers •Set strategy/plans 	ISAO Action: <ul style="list-style-type: none"> •Support implementations •Coordinate joint strategies •Assess impact of actions Member Org. Action: <ul style="list-style-type: none"> •Implement selected strategy •Review and adjust decisions and actions

The framework illustrates the benefits the LACL can provide members by meeting their needs through information sharing efforts in the context of what organizations are doing on a daily basis to manage their cyber-related risks.

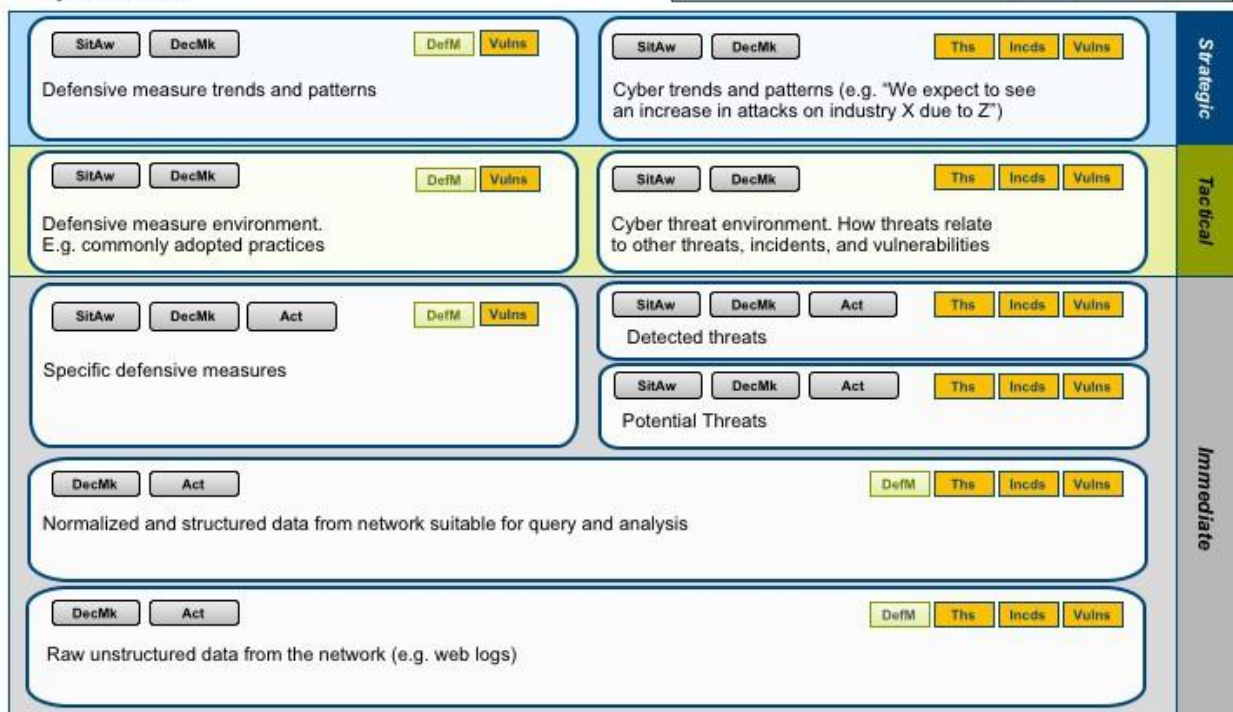
3.2 APPLYING SHARED INFORMATION

Figure 3 depicts, at a high level, how specific types of information--namely, threats, vulnerabilities and incidents--can be applied to affect situational awareness, decision-making, and actions focused on managing and mitigating cyber-related risks.

Further, progressive levels of analysis can turn raw, unstructured data into valuable knowledge and additional information from the operating environment. Armed with this knowledge and information, organizations can then prioritize efforts to defend against or respond to the most prevalent threats.

Figure 3. Applying Information to Cybersecurity Risks

Data is needed for immediate response to threats, making tactical decisions, and strategic planning. Information supports situational awareness, decision making, and taking action. The depiction below shows types of information and where it may be used.



3.3 FUNCTIONAL COMPONENT DESCRIPTIONS

Another way of describing the types of information an ISAO may consider sharing is to categorize the broad functions the ISAO provides its members. These functional categories can be broken down into components and aligned with supporting capabilities needed to support them.

In Table 2, these cross-cutting categories are decomposed into sub-categories to identify the more specific information capabilities needed to support those categories. The LACL Threat Intelligence Sharing Platform (TISP) provides member and partners the ability to sharing information as prescribed in Table 2.

Personal or organizational interests of the members participating in an ISAO generally value the following:

- New knowledge for a better understanding of the threat and vulnerability environment in which they are operating
- Recommendations for dealing with specific threats and vulnerabilities
- Receipt of situational alerts that may affect their security posture

- Validation of their understanding of a current situation or incident
- Additional information which may improve their current understanding of threats, vulnerabilities, and/or incidents
- Knowledge of the actions being taken by others
- Coordination of collective actions
- Feedback on the effectiveness of actions being taken by others individually or collectively

These personal or organizational interests can be used to describe four functional component categories that together make up the broad tactical and strategic efforts an ISAO can perform:

- Threat landscape awareness
- Response measures
- Coordination
- Trend and pattern analysis

These broad categories, as shown below, can be further decomposed to more specific functional elements and information sharing capabilities to support the personal or organizational interests of those participating in or working with an ISAO.

Table 2 describes these categories and sub-categories and identifies information sharing capabilities supporting them.

Table 2. Functional Categories and Information Sharing Capabilities

Functional Category or Sub category	Description	Information Sharing Capability
Threat landscape awareness	Know what's going on related to cybersecurity or other issues of interest to the LACL	
+ Collect information: — General	+ Obtain threat, vulnerability, and incident information from ISAO participants and other sources for information of interest	+ Anonymous and attributable submissions + Email and Listserve + Calls + Meetings + Secure portal submissions + Automation feeds + Direct cybersecurity partner feeds + Traffic Light Protocol (TLP) labeling implementation
+ Focus on community of interest	+ As necessary, encourage community of interest participation to build deeper trust relationships	+ Similar capabilities as above that can be segregated and tailored for community of interest participants

Functional Category or Sub category	Description	Information Sharing Capability
— Make appropriate information available	+ Distribute or make information available in accordance with TLP procedures and labelling	+ Distribution through appropriate communication channels (portal access, email, automation platforms, etc.)
— Analyze collected information	+ Review, de-conflict, validate, sanitize, and analyze collected information	+ Analysts and analysts' tools
	+ Conduct research or intelligence to alert the members of evolving or existing threats, incidents, and vulnerabilities	
— Develop alerts	+ Identify changes in situational awareness that may be of interest to ISAO participants and others	+ Communication mechanisms for levels of alert criticality + Multiple mechanisms for highest level of alerts
Response measures	Establish operational or procedural measures to mitigate the utility or deny the effectiveness of vulnerabilities or exploits to infrastructure, operations, or systems	
+ Distribute alerts and rapid notification	+ Provide developed alerts and notifications to appropriate participants or partners	+ Communication mechanisms for levels of alert criticality + Multiple and diverse mechanisms for highest level of alerts
+ Develop countermeasures: — Immediate — Long-term	+ Develop, in collaboration with participants and partners, countermeasures to mitigate the risks of new threats or vulnerabilities + Focus on immediate and then longer term measures	+ Conferencing and networking collaboration mechanisms for both technical experts and participants + Access to capabilities that provide searchable topic analysis for participants
+ Identify “best” and “good” practice recommendations	+ Based on interests of participants, make recommendations for “best” and “good” practices to mitigate and respond to cybersecurity and other relevant risks and incidents	+ Conferencing, networking, and forums for collaboration among technical experts and participants + Surveying capabilities + Publishing and providing references and a repository for availability of recommendations to participants + Access to capabilities that provide searchable topic analysis for participants
+ Determine effectiveness	+ Develop metrics and perform surveys to continually measure the effectiveness and satisfaction of participants with the services being provided	+ Participant survey capabilities
Coordination	Synchronize and integrate activities to ensure the pursuit of the shared objectives established by the ISAO.	
+ Establish coordination processes and capabilities	+ Policy and procedures established for assessing the need for coordination among members with shared interests to discuss and coordinate	+ Communication/network mechanism for a leadership group (identified sub-group) to make a decision to activate coordination

Functional Category or Sub category	Description	Information Sharing Capability
+ Activate coordination	+ Issue notification for an “emergency” call for coordination	+ Established diverse communication capability to initiate an “Emergency Call”
+ Establish coordination actions and efforts	+ Establish “playbooks” for various situations where coordination among participants is required	+ For ongoing incidents of specified severity implement conferencing capabilities to determine the status, countermeasures, and response information related to an ongoing situation
+ Assess coordination efforts	+ During and following coordination events continually assess decisions and actions taken	+ Survey capabilities. + Conferencing capabilities
Trend and Pattern Analysis	Collect information and attempt to spot a pattern or trend derived from the information of interest to the ISAO participants	
+ Retain historical information	+ Maintain history of submissions, analysis and decisions in a secure database	+ Secure operational database and software with appropriate access controls to segregate and deal with varied sensitivity of information
+ Perform strategic analysis: — Identify trends, discontinuities, or patterns of activity — Determine threat actors and motivations	+ Analyze the ISAO historical information along with other information to provide value-added insights on trends and new activity of significance to participants’ interests	+ Analysts and analysts’ tools + External collaboration mechanisms for analysts to engage other experts
+ Publish analysis and recommendations	+ Regularly communicate with ISAO participants and others based on ISAO policy and procedures	+ Communication channels and networking events for members to receive analysis + Access to capabilities that provide searchable topic analysis for participants

3.4 ESTABLISHING INFORMATION SHARING GOALS

The goal of the LA Cyber Lab (IS-ISAO) is to create a group of regionally based organizations sharing threat intelligence to collectively provide the greater Los Angeles business community with awareness of and actionable data to protect against cybersecurity attacks and cybercrime.

By creating a group of organizations with a common interest in sharing threat intelligence the LACL will have established a collective defense capability for the community. These public-private sector partnerships are the key to collaboration and the future of economic protection.

The LACL along with its partners and members considers the following questions as guidelines assisting the sharing community to achieve its goals.

- How will the information shared help members achieve their cybersecurity objectives? *Each Partner or Member will have their own objectives in cybersecurity. The LACL TISP provides a common place to exchange information and share threats as they are seen within organizations.*

- Which types of information does the LACL membership want that conveys relevant situational awareness? *Indicators of Compromise (IOCs)*
- Will the LACL provide raw data, analysis, or both to assist members in their tactical decision-making efforts? *The LACL TISP provides raw data which may be analyzed or not and is useful in various ways depending upon the security architecture of the organization.*
- Will members expect recommendations, related to action, including defensive measures, best practices, and/or procedures for incident coordination? *No, LACL is not advising Partners or Members as to how they should secure their networks and data. LACL will occasionally provide best practices for consideration and implementation as those practices become available.*
- Will the LACL provide analysis of a strategic nature, including related to things such as trends, threat actor targeting and threat actor motivations? *LACL provides trends on threat data within the TISP.*
- How will information sharing, mitigation, and analytic plans of the LACL relate to each other? *The LACL sharing plan is simple: data within the TISP is shared to all Partners and Members. LACL does not have mitigation or analytic plans. Analytics are incorporated into the TISP but not formally designated as a separate plan.*
- How will information sharing and trust be cultivated between the LACL and its members? *Trust is established over time and through the availability of quality data.*
- How will the LACL information sharing policy guide expectations and obligations? *The LACL holds regular meetings with its Advisory Board and solicits feedback from members. Together this collective feedback is used to guide the LACL's information sharing strategies and policies.*
- Are there specific types of information the LACL members want to share with each other? *Yes, generally speaking member of similar sectors have an interest in sharing near real-time data as a means of cyber defense.*
- What information do LACL members need to assist them in tactical decision making? *LACL members are provided the IOCs in their raw form. The IOCs can be leveraged in many ways to defend against attack, but the member must decide when and how to implement the intelligence.*
- What information sharing capabilities are achievable and sustainable within the resources of the LACL? *The LACL TISP is capable of providing a repository of IOC data for the region.*
- Could an existing ISAO fulfill the information needs being considered? *No, there are no other regionally based ISAOs providing threat intelligence in the Los Angeles area.*

¹ Consult ISAO 100-2, *Guidelines for Establishing an ISAO.*

4 INFORMATION AN ISAO MAY WANT TO SHARE

LACL and its members may wish to share information across ISAOs, with other ISAO members, and with various government entities. Using consistent standardized terminology, frameworks and data formats helps facilitate these cross-organizational information exchanges. Additionally, leveraging a consistent framework enables integration and analysis of threat information from disparate sources that may have different focuses, such as integrating indicator information with threat actor or incident information.

4.1 KEY FACTORS

There are several key factors to consider when evaluating the types of cybersecurity information an ISAO may want to share. In addition, there are various ways to share information, including network-to-network, machine-to-machine, human-to-human, or human-to-machine. Machine-to-machine sharing requires structured information and should use standardized data formats and protocols to enable interoperability. Human-to-human sharing can be most effective when using a common framework for describing cybersecurity information. This helps to facilitate a shared understanding among members, but the information may naturally be less structured than what is required for machine-to-machine sharing.

LACL utilizes a restful-API and STIX/TAXII protocols as a primary means to sharing information which links members to the TISP. LACL maintains a list of members and provides an alternative to machine-to-machine sharing when appropriate.

The Structured Threat Information eXpression (STIX)² language is used below to describe the types of information an ISAO may want to share. STIX terminology provides the depiction needed to convey core cyber threat concepts foundational to cybersecurity information sharing.

For automation-based exchanges to work effectively, established technical standards need to be used. There are various exchange languages used for automating the exchange of structured cybersecurity threat information. Efforts through the years have tried to settle on a single format for sharing cyber threat intelligence. Most, however, were focused within a specific area, such as incident response. The Incident Object Description Exchange Format³ is one example of a focused approach.

²See <https://stixproject.github.io/data-model/>

³See <https://www.ietf.org/rfc/rfc5070.txt>

The STIX language is commonly used for capturing and sharing cyber threat information. STIX is a structured, machine-readable format designed specifically to convey cyber threat information, addressing the complete cyber threat. STIX defines a framework for expressing and sharing cyber threat information in a consistent manner. This framework consists of a set of core attributes that include:

threat actors, campaigns, incidents, indicators, courses of actions, observables, and exploit targets, and tactics, techniques and procedures (TTPs), as well as the set of relationships among those core attributes.

The STIX framework is broad enough to support the full scope of cyber threat intelligence use cases and flexible enough to allow users or communities to define the subset of the STIX language they need for their specific use cases. STIX enables users to define profiles⁴ for specific cyber threat sharing needs. These profiles document which subset of the STIX language will be used during sharing. When using STIX, it may be helpful for ISAOs to develop or leverage well-known STIX profiles to document the specific data elements to be exchanged in a given scenario. STIX is in use by threat intelligence teams from government and industry, security product and service vendors, Information Sharing and Analysis Centers (ISACs), and major Computer Emergency Response Teams (CERTs).

LACL TISP is based on TruSTAR's platform which performs as a storage and collection location for ISAO threat intelligence. The TISP brings in various threat feeds into an integrated view allowing members to export the feed in various formats (e.g. JSON, CSV, etc.) While STIX is one means of sharing, LACL experience has shown that ISAO members prefer to access data directly in the TISP. Yet, for those security organizations which are STIX compliant and desire to utilize this protocol, LACL TISP creates a stash for the member to easily integrate with their security stack.

The following sections describe commonly shared cyber threat information an ISAO may wish to share. When applicable, these sections have been aligned with the terminology and definitions used in STIX to capitalize on that work.

4.2 INDICATORS

Indicators convey specific patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cybersecurity context and are used for detecting activity of interest. Indicators are widely shared today, with examples ranging from malicious file hashes to command and control IP addresses, phishing e-mails, and other types.

Effective indicator sharing includes contextual information to allow downstream consumers to determine whether an indicator is relevant to their organization, how to handle the indicator, what TTP is indicated, the valid time window of the indicator, and related incidents, threat actors, and campaigns.

The following fields are commonly shared:

- Title
- Description
- Pattern—the machine readable pattern
- Confidence—the level of confidence in the indicator
- Indicated TTP
- Valid time position—the time window for which the indicator is valid

Indicator sharing is more efficient via machine-to-machine information exchanges. One example of automated indicator sharing is the Department of Homeland Security (DHS)–operated Automated Indicator Sharing (AIS) initiative to enable cyber threat sharing among the federal government departments and agencies and the private sector.⁵ This initiative uses STIX and Trusted Automated eXchange of Indicator Information (TAXII)⁶ for the automated exchange of cyber threat information. TAXII defines a standardized set of services to enable the exchange. AIS has defined a profile of the STIX language for indicator exchange. The AIS STIX profile describes the specific data elements of the STIX language used for AIS cyber threat sharing. The profile provides a useful starting point for basic cyber threat indicator sharing—whether automated or manual—and can be easily leveraged to establish a consistent approach to sharing indicators within and among ISAOs.

Indicators are often generated through malware analysis, incident response, and endpoint and network monitoring. As such, indicator information frequently comes from a variety of sources including ISACs, CERTs, security product and service vendors, organization-specific security teams, and open source reporting. These various sources of indicator information drive the need to convey contextual information along with the shared indicators. *A common challenge to indicator sharing today is simply determining which indicators are relevant and useful in discovering intrusions into the environment.* LALC recommends sharing only information which is known to be an identified threat which improves the fidelity of the threat information as a whole.

Indicator reports may also include indicator sighting information. This reports a given indicator matched or was seen within some sector or even a specific organization. In aggregate this sighting information can assist in understanding the prevalence of specific campaigns or threat actors, targeting information, and more. This aggregate sighting information is widely seen as a low-cost and low-risk method of supporting more sophisticated cyber threat intelligence analysis. LACL TISP makes use of this feature and provides the ability for analysts to view common sightings of shared indicators.

⁴See <https://stixproject.github.io/documentation/profiles/>

4.3 VULNERABILITY INFORMATION

Vulnerability information may include details about the vulnerabilities in specific systems or infrastructure, specific application vulnerabilities, or general classes of vulnerabilities.

The following fields are commonly shared:

- Title
- Description
- Vulnerability ID—a reference to a Common Vulnerabilities and Exposures (CVE)⁷ threat or other well-known identifier
- Score—a Common Vulnerability Scoring System (CVSS)⁸ rating or similar score for the referenced vulnerability
- Affected software.

Mature software vendors routinely publish vulnerability information related to their products and services. Many governments issue vulnerability reports or security advisories to raise awareness as well. The US-CERT alerts⁹ are one example of these government advisories.

Shared vulnerability information frequently informs immediate response actions, especially when the information is related to recently discovered high-severity vulnerabilities in exposed systems. Vulnerability trends and more general classes of vulnerability information regularly inform tactical and strategic situational awareness and decision making.

⁵See <https://www.us-cert.gov/ais>

⁶See <https://taxiiproject.github.io/about/>

⁷See <https://cve.mitre.org/>

⁸See <https://www.first.org/cvss>

4.4 COURSES OF ACTION

What can you do with this information? Often LACL members will share their own thoughts as guidance for others to consider. Courses of action are specific measures to mitigate a threat or respond to an incident. They may be relatively targeted, such as blocking a specific IP address, or may encompass enterprise practices, such as using application whitelisting. As such, sharing courses of action can span the full range of immediate, tactical, and strategic information to impact decision making and actions.

The following fields are commonly shared:

- Title
- Description

- Type—Training, monitoring, patching, blocking, etc.
- Objective
- Impact
- Cost
- Efficacy
- Course of action—firewall or intrusion detection system rule, specific configuration change, etc.

Sharing courses of action can enable automated actions to mitigate threats as well as enable organizations to collaborate and arrive at the overall best course of action given a variety of options.

4.5 INCIDENTS

Incident information is specific information related to or discovered while investigating or responding to a cybersecurity incident. The amount and level of detail included in shared incident information varies widely depending upon the intended use of the shared information and sensitivities related to financial, reputational, or other concerns. LACL does not automatically share sensitive or incident information, members may share this type of information at their discretion.

The following fields are commonly shared:

- Title
- Description
- Category—improper usage, scanning or probing, denial of service, etc.
- Reporter—the reporting source of the incident description
- Victim—details about the victim of the incident
- Affected assets—describes the assets that were affected during the incident
- Impact assessment—describes the impact of the incident
- Related indicators—IP addresses, file hashes, domains, etc.
- Leveraged TTPs—attack techniques, malware, tools, etc.
- Attributed threat actors
- Intended effect—theft, disruption, account take over, fraud, etc.
- Related incidents
- Courses of action

The U.S. government publishes well-known guides for reporting incident information and incident handling, such as the following:

- *The Federal Incident Notification Guidelines* document provides guidance for submitting incident notifications to the United States Computer Emergency Readiness Team (US-CERT).¹⁰
- The National Institute of Standards and Technology (NIST) published *Special Publication 800-61, Computer Security Incident Handling Guide*, a useful resource on incident handling.¹¹

These are excellent references for the type of information commonly shared to support incident response and analysis.

Sharing incident information can enable or support a wide variety of use cases, each with different incident information requirements. Incident information sharing can enable large scale analysis to uncover adversary trending across the cybersecurity ecosystem. Detailed incident information sharing may enable advanced cyber threat intelligence analysis related to specific threat actors and

⁹See <https://www.us-cert.gov/ncas/alerts>

¹⁰See <https://www.us-cert.gov/incident-notification-guidelines>

¹¹See <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

campaigns. Incident information sharing can also help uncover key indicators of malicious activity to inform partner cyber defenses.

4.6 THREAT ACTORS

Threat actor information describes malicious actors that may represent a cyber threat or have been historically observed or related to known incidents.

The following fields are commonly shared:

- Names—short names or aliases used for the threat actor
- Description—a textual description of the threat actor
- Identity—Information that may identify the actor
- Type—hacker, hacktivist, state actor, electronic crime actor, insider threat, etc.
- Motivation—political, economic or financial, ideological, military, etc.
- Sophistication—novice, practitioner, expert, innovator, etc.
- Intended effects—military, economic, or political advantage, theft, destruction, disruption, etc.
- Observed TTPs—TTPs an actor has been observed to use
- Related campaigns—campaigns that have been attributed to the actor

Tracking and sharing threat actor information is critical for cyber threat intelligence analysis. This information allows organizations to develop an understanding of the threats they face as well as the specific objectives and capabilities an adversary or group is believed to have employed. Sharing threat

actor information among organizations can help all participants develop a much more comprehensive understanding of these threats.

Threat actor information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs may operate their own cyber threat analysis teams and track threat actors relevant to managing their cybersecurity risk or risk to their members.

Threat actor information is frequently more strategic in nature and used to inform situational awareness and decision making.

¹²See <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

4.7 TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

Context is the key to understanding what and how threat actors are exploiting vulnerabilities. LACL makes every effort to enrich data as it is shared to afford members the greatest ability to defend their networks and data. Tactics, techniques and procedures represent a fairly broad set of information used to describe the behavior or capabilities of a threat actor or campaign. TTPs characterize what adversaries do and how they do it. As such, TTPs encompass specific adversary behaviors, the resources leveraged, target victim information, and the vulnerabilities or weaknesses being targeted.

The following fields are commonly shared:

- Title
- Description
- Intended effect
- Behavior—specific attack patterns, malware, or exploits
- Resources—tools, infrastructure, or personas
- Victim targeting—people, organizations, information or access being targeted
- Kill chain phase
- Related TTPs

Malware samples represent one commonly shared type of TTP. Sharing malware samples can enable broad distributed analysis of the sample as well as higher-level trending of both malware and the types of organizations being targeted.

TTPs are a critical component to cyber threat intelligence analysis and they are frequently related or shared in the context of incidents to describe the TTPs detected during an incident investigation. Cyber threat indicators relate low-level observables to TTPs to give context to what defenders should look for. Campaigns and threat actors are often related to TTPs to characterize either previously observed or expected adversary capabilities.

Aggregated TTP information can enable cyber threat analysts to develop a more holistic understanding of the threat or more narrowly advance the understanding

of a specific adversary. This information may inform strategic, tactical, and immediate situational awareness, decision making, and actions.

4.8 CAMPAIGNS

Campaign information can relate information about the intended effects of an adversary or group with the tools they employ, the threat actors believed to participate, the incidents associated with the group, and other related campaigns.

The following fields are commonly shared:

- Names—short names or aliases used for the campaign
- Description
- Intended effects—Military, economic, or political advantage, theft, destruction, disruption, etc.
- Related TTPs
- Related incidents
- Associated campaigns
- Attribution (related threat actors)

Tracking and sharing campaign information is critical for threat intelligence analysis. This information allows organizations to develop an understanding of the threats they face as well as the specific objectives and capabilities an adversary or group is believed to have employed. Sharing campaign information among organizations can help all participants develop a much more comprehensive understanding of these threats.

Organizations may be reluctant to include attribution information when sharing campaign information due to its sensitive nature. Sharing campaign attribution information is not always necessary to facilitate a broader understanding of a given campaign.

Campaign information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs may operate their own cyber threat analysis teams and track campaigns relevant to managing their cybersecurity risk or risk to their members.

Campaign information is frequently more strategic in nature and used to inform situational awareness and decision making.

4.9 ANALYTICAL REPORTS

LACL TISP provides the ability to produce specific reports based upon the analyst's query. Participants who engage in analysis can find benefits in their immediate, tactical and strategic decision-making.

Common communication report types are alerts, notifications, and assessments. The following are examples of content for information analysis reporting:

- The impact of threats to core corporate functions
- Description of threat activity relative to an attack life cycle
- Trends of malicious activity as it relates to an organization's infrastructure (e.g. infrastructure most targeted, configurations most exploited, etc.)
- Effectiveness of mitigations
- Cyber threat trend reports
- Threat horizon reports
- Proactive (assessments) and reactive reporting (post-mortem to an incident)

4.10 THREAT INTELLIGENCE REPORTS

Threat intelligence reports are a broad category of cyber threat information ranging from high-level trending reports to detailed analysis of specific campaigns.

Vendors, governments, and independent organizations produce various types of reports, including open source intelligence reports. Some are targeted at specific incidents, some are predictive, while others describe the current state of the cyber threat landscape. These reports can include the full range of cyber threat intelligence providing strategic, tactical, and immediate response value. The report can include campaign, threat actor, TTP, and indicator information. Some reports are the result of several years of analysis and tracking of cyber threats.

4.11 SECURITY ADVISORIES AND ALERTS

Security advisories and alerts are published by a variety of sources, including international CERTs, governments, software and security tool vendors, ISACs, not-for-profit organizations, and security researchers. These publications vary from the rebroadcasting of important software vendor's security advisories to tailored products aimed to raise awareness of important new vulnerabilities and security issues. LACL reviews advisories and alerts for dissemination to its members and communicates this information via its membership list.

Many of the major international CERTs provide security advisories and alerts. For example, US-CERT publishes alerts about current security issues, vulnerabilities, and exploits. These alerts attempt to describe the issue, explain the impact of the issue, and offer suggested mitigations to address the issue.¹³

Sharing security advisories and alerts can provide the full range of immediate, tactical, and strategic information to impact decision making and actions.

¹³See <https://www.us-cert.gov/ncas/alerts>

4.12 OPERATIONAL PRACTICES

Sharing operational cybersecurity practices among ISAO members is an important way for organizations to collaborate and build trust, learn from each other and collect feedback as they mature their own cybersecurity practices. This type of sharing enables an organization to benefit from methods for solving a problem that other members may be using successfully. This type of information can include best or effective practices, effective architectures, effective or ineffective system configurations, manning strategies, and more. Sometimes sharing what did not work is as valuable to the ISAO membership as knowing what did. LACL continues to identify secure ways to share this type of information and promote this type of collaboration.

5 STEPS TO CONSIDER WHEN SHARING INFORMATION

The first step is to identify what information an ISAO and its members will share. The ISAO and its members should determine what information is shared and when it is shared based on the goals and mission of the ISAO and the needs and capabilities of its members and customers. Identification of what information to share is the basis on which subsequent decisions should be made.

After identifying the information to be shared, the ISAO and its members should identify sensitive data that they wish to share and the procedures for handling that data. For example, some ISAOs may choose to enable sharing without attribution, while other ISAOs may choose to require attributing shared information with a specific member. Non-attribution could make a member feel more comfortable in sharing, but knowing who is sharing the information could provide greater confidence in its quality and accuracy. Other examples could include, but are not limited to, personally identifiable information (PII), business sensitive information, or information with legal requirements for protection. ISAOs should establish the policies that they determine best meet the operational needs and legal requirements of their organization, membership, and customers. More information on sensitive data can be found in Section 8, Operational Considerations, and Section 9, Information Privacy.

Once the information to be shared and the sensitivity issues associated with it have been identified, it is important for members to agree on the mechanism and methods to be used to meet the goals of the ISAO.

LACL has considered the following:

- Provide a platform for and facilitate member sharing: [LACL TISP](#)
- Implement and manage technology that gathers information: [Use of feeds integrated into the TISP](#)
- Subscribe to a third-party service providing threat intelligence feeds: [LACL utilizes both paid and free threat feeds](#)
- Collect, aggregate, and disseminate open-source reporting: [LACL collects and incorporates information from OSINT](#)
- Collect, aggregate, and disseminate reporting from partner organizations:

LACL partners provide threat intelligence data which is disseminated to LACL members.

ISAOs can choose to share information via automation, human interaction, or a combination of the two. Sharing among members and the ISAO may be done through machine-to-machine automation. Sharing indicators in an automated fashion can enable information to be shared more rapidly, increase the volume of indicators shared, and also increase the quality of shared data. This technology is emerging and needs to be driven by organizationally established policies for automated information exchange when sharing between members and potentially other ISAOs. In most cases, an ISAO will share with members using multiple means. Human-to-human sharing can increase trust among participants, making them more willing to share. As such, there is value in both automated exchange and human exchange.

To capture the goals, principles and methods an ISAO will operate under, an ISAO and its members should develop information sharing policies guiding members in how they can use the information shared within the ISAO and among its partners. These policies should include the types of information to be shared, the appropriate methods for sharing, identification and handling of sensitive data, and safeguarding requirements. LACL data sharing consideration include the following:

- How should information shared be marked? *Members have the ability to mark information as they desire.*
- Can members externally share the information they receive from the ISAO? *Yes, information from LACL can be further shared by members.*
- Can the ISAO share the information with other partners or ISAOs? *Yes, LACL participates with other ISAOs in sharing information.*
- How should information shared over the phone or during virtual and in person meetings be handled? *Generally, LACL information is not sensitive and can be shared to any organization. In the circumstances which require grater sensitivity, LACL will set up a closed method for sharing.*
- What policies, privacy controls, and protection should an ISAO have for shared information in motion and at rest? *LACL information is cloud based with encryption for data rest. Data is protected by role based access controls via credentials which are issued and maintained by LACL.*
- Asking members to sign a non-disclosure agreement: *Not at this time.*
- Using a carefully designed process for information sharing: *LACL uses access controls for the TISP and considers additional steps when warranted.*
- Using the Traffic Light Protocol (TLP)¹⁴ or similar to ensure that sensitive information is only shared with those who are authorized to receive it: *TLP can be used by members at their discretion.*

¹⁴See <https://www.us-cert.gov/tlp>

To ensure that members share and receive information valuable to them and others, ISAOs should consider establishing periodic reevaluations of these policies to ensure member needs are continuing to being met.

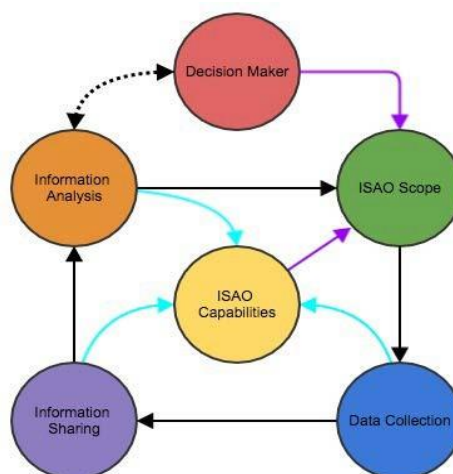
6 INFORMATION ANALYSIS

Successful information sharing and analysis depends on the production of actionable intelligence accessible and useful to participating analysts. The purpose of information analysis is to learn from and understand the data, combining context with other data, to produce information and gain insights which are not readily obvious. Information sharing and information analysis interdependence, combined with data collection and an ISAO's scope and capabilities, creates the framework for delivering intelligence to decision makers, as shown in Figure 4.

Cybersecurity information analysis involves reviewing data for signs or indications of unusual or malicious activity. The findings from the review can identify artifacts or evidence that analysts can use to link with similar threat data, helping to identify malicious TTPs, threat groups, or campaigns. ISAOs all perform some form of analysis, even if it is only the decision to share relevant information. ISAOs however, are uniquely positioned to bring together data from multiple sources and engage the expertise of their participants to produce actionable intelligence.

Information analysis involves interpretation and operational learning based on available data sources.

Figure 4. Framework for Delivering Intelligence



The first stage is the initial review of shared data. LACL has already received (collected) threat intelligence from its sources and reviews the data for potential sharing. One example might be the assessing of shared data to identify related threats across multiple organizations. In the second stage, analysts interpret relevant threat data to produce threat group, campaign summaries, or business risk assessments. LACL relies on members to contribute their assessments of the threat data in order to share with others in the ISAO. LACL utilizes IBM's IRIS analytics and X-Force Exchange to determine the severity of indicators of compromise.

Information analysis has inherent challenges. First, identifying the questions of interest to ISAO members which in the LACL's case is identifying known threats in the form of IOCs. Second, identifying the relevant data among multiple streams of data feeds and data repositories which the LACL has sought to manage through analytical review of the OSINT and federal government feeds.

LACL is reliant upon partners to share only data which is deemed valuable to other security professionals attempting to identify & block threats in their environment. Third, making analysis available, at the appropriate level, to ISAO members and helping them understand its relevance to other data, and its applicability to their organization which LACL does through the TISP.

ISAOs and its membership need to agree on the data points collected and how data will be accessed and securely stored. The ISAO can then consider their analytic approach and the types of reports which will be valuable to their members. ISAO members may have different appetites for intelligence consumption. For example, an ISAO focused on security or network operations may desire information that filters relevant data from network noise. Another ISAO may choose to engage on threat activity that occurs across multiple members. An ISAO should consider a survey of their members to understand what type of reporting is most useful and what each member can contribute to the aggregate collection. LACL has specifically identified the use case of IOC sharing as its primary function. Additionally, the LACL attempts to share enriched data regarding IOCs as it becomes available via alerting and through electronic communications.

The analytical options an ISAO may provide could include detection of first-seen or anomalous activity, identification of an exploit to a software or network vulnerability, collection of related threat activity, or attribution to an individual, criminal enterprise, or nation-state. LACL is creating a threat knowledge base which enables members to use analytic methods and share their knowledge and assessments. The knowledge base is being aggregated (crowd sourced) from partners and members who continue to enrich data within the TISP.

Analyst assessments help to better understand relevant threat information; however, the analyst's environment or visibility may introduce bias when categorizing threat or attributing threat activity to an actor. ISAOs are uniquely placed to help mitigate against this bias. By establishing a threat intelligence sharing community, the LACL TISP helps foster a culture which reduces analyst bias and provides continuous feedback through detection, peer communication,

and external confirmation.

Further considerations which the LACL may choose to implement for the enrichment of threat data include:

- Collection of data to assist in sharing trends and pattern analysis among the membership
- An anonymous member survey
- Identify and introduce collaborative tools, which members can collect aggregated metrics from each of the organizations on an agreed upon frequency
 - # of phishing attempts,
 - # of intrusion attempts,
 - # of successful intrusions,
 - # number of accounts compromised, and distributed denial of services attacks.
- Dashboards for trend analysis

6.1 ANALYTICAL CONSIDERATIONS

An ISAO offering dedicated information analyst services should be capable of securely storing data from varied data sources (both privileged and public) and leveraging analysts experienced in data review, threat interpretation, and development of intelligence assessments.

Before doing analysis, ISAOs may want to begin by helping their members take data quality measurements. The validity of trend and pattern analysis relies on accurate and relevant inputs.

If member organizations agree, an ISAO may consider utilizing sensors on member networks and report attributes back to a secure shared repository managed by the ISAO for generating reports and alerts. Some ISAOs may allow members access to the repository allowing individual members the ability to query and generate their own analytical reports.

ISAOs should consider using a common vocabulary for reporting cyber activity, which can be aggregated across ISAOs and, if they choose, with government agencies.

As ISAOs mature and aggregate data, they can look at creating baselines of normal behavior and doing predictive analytics which will identify anomalies and indicators of future actions.

Analysts ultimately communicate their assessments to decision makers.

Common communication report types are alerts, notifications or assessments. ISAOs may need to survey their members to determine the content format that works best for their decision makers.

6.2 ANALYSIS SERVICES

LACL provides a trusted environment for its participants to encourage analysts to collaborate and share relevant information. LACL works with the City of Los Angeles' Integrated Security Operations Center and the Mayor's Office of Public Safety to provide regional leadership to local municipal governments.

ISAOs perform some form of analysis, ranging from the decision to share relevant information, to full pattern and trend analysis. In addition to the items discussed below, an ISAO may produce other operationally oriented analysis products. Further, beyond these operational products, ISAOs may be in a position to provide trending analysis reporting and strategic analysis to help those who make decisions affecting their organization's future planning and resource requirements.

The following are examples of how an ISAO can support analysis:

- **Risk awareness and mitigation communications.** One of the most valued analytical contributions an ISAO can make is to promote the collaboration among ISAO participants, its analysts, and others to raise awareness and educate participants on cybersecurity risks and approaches to be considered for mitigating those risks. In some cases, the sharing of collective knowledge and collaboration among expert personnel might involve only a small number of the ISAO participants, but could result in broader communication to the ISAO participants. These "*tactical*" or operations-focused communications can provide guidance to prevent successful attacks, identify methods or procedures to mitigate specific risks, identify effective practices being applied by others, and report details from participants on their experiences and the effectiveness of actions they have taken.
- LACL continually seeks opportunities to connect members through various forums both within the TISP and in designated meetings. These communications are tailored for various audiences within the ISAO constituency (executives, managers, and operational personnel) and delivered as required and/or as a periodic communication. Communication can take the form of emails, reports, briefings (webinars), conference calls, and other networking/collaboration events among participants and others. These communications assist those responsible for making informed decisions for their organization.
- **Alert notifications.** LACL provides alerts about new, changing, or escalating cybersecurity risks or incidents. LACL alerts members and partners to urgent, crisis, or other levels of notification and helps provide information and recommendations to their members and partners on immediate actions they can take to mitigate risks.
- **Incident response coordination.** LACL does not provide incident response

to ISAO members. However, LACL does provide contacts to available resources within the community depending upon the circumstances.

7 ARCHITECTURAL CONSIDERATIONS

People share information in many ways, but information sharing can be viewed through three architectural constructs: sharing models, sharing methods, and sharing mechanisms.

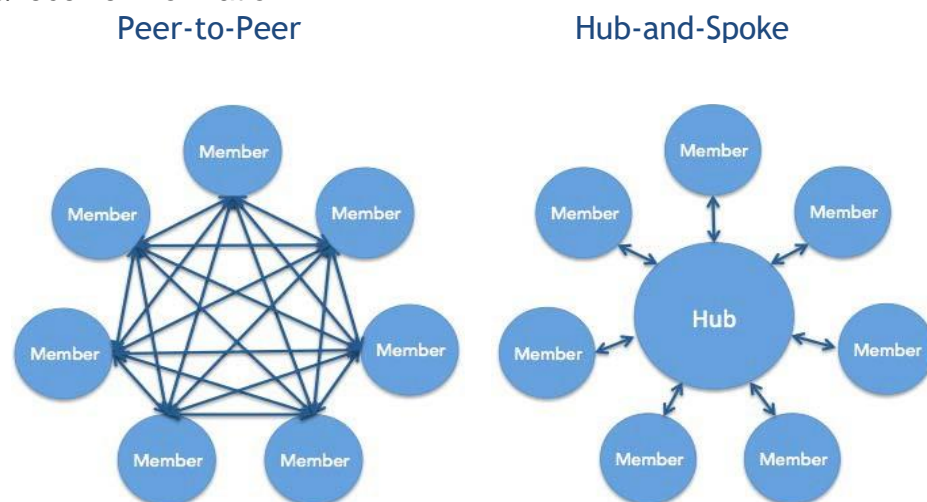
Ultimately, how models, methods, and mechanisms are implemented will vary widely based upon ISAO member needs, administrator capabilities, community goals, available technology, and the centers and dynamics of trust in a community.

ISAOs should consider what models and mechanisms could be a good fit for the context in which each operates. This can best be accomplished by comprehensively mapping all information sharing and analytic services and touch points to the delivery of sustainable member value. Doing so enables ISAOs to construct an information sharing and analytic architecture to provide long term strategic sustainment of member value and ISAO viability and maturation.

7.1 SHARING MODELS

This section details two common sharing models ISAOs may consider adopting: peer-to-peer and hub-and-spoke. They are driven primarily by the role of an information “authority” and can be blended into hybrid approaches.

Peer-to-peer and hub-and-spoke sharing models may be the most useful basic arrangements that new ISAOs can consider when getting established. LACL is a hub and spoke model where members connect to the LACL TISP and share/receive information.



7.1.1 PEER-TO-PEER

The peer-to-peer sharing model is defined generally by the ability of any member

of a community to interact and share with any other member. Peer-to-peer networks can be especially beneficial for smaller communities or when members only interact with a part of a community. They may also be especially beneficial for those whose members have asymmetrical trust relationships or share under highly dynamic conditions that often change based upon content, current threat, and so on. Members generally have a high degree of choice when determining with whom they share in the community. In this model, there is no “gatekeeper” governing event-by-event sharing, or how and what sharing occurs. That is not to say an authority (ISAO administration, for example) does not create or enforce a sharing policy, or perform other authoritative duties. Instead, members of the community generally share when, what, and with whom they see fit, based upon established ISAO policy and procedures and within the confines of the tools used.

A challenge with this model is the difficulty managing many trust relationships when community membership grows. In addition, redundant sharing of the same information may be more likely in this model, and it may lead to inefficient “churn” depending upon ISAO technology and other conditions.

7.1.2 HUB-AND-SPOKE (LACL)

Generally, the hub-and-spoke sharing model incorporates a “gatekeeper” at the center, or hub, of the community. Members share through the hub while some combination of people, process, and technology drives redistribution out to the rest of the community. This sharing model provides opportunities to centralize, formalize, or otherwise influence information exchange for the benefit of the community. The LACL administers funneling and vetting of widely disparate member and vendor threat intelligence, offloading threat analysis services from the membership to achieve economies of scale, enforcing policy, or simply playing a more central and visible role in the day-to-day activities of the ISAO. In addition, the hub is a logical place for a single “ground truth” to exist for the community, whether that has to do with policies and procedures, analysis of recent incidents or campaigns, or other areas relevant to the ISAO.

There are a few challenges to consider with this model. Dependency on the hub could lead to problems if the hub is not performing as well as it should. A high degree of trust should exist in the people, process, and technology at the hub in order for this sharing model to succeed. And regardless of the level of trust in the hub, members will always have varying degrees of trust relationships elsewhere among ISAO membership. Always funneling threat data or cyber threat indicators exclusively through the hub could inhibit the growth of personal relationships among ISAO members. Relationship building will lead to trust among the membership, and trust is arguably the primary key performance indicator for successful threat intelligence sharing.

7.1.3 HYBRID APPROACH

An ISAO can address some of the challenges of the peer-to-peer and hub-and-spoke models by forming a hybrid approach combining elements of both. This

could take virtually limitless forms, but the following are some possibilities to consider:

- Channel some kinds of threat intelligence through the hub for redistribution or analysis, based upon hub strengths and core competencies. Budget, people, technology, or geography, and how these factors impact member requirements and objectives could all help determine what obligations and tasks are a good fit for the hub.
- Leverage peer-to-peer sharing for certain kinds of intelligence, such as strategic intelligence. Peers working together to build a threat actor profile, for example, is a great way to leverage community resources, build relationships and trust among ISAO membership, and make a positive contribution back to the ISAO community. And the work product could be redistributed through the ISAO hub, combining aspects of both peer-to-peer and hub-and-spoke models.

These sharing models are high-level conceptualizations of how an ISAO can share information. Once a newly forming ISAO has a good sense of what it wants to do, selecting the appropriate sharing methods and mechanisms it employs will be critical to getting things done efficiently and effectively.

7.2 SHARING METHODS

This section details methods that can be applied to either of the above models. Sharing methods are largely directed by community requirements and concepts of operations, and also tied to the tools and technology adopted by an ISAO to enable certain kinds of sharing. LACL utilizes the following sharing methods.

7.2.1 PUBLISH–SUBSCRIBE (LACL)

A publish-subscribe method for sharing threat intelligence consists of a producer who publishes information on a regular or irregular basis, and whose publications are individually subscribed to by one or more community members. This approach can be applied in either the peer-to-peer or the hub-and-spoke sharing models. In the case of a peer-to-peer network, a producer could, for example, automate cyber threat indicator sharing into a repository from which other members pull feeds, or a producer can post to a message board/forum and subscribers receive alerts. In the case of the hub-and-spoke model, the publisher may be the ISAO hub and the producers (members) could submit to the hub for processing— usually to verify, refine, de-duplicate, or correlate with other known threat intelligence—before publishing it out to the ISAO subscriber base. The precise role of the hub can vary widely, depending upon the ISAO CONOPS and other conditions. One of the benefits of the publish-subscribe method in a hub-and-spoke model is the ability for the ISAO to aggregate and analyze information in a central location and then publish a richer, more complete picture of an incident or actor. This is very useful in a rapidly evolving environment when many participants may be sharing different observations and analyses.

7.2.2 CROWDSOURCING (LACL)

Crowdsourcing occurs when ISAO members collectively contribute to a discussion thread, an automated cyber threat sharing repository, or another system to organically transform granular threat data into more coherent threat intelligence. By virtue of participating in crowdsourcing the intelligence picture, the information is also shared with members. Like the publish-subscribe method above, crowdsourcing can take place in both peer-to-peer and hub-and-spoke networks—the key distinction being the presence of a central party directing the crowdsourcing through the hub, versus true organic freewheeling among the community. Both, of course, can be very effective. One of the benefits of crowdsourcing is that the virtual social interactions among ISAO members help to build trust and strengthen the community.

7.3 SHARING MECHANISMS

A variety of mechanisms and practices can be used to share information among an ISAO's members and partners. Table 3 depicts the types of mechanisms and practices an ISAO may want to consider as initial or additional sharing capabilities. The mechanisms and practices selected will need to be tailored to the scope, timeliness, and sensitivity of the information to be shared.

Information sharing can occur one-to-one, one-to-many, many-to-many, and many-to-one. As a result, practices an ISAO selects for communication and sharing information must reflect the overall objectives it is seeking to achieve for its members.

Due to the sensitivity of some information, methods and mechanisms used to share information must be capable, in accordance with an ISAO's policies or other authoritative restrictions, to protect and provide information to authorized members. For example, an ISAO using a Traffic Light Protocol (TLP) to handle and distribute sensitive information will need to use mechanisms providing it the capabilities to comply with its TLP policy.

If source anonymity is required, additional information sharing processes, procedures, and features will be needed by the ISAO. For that reason, the practices selected by an ISAO and its operational procedures will need to provide the operational, security, and management features necessary to meet the ISAO members' objectives.

Information sharing mechanisms should also be selected with consideration for the importance, timeliness, and criticality of receipt of information by ISAO participants. Members should be able to authenticate and trust the information comes from expected sources. In some cases, positive confirmation of receipt of information may be required to ensure delivery of time-sensitive information.

Effective ways of sharing information among ISAOs can include the use of automated information sharing platforms for primary indicators and defensive measures, as well as follow-on information from ISAO members. ISAO's may also include feeds received from threat intelligence firms to supply members with

information, or members may subscribe to these feeds and relay relevant information to the ISAO and other members. Email, chat, and social media platforms may also be used to enable collaboration and information sharing between personnel from ISAO members.

Table 3 below lists a number of sharing mechanisms to consider.

Table 3. Sharing Mechanisms to Consider

The mechanisms listed below provide general guidance on various options and their applicability:								
Description		Applicable To (* Note)				Can provide Anonymity	Access control features	Comment
		one to one	one to many	many to many	many to one			
In person meetings	Individuals physically meet with participation restricted to authorized individuals.		X	X		No	One Level: All authorized receive the information.	Access control to information can be restricted to a selected participating community through procedures.
Tele-conferencing/WebEx, etc.	Commercial conferencing and collaboration services		X	X		No/Yes	One Level: All authorized receive the information.	A central management function required to achieve anonymity but in general not anonymous. Access control to information can be restricted to a selected participating community through procedures.
Email (general)	Internet-based email	X	X	X	X	No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous. Distribution restrictions possible but difficult to manage for a large number of participants.
Email (with encrypted message)	Encrypted file or message	X	X			No/Yes	Access to information based on	Use of end-to-end encryption mechanisms, e.g. S/MIME, PGP, etc.
Email - List servers	Services for managing email lists		X	X		No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous.
Messaging Services (Short, Enhanced and Multi-media)	Carrier and vendor based services	X	X			No	Distribution can be restricted	Examples, Slack, HipChat, etc. Challenge-reply authentication can prevent spoofing.
Peer-to-Peer Networks	Characterized as a server-less network.			X		No	Distribution can be restricted	Security policies should be implemented to define what types of P2P software is acceptable and what information can be shared through them due to various risks.

The mechanisms listed below provide general guidance on various options and their applicability:								
Description		Applicable To (* Note)				Can provide Anonymity	Access control features	Comment
		one to one	one to many	many to many	many to one			
Website (Public)	All pages available at the sites URL		X			No/Yes	No restrictions	Central management trusted to be responsible for assuring posted information is anonymous.
Website (Private)	Selected pages at website require access credentials		X			No/Yes	One Level: Those with website access credential	Central management trusted to be responsible for assuring posted information is anonymous.
Secure Portal	Electronic gateway to a collection of digital files, services, and information, accessible over the Internet through a web browser. A client-server based system with multi-levels of access control to searchable databases.		X	X	X	No/Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	Central management enforces authorization and rules-based access control policies. Anonymity achieved through an anonymous access credential distribution process and posting/review by portal management policies and procedures.
Automated Mechanisms	Structured representations of cyber threat information automatically shared among trusted partners and communities in a machine processing structure.	X	X	X	X	Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	An example is STIX™ (Structured Threat Information eXpression) language < https://www.mitre.org/sites/default/files/publications/stix.pdf >
Notification Services	Notification Services generate and send messages to users or other applications that have subscribed to the service.	X	X			No	Multi-levels of access control based on authorized access policies and authorized credentials.	Notifications may be by e-mail, telephone, fax, text messages, etc.
* Note:	One-to-One	One sender and One Receiver						
	One-to-Many	One Sender and Many Receivers						
	Many-to-One	Many Senders and One Receiver						
	Many-to-Many	Many Senders and Many Receivers						

8 OPERATIONAL CONSIDERATIONS

The trusted relationships essential to an effective ISAO are best achieved when organizations embrace a culture of operational security among their members, partners, and those with whom they share information. This culture is enabled through well-designed ISAO operational policies, procedures, awareness, and good practices.

LACL's operational security efforts include the following considerations:

- Establishing the criteria and vetting process for those eligible to participate in the ISAO: LACL allows membership and participation from legally established entities, basic vetting occurs during membership request when the url of the organization is verified to exist.
- Examining the full range of the sensitive information an ISAO will be handling and communicating, and then using a risk-based assessment to develop the ISAO's operating rules,¹⁵ information policies, and controls to be implemented across the ISAO and for members when interacting with the ISAO. LACL has established policies and procedures for the IS-ISAO. The majority of these documents are internal to the intellectual property, governance and administration of the LACL.
- Defining policies that address any identification of membership, the ownership of the information shared with the ISAO, the use of the information shared, and the sharing of information among members and with others, along with any analytic product developed by the ISAO. To implement these policies, the agreed upon controls and practices to be exercised by members should be documented and be a condition for participation in the ISAO. LACL TISP participation is voluntary and information shared therein is considered the property of LACL. LACL members are expected to observe constraints on information which they receive if specifically called for by the sharing member.
- Specifying how information is to be provided to the ISAO and its members along with any review processes that may be implemented to protect the confidentiality and privacy of the content. LACL provides information three ways: via email, in person and via TISP access.
- Establishing procedures for expediting and prioritizing the timely sharing of information, allowing members to achieve the greatest value and to meet any immediate threat that could be posed by the attacks. LACL does not inhibit the timely sharing of information. As information is published to the TISP it become immediately available.
- Defining the labeling and handling procedures for the range of sensitive information to be handled within the ISAO and among members which could include using the Traffic Light Protocol (TLP)¹⁶ approach currently used by ISACs and others for these purposes. Members are required to predetermine the TLP level of their information prior to publishing it to the TISP. TISP data is TLP White by default unless otherwise marked.
- Specifying procedures and practices where anonymity of information sources will enhance the sharing and trust among members and maintaining them in the operations of the ISAO. In practice there will be times when the owner of the information can decide that anonymity is not necessary or practical, and procedures should accommodate an information owner's prerogative. LACL does not share which members published information or what information was published by the member. Each member has a segmented area within the TISP to participate with the LACL. LACL information is shared and

published by the LACL without attribution of any member.

- The leadership/management of an ISAO should ensure there is an active and periodic awareness effort to keep members informed of the expected code of conduct and their responsibilities in accordance with the ISAO's security and privacy policies. Any changes made should be fully vetted with and promulgated to participants. LACL internally manages policy enforcement and communicates policy changes to its membership as needed and on a periodic basis.
- Developing specific operating rules for automation capabilities for real-time or near-real time information sharing, if used by the ISAO, because of the critical impacts (both positive and negative) such capabilities can have on an ISAO or those participating in the automated sharing of information. LACL maintains overall control of member access to the TISP. The TISP is managed by role based access control policies. LACL can add or remove members at its sole discretion.

These operational considerations only highlight general aspects ISAOs should consider establishing. An ISAO's specific operational security policies and procedures must address its specific operations and the sensitivity of information being handled. ISAO operations will change over time, and periodic review of operational security procedures and policies may require updates. Annual reviews can be an effective check to ensure they are up to date. Any changes made should be consistent with the organization's governing documents.

¹⁵As an example, the "Operating Rules" of the FS-ISAC are available at https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf

¹⁶See <https://www.us-cert.gov/tlp>

9 INFORMATION PRIVACY

Before sharing cyber threat indicators, it is important to consider the privacy implications of what is being shared, including:

- whether the indicator contains information the ISAO knows at the time of sharing to be personal information about a specific individual or that identifies a specific individual;
- whether that identifying information is not directly related to a cybersecurity threat, and if so,
- whether the ISAO or member has identified and removed, as appropriate, such information.

Given the nature of a cyber threat indicator, oftentimes an individual whose personal information is directly related to a cybersecurity threat does not have the opportunity to consent to involvement in the process used to collect that information or access or correct that information. ISAOs should attempt to limit the impact of the data they collect on individual privacy where they can do so and maintain the effectiveness of cyber threat information sharing arrangements.

It is permissible under the Cybersecurity Information Sharing Act of 2015¹⁷ to share personal information as part of a cyber threat indicator but only in circumstances where it is directly related to the threat at the time of sharing. ISAOs may be at risk even beyond a possible failure to qualify for liability protections under Cybersecurity Information Sharing Act of 2015 without appropriate limitations on the receipt, retention, use, and dissemination of personally identifiable information (PII) when it is not part of a cyber threat indicator.¹⁸ DHS has issued privacy guidance¹⁹ concerning information shared with the U.S. government. In some instances, sensitive information such as PII, intellectual property, and trade secrets may be inadvertently encountered when handling cyber threat information. The improper disclosure of such information could cause harm to individuals, companies and others. Accordingly, organizations should consider and implement security and privacy controls and handling procedures necessary to protect this information from unauthorized disclosure or modification.

Often data requires protection, either by law, regulation, or contractual obligation. This includes PII and other sensitive information afforded protection under the Sarbanes-Oxley Act, the Payment Card Industry (PCI) Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA),²⁰ the Federal Information Security Modernization Act (FISMA) of 2014, the Gramm-Leach-Bliley Act (GLBA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Children's Online Privacy Protection Act (COPPA), among others. The Federal Trade Commission and States each address privacy and data protection and, depending on the source and type of any personal information, and whether there are any relevant cross-border transfers, the law of non-U.S. jurisdictions may apply.

LACL maintains limited PII data of its members (e.g. name, email, address, phone, etc.) and attempts to minimize all sensitive data collection. LACL members are acknowledge that sharing with the LACL is voluntary and their information is no longer considered private upon publishing to the LACL or LACL TISP unless specifically marked utilizing TLP.

¹⁷See <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>

¹⁸See National Institute of Standards and Technology, U.S. Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

¹⁹See https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

²⁰See <https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf>

9.1 CORE PRINCIPLES

Depending on what information is to be collected and shared, and where, developing privacy policies to meet the various applicable laws can be complex. LACL and its members should consider the following principles:

- LACL members are encouraged to identify and contribute indicators critical to identifying threats, while making efforts to minimize the PII shared with other members, and ensure compliance with all existing privacy regulatory and legal requirements at the federal, state, and local levels.
- If a member inadvertently submits PII not directly part of a cyber threat indicator to the LACL, the member may notify the LACL via email at tisp@lacyberlab.org to request assistance.
- The LACL may remove and remediate PII or other types of sensitive information when notified by a member.

The DHS document *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*²⁵ provides examples of certain personally identifiable information that can be part of a threat indicator and be shared. This includes particular IP addresses in certain circumstances and gives examples of personal or other information that should not be shared and of impermissible uses of shared information.

10 INFORMATION SECURITY

LACL has established internal information security policies including the following:

1. Analysis Methodology
2. IOC Use Cases (MISP)
3. LACL Change Management Form
4. LACL FAQs
5. LACL Information Protection Security Change Management Policy
6. LACL Information Protection Security Password Policy
7. LACL Intellectual Property

8. LACL Middleware Email Scoring
9. LACL Mobile App Dashboard Language
10. LACL Mobile App Security Policy
11. LACL Mobile App User Manual
12. LACL Mobile Data Retention Policy
13. LACL Partner Sharing Policy
14. LACL Systems & Infrastructure
15. LACL Threat Data Sources
16. LACL Threat Sharing Capability
17. LACL TISP Dashboards
18. LACL TISP IBM X-Force Exchange Risk Score
19. Threat Intelligence Sharing RFP Diagram

APPENDIX A ADDITIONAL RESOURCES

This appendix is a list of resources that provides useful information for ISAOs.

Cybersecurity Information Sharing Act of 2015

<https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>

Cybersecurity and Infrastructure Security Agency (CISA) implementation guidance for private sector

https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

Cyber Information Sharing and Collaboration Program (CISCP)

The CISCP is a program managed by the US-DHS National Cybersecurity Communications Integration Center. This is the main information sharing program between public and private entities.

<https://www.dhs.gov/ciscp>

Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT) Automated Indicator Sharing (AIS)

<https://www.us-cert.gov/ais>

https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf.

Department of Homeland Security and the Department of Justice

Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, including at p. 14 and Annex 1: Sharing of Cyber Threat Indicator and Defensive Measure Sharing between Non-Governmental Entities under the Cybersecurity Information Sharing Act of 2015, June 15, 2016.

https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

European General Data Protection Regulation (GDPR)

These are a set of regulations for countries in the European Union to strengthen data protection for individuals.

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

EU Network and Information Security (NIS) Directive

The NIS Directive is a European wide legislation aimed at enhancing and increasing cybersecurity capabilities of all EU states.

<https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive>

Public Key Infrastructure (PKI)

PKI consists of all of the policies, procedures, and technology that is used to establish secure communication between two parties. Public-key encryption is also known as asymmetric-key cryptography. It uses a key pair to encrypt and decrypt. The keys are made up of one public and one private. Both keys are mathematically associated.

[https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx)

<http://searchsecurity.techtarget.com/definition/PKI>

https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm

PCI Security Standards Council, LLC (2016). Requirements and Security Assessment Procedures Version 3.2 Wakefield, MA.

Payment Card Industry Data Security Standard (PCI DSS) Requirements and security standards.

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1470830604318

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity,

The NIST Cybersecurity Framework is a voluntary set of standards to increase cybersecurity and reduce risk to critical infrastructure.

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

U.S House of Representatives (2014). Federal Information Security Modernization Act. Washington DC.

The Federal Information Security Modernization Act updates and expands the framework initiated in Title III of the e-Government Act of 2002, i.e., the Federal Information Security Management Act (FISMA) of 2002.

<https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>

U.S House of Representatives (1999). Gramm-Leach-Bliley Act. Washington DC.

The Gramm-Leach-Bliley Act (GLBA) is the Financial Modernization Act of 1999 and sets controls for the way financial institutions handle personally identifiable information (PII) and other sensitive data.

<https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf>

U.S. House of Representatives (1996). Health Insurance Portability and Accountability Act. Washington DC.

The Health Insurance Portability and Accountability Act (HIPAA) places limits on who has access to and provides protections on all forms of health information of individuals.

<https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf>

U.S. House of Representatives (2009) Health Information Technology for Economic and Clinical Health Act. Washington DC.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was enacted as part of the American Recover and Reinvestment Act (ARRA) of 2009. The purpose of the law was to encourage the implementation and “meaningful use” of health information technology.

<https://www.congress.gov/111/plaws/publ5/PLAW-111publ5.pdf>

<http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html>

U.S. House of Representatives (2002). Sarbanes-Oxley Act. Washington DC.

The Sarbanes-Oxley Act of 2002 (SOX) is the Corporate and Auditing Accountability and Responsibility Act.

<https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf>

US-CERT Traffic Light Protocol

The Traffic Light Protocol was developed by US-CERT to designate sensitive information and to ensure the correct distribution of that information.

<https://www.us-cert.gov/tlp>

APPENDIX B GLOSSARY

Selected terms used in the publication are defined below.

Alert: Timely information about current security issues, vulnerabilities, and exploits.

Analysis: A detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand.

Automated Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.

Campaigns: In the context of cybersecurity, a campaign or attack via cyberspace that targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, destroying the integrity of the data, or stealing controlled information.

Computer Security Incident: See "Incident."

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Cyber Threat Information: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems.

Cybersecurity Information: Data-related risks and practices relevant to improving the security of an information system.

Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system.

Cybersecurity Threat: An action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber Threat Indicator: Information that is necessary to describe or identify—

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or
- any combination thereof.

Defensive Measure: An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response: An organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Indicator: An artifact or observable evidence that suggests that an adversary is preparing to attack, that an attack is currently underway, or that a compromise may have already occurred.

Malware: A program that is covertly inserted into another program or system with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Malicious Cyber Command and Control: A method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system.

Malicious Reconnaissance: A method for actively probing or passively monitoring an information system for the purpose of discerning its security vulnerabilities, if such method is associated with a known or suspected cybersecurity threat.

Monitor: To acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.

Mitigation: The act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.

Operational Analysis: Examination of any combination of threats, vulnerabilities, incidents, or practices that results in methods to protect specific data, infra- structure, or functions (for example, incident analysis, identification of specific tactics, techniques, procedures, or threat actors, etc.)

Secure Portal: A web-enabled resource providing controlled secure access to and interactions with relevant information assets (information content, applications, and business processes) to selected audiences using web-based technologies in a personalized manner.

Security Control: The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security Vulnerability: Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Sensitive Information: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Situational Awareness: Comprehension of information about the current and developing security posture and risks, based on information gathered, observation, analysis, and knowledge or experience.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an

information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Actor: An individual or group involved in malicious cyber activity.

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Trend Analysis: Examination of data to identify any combination of broad, non-obvious, or emerging actions (for example, threat actor campaigns and intent, common vulnerabilities and configurations exploited, merging operational analytics with non-like data streams such as assessments, etc.).

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

APPENDIX C ACRONYMS

AIS	Automated Indicator Sharing
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CVE	Common Vulnerabilities and Exposures
CONOPS	Concept of Operations
DHS	Department of Homeland Security
GDPR	General Data Protection Regulation (Directive 95/46/EC)
HIPAA	Health Information Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
LACL	Los Angeles Cyber Lab
NCCIC	National Cybersecurity & Communications Integration Center
NIS	Network and Information Security Directive (NIS)
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
PII	Personable Identifiable Information
SO	Standards Organization
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TISP	Threat Intelligence Sharing Platform
TLP	Traffic Light Protocol
TTP	Tactics, Techniques & Procedures



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)
Supported by the U.S. Department of Homeland Security

Information Protection & Security

LA Cyber Lab Mobile Application Middleware Architecture and
Configuration

January 9, 2020

Table of Contents

- LA Cyber Lab Mobile Application Cloud Architecture* 3**
- Overview 3**
- Amazon Web Services 4**
 - AWS Account Information 4
 - Amazon Simple Email Service 4
 - LACL Virtual Private Cloud (VPC)..... 16
 - AWS Elastic Beanstalk..... 23
 - AWS Relational Database Service 26

LA Cyber Lab Mobile Application Cloud Architecture

Overview

The technical components that support the LA Cyber Lab (LACL) Mobile Application include:

- A mobile application built for IOS and Android operating systems,
- Application Programming Interfaces (APIs) developed to retrieve application data and communicate with the LACL Threat Intelligence Sharing Platform.
- Amazon Simple Email Services to send, receive and process emails
- Amazon Relational Database Service used to store application data

The technical components and services, referred to as the “Middleware”, implemented to support the mobile application (i.e. APIs, database, and email) are all hosted on Amazon Web Services (AWS). This document is intended to provide information on how the middleware components have been implemented and configured. Figure 1 below is a provides a high-level view of the system components. Each of the component’s functions and configuration will be described in the following sections.

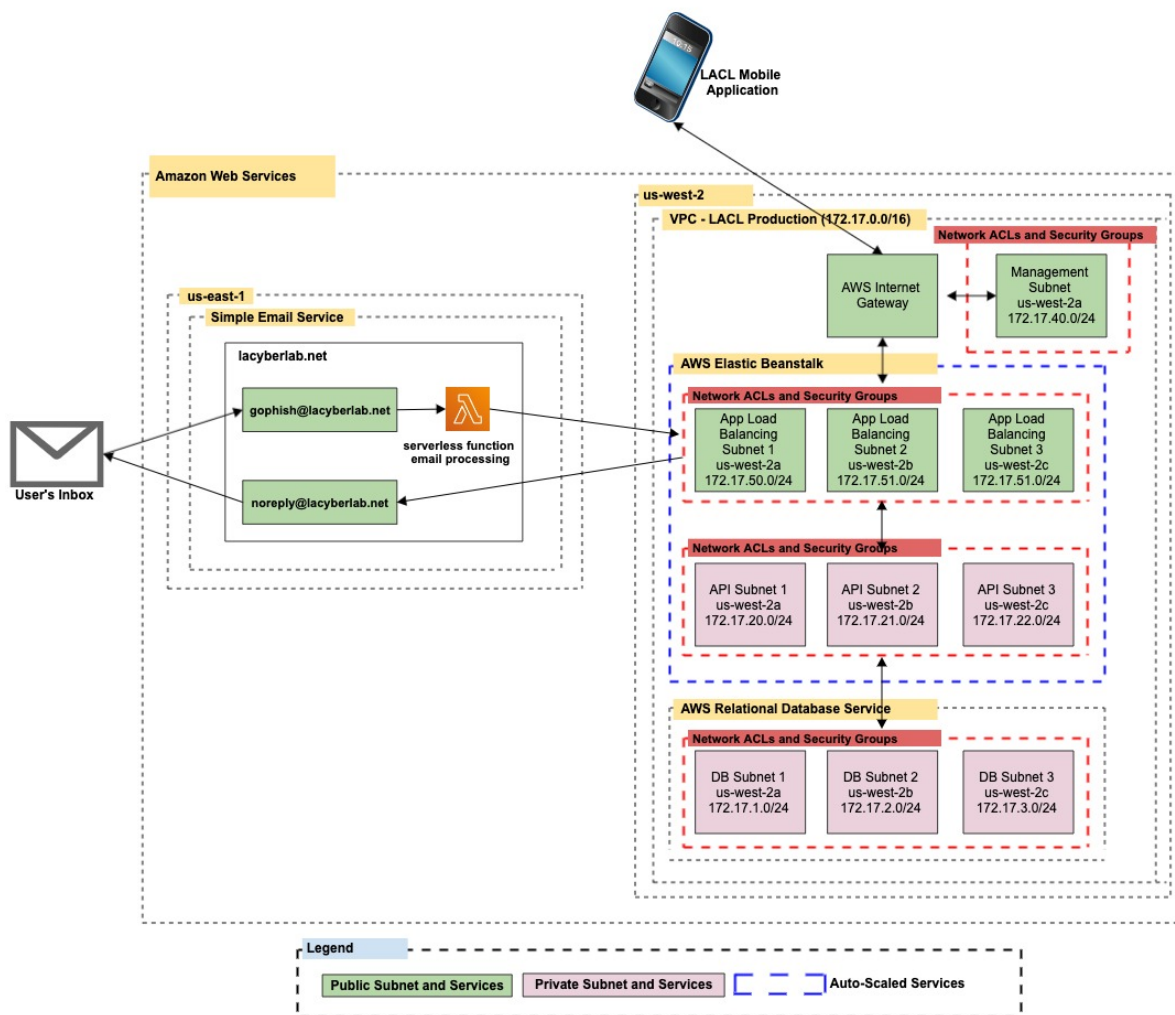


Figure 1 - LACL Mobile Application Middleware Architecture

Los Angeles Cyber Lab – InfoSec Mobile Application

Amazon Web Services

Amazon Web Services is the public cloud service provider used to host the LACL Mobile Application Middleware. The Middleware is built using a combination of AWS Infrastructure and Platform as a Service resources. Instances of these resources are deployed within **us-east-1** and **us-west-2** regions across multiple availability zones within the respective regions. Where available, AWS Platform as a Service options are used to reduce the burden of infrastructure and software lifecycle management.

Within **us-east-1**, Amazon’s Simple Email Service and Lambda have been implemented to send, receive and process email. Within **us-west-2**, Amazon Elastic Load Balancers along with Elastic Beanstalk and Relation Database Services have been implemented to host a series of APIs and backend database instances. The APIs and database instances have been deployed across multiple availability zones in a highly available and fault tolerant configuration. Network ACLs and Security Groups are implemented to segregate publicly accessible resources (i.e. internet facing services) from private resources.

AWS Account Information

The LACL middleware is currently hosted within The Rosslyn Group’s AWS account. This was done under the direction of the LACL leadership. The root account is secured through multi-factor authentication (TOTP), a strong password, and by the removal of its API credentials. Users are provisioned by The Rosslyn Group until the resources are migrated over to an LACL AWS Account.

The sign-in URL for the account is- <https://lacyberlab.signin.aws.amazon.com/console>.

Amazon Simple Email Service

Amazon Simple Email Service (Amazon SES) is a highly scalable and cost-effective service for sending and receiving email. Amazon SES eliminates the complexity and expense of building an in-house email solution or licensing, installing, and operating a third-party email solution. Within the LACL Middleware, Amazon SES is used to host the inbox (gophish@lacyberlab.net) that users forward emails to as well as used to send email to users for registration verification and password reset. The “lacyberlab.net” domain is owned by the LACL and its DNS has been configured to send and receive email through Amazon SES. Table 1 below describes the DNS entries that were added to the lacyberlab.net DNS provider (Cloudflare) to enable email services through Amazon SES for the domain –

Record Name	Record Type	Record Value
amazonses.lacyberlab.net	TXT	XGKh7EjaH3UtNqBt7H4GcHzqt roBNGTssmEzCE0A7oM=
aakkcmgshl4kauciquophzewht6rrpja._domainkey.lacyberlab.net	CNAME	aakkcmgshl4kauciquophzewht6rrpja.dkim.amazonses.com
cvimzu7n4zscr6qvyz3n4v7ofvf4ttxc._domainkey.lacyberlab.net	CNAME	cvimzu7n4zscr6qvyz3n4v7ofvf4ttxc.dkim.amazonses.com

Los Angeles Cyber Lab – InfoSec Mobile Application

w6brudnrd7lbu4va2filv24tkgzajr7u._domainkey.lacyberlab.net	CNAME	w6brudnrd7lbu4va2filv24tkgzajr7u.dkim.amazonses.com
lacyberlab.net	MX	10 inbound-smtp.us-east-1.amazonaws.com

Table 1 - Amazon SES DNS Entries

Receiving Email

The mobile application instructs users to forward suspicious emails to gophish@lacyberlab.net to receive a determination on the risk of the email. After the user forwards their message to gophish@lacyberlab.net, Amazon SES receives the email and triggers serverless functions (Lambda) to process the message. Figure 2 provides a summary view of the rules configured within Amazon SES to process the incoming message.

The screenshot shows the configuration for an Amazon SES rule set named 'gophish'. The rule is enabled and has a recipient of 'gophish@lacyberlab.net'. The rule actions are:

Pos.	Rule name	Status	TLS	Recipients
1	gophish	Enabled		gophish@lacyberlab.net

Recipients	Actions
gophish@lacyberlab.net	<ol style="list-style-type: none">Lambda Action Invoke Lambda function <code>validateEmail</code> as RequestResponseS3 Action Write to S3 bucket <code>gophish.lacl.prod</code>Lambda Action Invoke Lambda function <code>gophishProd</code> as RequestResponse

Figure 2 - Amazon SES Rule Set

1. The first serverless function (Lambda Action) is executed to determine if the sender address is a verified address of a registered LACL user. If the sender address is not a verified address of a registered user, the message will be discarded.
2. If the message is from a verified sender address of a registered user, then the email is sent to an S3 bucket (S3 Action) for temporary storage to allow email processing - <https://s3.amazonaws.com/gophish.lacl.prod>. Note the S3 bucket and objects are not publicly accessible as they require the use of an IAM account that has specific S3 bucket permissions.
3. After the email is sent to S3, another Lambda function (Lambda Action) is executed to parse the email contents and make a request to a Middleware API to submit the email contents to the Threat Intelligence Sharing Platform. After processing, the email is deleted from the S3 bucket therefore leaving no remnants of the forwarded email content within the LACL Middleware.

For reference, below is the code for both Lambda functions that are invoked during email during processing. Note that there are environment variables that sourced from the runtime to populate the secrets and configuration settings needed for execution. The secrets are provided in a separate password protected document.

First Lambda Action - validateEmail Lambda Function

Runtime – Node.js 10.x

```
'use strict';

// load AWS SDK module, which is always included in the runtime environment
const AWS = require('aws-sdk');
const API_ENDPOINT = process.env.API_ENDPOINT;
const LAMBDA_EMAIL = process.env.LAMBDA_EMAIL;
const LAMBDA_PASSWORD = process.env.LAMBDA_PASSWORD;

// AWS SES Configuration

const sesConfig = {
  'apiVersion': '2010-12-01',
  'accessKeyId': process.env.AWS_SES_ACCESS_KEY_ID,
  'secretAccessKey': process.env.AWS_SES_SECRET_ACCESS_KEY,
  'region': process.env.AWS_SES_REGION
};

/* Defines the LACL API as a "service" leveraging constructs
that are built into the AWS SDK. This reduces the need for third
party dependencies to call out to APIs
*/
const svc = new AWS.Service({

  // the LACL API base URL
  endpoint: API_ENDPOINT,

  // don't parse API responses
  // (this is optional if you want to define shapes of all your endpoint responses)
  convertResponseTypes: false,

  // defines the LACL API endpoints
  apiConfig: {
    metadata: {
      protocol: 'rest-json'
    },
  },
  operations: {
    // Authentication endpoint
    Authenticate: {
      http: {
        method: 'POST',
        requestUri: '/auth/login'
      },
      input: {
        type: 'structure',
        required: [ 'data' ],
        payload: 'data',
        members: {
          'data': {
            type: 'structure',
            required: [ 'registeredProfileEmail', 'password' ],
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
        members: {
            'registeredProfileEmail': {},
            'password': {sensitive: true}
        }
    }
},
output: {
    type: 'structure',
    members: {
        'authToken': {
            // the token is returned as an HTTP response header
            location: 'header',
            // the header name
            locationName: 'Authorization'
        }
    }
},
// Validate Email
Validate: {
    http: {
        method: 'GET',
        requestUri: '/auth/validate'
    },
    input: {
        type: 'structure',
        required: [ 'auth', 'registeredProfileEmail' ],
        members: {
            'auth': {
                location: 'header',
                locationName: 'Authorization',
                sensitive: true
            },
            'registeredProfileEmail': {
                location: 'querystring',
                locationName: 'registeredProfileEmail'
            }
        }
    },
    output: {
        type: 'structure',
        members: {
            'isValidEmail': {location: 'body', locationName: 'isValidEmail'},
            'message': {location: 'body', locationName: 'message'},
        }
    }
}
});

// disable AWS region related login in the SDK
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
svc.isGlobalEndpoint = true;

/*
Triggered from AWS SES receipt rule
Performs the following actions:
  1. Calls Validate API to verify sender
*/
exports.handler = function(event, context, callback) {
  console.log('Process Email - verify sender');

  let sesNotification = event.Records[0].ses;
  console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

  // get the sender email address from the message
  let sender = sesNotification.mail.source;
  console.log("The from address pulled from ses notification is: ", sender);

  let authorizationToken;

  /*
  Authenticate the lambda user and retrieve Authorization token
  to call remaining APIs
  */
  svc.authenticate({
    data: {
      registeredProfileEmail: LAMBDA_EMAIL,
      password: LAMBDA_PASSWORD
    }
  }, (err, data) => {
    if (err) {
      console.log('Authentication Error: ', err);
      callback(null, {'disposition':'STOP_RULE'});
    } else {
      authorizationToken = data.authToken;
      console.log('The authorization toke is: ', authorizationToken);
      // Get the email from S3
      svc.validate({
        auth: `Bearer ${authorizationToken}`,
        registeredProfileEmail: sender
      }, (err, data) => {
        if (err) {
          console.log('Error verifying sender: ', err);
          callback(null, {'disposition':'STOP_RULE'});
        } else {
          if (data.isValidEmail === 3) {
            console.log('Sender email address was verified, continue processing: ', data.message);
            callback(null, {'disposition':'CON'});
          } else {
            console.log('Sender is not a verified email address: ', data.message);
            callback(null, {'disposition':'STOP_RULE'});
          }
        }
      });
    }
  });
};
```

```
    }  
  });  
};
```

Second Lambda Action - gophishProd Lambda Function Runtime – Node.js 10.x

```
'use strict';  
  
// load AWS SDK module, which is always included in the runtime environment  
const AWS = require('aws-sdk');  
const simpleParser = require('mailparser').simpleParser;  
const s3 = new AWS.S3();  
const BUCKET_NAME = process.env.S3_BUCKET_NAME;  
const API_ENDPOINT = process.env.API_ENDPOINT;  
const LAMBDA_EMAIL = process.env.LAMBDA_EMAIL;  
const LAMBDA_PASSWORD = process.env.LAMBDA_PASSWORD;  
const TRUSTAR_INBOX = process.env.TRUSTAR_INBOX;  
const EMAIL_SENDER_ADDRESS = process.env.EMAIL_SENDER_ADDRESS;  
  
// const currentDate = function() {  
//   const d = new Date();  
//   let month = "" + (d.getMonth() + 1);  
//   let day = "" + d.getDate();  
//   const year = d.getFullYear();  
  
//   if (month.length < 2) month = '0' + month;  
//   if (day.length < 2) day = '0' + day;  
  
//   return [year, month, day].join('-');  
// }  
  
const currentDate = new Date().toISOString().slice(0,10);  
  
// AWS SES Configuration  
  
const sesConfig = {  
  'apiVersion': '2010-12-01',  
  'accessKeyId': process.env.AWS_SES_ACCESS_KEY_ID,  
  'secretAccessKey': process.env.AWS_SES_SECRET_ACCESS_KEY,  
  'region': process.env.AWS_SES_REGION  
};  
  
/* Defines the LACL API as a "service" leveraging constructs  
that are built into the AWS SDK. This reduces the need for third  
party dependencies to call out to APIs  
*/  
const svc = new AWS.Service({  
  
  // the LACL API base URL  
  endpoint: API_ENDPOINT,  
  
  // don't parse API responses
```


Los Angeles Cyber Lab – InfoSec Mobile Application

```
// (this is optional if you want to define shapes of all your endpoint responses)
convertResponseTypes: false,

// defines the LAACL API endpoints
apiConfig: {
  metadata: {
    protocol: 'rest-json'
  },
  operations: {
    // Authentication endpoint
    Authenticate: {
      http: {
        method: 'POST',
        requestUri: '/auth/login'
      },
      input: {
        type: 'structure',
        required: [ 'data' ],
        payload: 'data',
        members: {
          'data': {
            type: 'structure',
            required: [ 'registeredProfileEmail', 'password' ],
            members: {
              'registeredProfileEmail': {},
              'password': {sensitive: true}
            }
          }
        }
      },
      output: {
        type: 'structure',
        members: {
          'authToken': {
            // the token is returned as an HTTP response header
            location: 'header',
            // the header name
            locationName: 'Authorization'
          }
        }
      }
    },
    // validate sender email and create report
    CreateReport: {
      http: {
        method: 'POST',
        requestUri: '/reports/create/internal'
      },
      input: {
        type: 'structure',
        required: [ 'auth', 'data' ],
        payload: 'data',
        members: {
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
    'auth': {
      location: 'header',
      locationName: 'Authorization',
      sensitive: true
    },
    'data': {
      type: 'structure',
      required: [ 'userEmail', 'reportDate', 'reportExtSource', 'defaultScoreStdId', 'reportTitle',
'reportDetail', 'notificationMessage' ],
      members: {
        'userEmail': {},
        'reportDate': {},
        'reportExtSource': {},
        'defaultScoreStdId': {},
        'reportTitle': {},
        'reportDetail': {},
        'notificationMessage': {}
      }
    }
  },
  output: {
    type: 'structure',
    members: {
      'success': {location: 'body', locationName: 'success'},
      'message': {location: 'body', locationName: 'message'},
      'reportId': {location: 'body', locationName: 'reportId'}
    }
  }
},
// update report with external Id
UpdateExternal: {
  http: {
    method: 'PUT',
    requestUri: '/reports/create/external'
  },
  input: {
    type: 'structure',
    required: [ 'auth', 'reportId', 'externalReportId', 'reportExtSourceId' ],
    members: {
      'auth': {
        location: 'header',
        locationName: 'Authorization',
        sensitive: true
      },
      'reportId': {
        location: 'querystring',
        locationName: 'reportId'
      },
      'externalReportId': {
        location: 'querystring',
        locationName: 'externalReportId'
      }
    }
  }
},
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
        'reportExtSourceId': {
            location: 'querystring',
            locationName: 'reportExtSourceId',
            type: 'integer'
        }
    },
    output: {
        type: 'structure',
        members: {
            'success': {location: 'body', locationName: 'success'},
            'message': {location: 'body', locationName: 'message'},
            'externalReportId': {location: 'body', locationName: 'externalReportId'}
        }
    }
}
});
```

```
// disable AWS region related login in the SDK
svc.isGlobalEndpoint = true;
```

```
/*
```

```
Triggered from AWS SES receipt rule after S3 action
```

```
Performs the following actions:
```

1. Calls CreateReport API to verify sender
2. Sends outbound email via SES to TruSTAR inbox for analysis
3. Calls UpdateExternalID to update report with the messageID returned from AWS SES outbound email

```
*/
```

```
exports.handler = function(event, context, callback) {
    console.log('Process Email - verify sender');
```

```
    let sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));
```

```
    // get the sender email address from the message
    let sender = sesNotification.mail.source;
    console.log("The from address pulled from ses notification is: ", sender);
```

```
    /* Retrieve the messageID from the message
       AWS uses messageID as the S3 object key for the email
    */
```

```
    let messageID = sesNotification.mail.messageId;
    console.log("The message Id from email is: ", messageID);
```

```
    let authorizationToken;
    let params;
    let reportID;
```

```
    /*
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
Authenticate the lambda user and retrieve Authorization token
to call remaining APIs
*/
svc.authenticate({
  data: {
    registeredProfileEmail: LAMBDA_EMAIL,
    password: LAMBDA_PASSWORD
  }
}, (err, data) => {
  if (err) {
    console.log('Authentication Error: ', err);
    callback(null, {'disposition':'STOP_RULE'});
  } else {
    authorizationToken = data.authToken;
    console.log('The authorization token is: ', authorizationToken);
    // Get the email from S3
    s3.getObject({
      'Bucket': BUCKET_NAME,
      'Key': messageId
    }, function(err, data) {
      if (err) {
        console.error('Error retrieving email from S3: ', err);
        callback(null, {'disposition':'STOP_RULE'});
      } else {
        /* Parse the received email, and call createReport to
        verify sender. If sender is not verified then delete
        email from S3 and stop processing of receipt rule
        If sender is verified, prepare email to send to TruSTAR
        */
        console.log(data.Body);
        simpleParser(data.Body, (err, parsed) => {
          if (err) {
            console.log('Error while parsing raw email retrieved from S3', err);
            callback(null, {'disposition':'STOP_RULE'});
          } else {
            svc.createReport({
              auth: authorizationToken,
              data: {
                userEmail: sender,
                reportDate: currentDate,
                reportExtSource: '1',
                defaultScoreStdId: '1',
                reportTitle: parsed.subject,
                //reportDetail: parsed.text.substring(0, 1000),
                reportDetail: "",
                notificationMessage: 'Email Received'
              }
            }, (err, data) => {

              if (err) {
                if (err.message === 'Email is invalid') {
                  console.log('Sender email is invalid', err);
                  s3.deleteObject({
```

```
        Bucket: BUCKET_NAME,
        Key: messageId
    }, function(err, data) {
        if (err) {
            console.log('error deleting email from S3', err);
            callback(null, {'disposition':'STOP_RULE'});
        }
    });
    callback(null, {'disposition':'STOP_RULE'});
} else {
    console.log('Error during call to createReport: ', err);
    callback(null, {'disposition':'STOP_RULE'});
}
}

else {
    console.log('data is: ', data);
    console.log('Created a report. The report ID is:', data.reportId);
    reportID = data.reportId;
    let hashedAttachments = "";
    if (parsed.attachments.length !== 0) {
        for(let val of parsed.attachments) {
            hashedAttachments += `Filename: ${val.filename}`;
            hashedAttachments += ` MD5:${val.checksum}`;
        }
    }
    //Populate email parameters
    params = {
        Source: EMAIL_SENDER_ADDRESS,
        Destination: {
            ToAddresses: [
                TRUSTAR_INBOX
            ]
        },
        Message: {
            Subject: {
                Charset: "UTF-8",
                Data: `key:[${reportID}] {MobileApp} "${parsed.subject}"`
            },
            Body: {
                Text: {
                    Data: `${parsed.text} Hashes of Attachments: ${hashedAttachments}`
                }
            }
        }
    }

    new AWS.SES(sesConfig).sendEmail(params, function(err, data) {
        if (err) {
            console.log('Error when trying to send email to TruSTAR via SES', err);
            callback(null, {'disposition':'STOP_RULE'});
        } else {
            console.log('Email sent to TruSTAR. MessageID is: ', data.MessageId);
        }
    });
}
```

```
    svc.updateExternal({
      auth: authorizationToken,
      reportId: reportID,
      externalReportId: data.MessageId,
      reportExtSourceId: 1
    }, (err, data) => {
      if (err) {
        console.log('Error updating the report external id: ', err);
        callback(null, {'disposition':'STOP_RULE'});
      } else {
        console.log('Successfully updated externalID to: ', data.externalReportId);
        s3.deleteObject({
          Bucket: BUCKET_NAME,
          Key: messageId
        }, function(err, data) {
          if (err) {
            console.log('error deleting email from S3', err);
            callback(null, {'disposition':'STOP_RULE'});
          }
        });
        callback(null, {'disposition':'STOP_RULE'});
      }
    });
  }
});
}
});
}
});
}
});
}
});
};
```

There are many benefits to Lambda, the discussion of which is out of scope for this document, but one worth mentioning is its inherent scalability. For every invocation of the function, Lambda efficiently spins up a new instance to service the request. So if 100 emails were concurrently sent to the gophish@lacyberlab.net, then Lambda would service all requests concurrently by instantiating 100 instances of the function. Additionally, Lambda serves as a cost-effective option as Amazon only charges for the compute used for the execution of the function (in fact, Amazon gives 1,000,000 free Lambda requests per month).

Sending Email

Amazon SES is also configured to send emails from the “lacyberlab.net” domain. This is in support of the email address verification and password reset functions of the mobile application. The Middleware APIs programmatically send emails from the “lacyberlab.net” domain using Amazon SES SMTP interface. The credentials for this interface are managed

Los Angeles Cyber Lab – InfoSec Mobile Application

within the AWS account and are also stored as environment variables within the API runtime. The only email send address used by the application is noreply@lacyberlab.net.

LACL Virtual Private Cloud (VPC)

Amazon VPC allows for the provisioning of a logically isolated section of the AWS cloud where AWS resources can be launched in a virtual network defined by the user. AWS allows complete control over the virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways. For the LACL production environment, an Amazon VPC is configured in **us-west-2**. This VPC provides the network onto which the Application Load Balancers, Elastic Beanstalk EC2 instances, and Amazon RDS instances are deployed. Below are tables that provide the subnet information, along with associative route tables, network ACLs and security group configuration for the VPC.

VPC Name: LACL-Production

IP Address Space: 172.17.0.0/16

Subnet Name	Function	Availability Zone	IP V4 CIDR	Public IPV4 Configured
LB-Subnet1	For load balancer deployments	us-west-2a	172.17.50.0/24	Yes
LB-Subnet2	For load balancer deployments	us-west-2b	172.17.51.0/24	Yes
LB-Subnet3	For load balancer deployments	us-west-2c	172.17.52.0/24	Yes
API-Subnet1	For API deployments	us-west-2a	172.17.20.0/24	Yes (only for outbound elastic beanstalk registration, public inbound access blocked by stateful firewall)
API-Subnet2	For API deployments	us-west-2b	172.17.21.0/24	Yes (only for outbound elastic beanstalk registration, public inbound access blocked by stateful firewall)
API-Subnet3	For API deployments	us-west-2c	172.17.22.0/24	Yes (only for outbound elastic

Los Angeles Cyber Lab – InfoSec Mobile Application

				beanstalk registration, public inbound access blocked by stateful firewall)
DB-Subnet1	For Database instance (RDS) deployments	us-west-2a	172.17.1.0/24	No
DB-Subnet2	For Database instance (RDS) deployments	us-west-2b	172.17.2.0/24	No
DB-Subnet3	For Database instance (RDS) deployments	us-west-2c	172.17.3.0/24	No
MGMT-Subnet1	For bastion host deployments (privileged access to private resources)	us-west-2a	172.17.40.0/24	Yes

Table 2 - VPC Subnet Overview

Subnet Name	Route Table	Network ACLs	Security Group Rules
LB Subnets	Destination: 172.17.0.0/16 Target: local Destination: 0.0.0.0/0 Target: Production Internet Gateway	Inbound: Rule #: 100 Type: HTTPS Port: 443 Source: 0.0.0.0/0 ALLOW Rule #: 110 Type: Custom TCP Port Range: 1024-65535 Source: 172.17.0.0/16 ALLOW Rule #: * Type: All Traffic Port Range: All DENY	Inbound: Type: HTTPS Port: 443 Source: 0.0.0.0/0 Outbound: Type: HTTP Port: 80 Destination: sg-0ac97a78b530b5584 (API Security Group)

Los Angeles Cyber Lab – InfoSec Mobile Application

Subnet Name	Route Table	Network ACLs	Security Group Rules
		<p>Outbound: Rule #: 100 Type: HTTP Port: 80 Destination: 172.17.0.0/16 ALLOW</p> <p>Rule #: 110 Type: Custom TCP Port Range: 1024-65535 Destination: 0.0.0.0/0 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All DENY</p>	
API Subnets	<p>Destination: 172.17.0.0/16 Target: local</p> <p>Destination: 0.0.0.0/0 Target: Production Internet Gateway</p>	<p>Inbound: Rule #: 100 Type: HTTP Port: 80 Source: 172.17.50.0/24 ALLOW</p> <p>Rule #: 110 Type: HTTP Port: 80 Source: 172.17.51.0/24 ALLOW</p> <p>Rule #: 120 Type: HTTP Port: 80 Source: 172.17.52.0/24 ALLOW</p> <p>Rule #: 130</p>	<p>Inbound: Type: HTTP Port: 80 Source: sg-0cd1b2d6de6dce246 (Load Balancer Security Group)</p> <p>Type: SSH Port: 22 Source: 172.17.40.0/24</p> <p>Outbound: Type: All traffic Port: All Destination: 0.0.0.0/0</p>

Los Angeles Cyber Lab – InfoSec Mobile Application

Subnet Name	Route Table	Network ACLs	Security Group Rules
		<p>Type: SSH Port: 22 Source: 172.17.40.0/24 ALLOW</p> <p>Rule #: 140 Type: Custom TCP Port Range: 1024-65535 Source: 0.0.0.0/0 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All Source: 0.0.0.0/0 DENY</p> <p>Outbound: Rule #: 110 Type: HTTPS Port: 443 Destination: 0.0.0.0/0 ALLOW</p> <p>Rule #: 120 Type: Custom TCP Port Range: 1024-65535 Destination: 0.0.0.0/0 ALLOW</p> <p>Rule #: 130 Type: MySQL/Aurora Port: 3306 Destination: 172.17.1.0/24 ALLOW</p> <p>Rule #: 140</p>	

Los Angeles Cyber Lab – InfoSec Mobile Application

Subnet Name	Route Table	Network ACLs	Security Group Rules
		<p>Type: MySQL/Aurora Port: 3306 Destination: 172.17.2.0/24 ALLOW</p> <p>Rule #: 150 Type: MySQL/Aurora Port: 3306 Destination: 172.17.3.0/24 ALLOW</p> <p>Rule #: 160 Type: SMTPS Port: 465 Destination: 0.0.0.0/0 ALLOW</p> <p>Rule #: 170 Type: HTTP Port: 80 Destination: 0.0.0.0/0 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All Destination: 0.0.0.0/0 DENY</p>	
DB Subnets	Destination: 172.17.0.0/16 Target: local	<p>Inbound: Rule #: 100 Type: MySQL/Aurora Port: 3306 Source: 172.17.20.0/24 ALLOW</p>	<p>Inbound: Type: MySQL/Aurora Port: 3306 Source: 172.17.20.0/24</p> <p>Type: MySQL/Aurora Port: 3306</p>

Los Angeles Cyber Lab – InfoSec Mobile Application

Subnet Name	Route Table	Network ACLs	Security Group Rules
		<p>Rule #: 110 Type: MySQL/Aurora Port: 3306 Source: 172.17.21.0/24 ALLOW</p> <p>Rule #: 120 Type: MySQL/Aurora Port: 3306 Source: 172.17.22.0/24 ALLOW</p> <p>Rule #: 130 Type: MySQL/Aurora Port: 3306 Source: 172.17.40.0/24 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All Source: 0.0.0.0/0 DENY</p> <p>Outbound: Rule #: 110 Type: All Traffic Port: All Destination: 172.17.20.0/24 ALLOW</p> <p>Rule #: 120 Type: All Traffic Port: All Destination: 172.17.21.0/24 ALLOW</p> <p>Rule #: 130</p>	<p>Source: 172.17.21.0/24</p> <p>Type: MySQL/Aurora Port: 3306 Source: 172.17.22.0/24</p> <p>Type: MySQL/Aurora Port: 3306 Source: 172.17.40.0/24</p> <p>Outbound: Type: All traffic Port: All Destination: 0.0.0.0/0</p>

Los Angeles Cyber Lab – InfoSec Mobile Application

Subnet Name	Route Table	Network ACLs	Security Group Rules
		<p>Type: All Traffic Port: All Destination: 172.17.22.0/24 ALLOW</p> <p>Rule #: 140 Type: All Traffic Port: All Destination: 172.17.40.0/24 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All Destination: 0.0.0.0/0 DENY</p>	
MGMT Subnet	<p>Destination: 172.17.0.0/16 Target: local</p> <p>Destination: 0.0.0.0/0 Target: Production Internet Gateway</p>	<p>Inbound: Rule #: 100 Type: RDP Port: 3389 Source: 0.0.0.0/0 ALLOW</p> <p>Rule #: 110 Type: Custom TCP Port: 32768 - 65535 Source: 0.0.0.0/0 ALLOW</p> <p>Rule #: * Type: All Traffic Port Range: All Source: 0.0.0.0/0 DENY</p> <p>Outbound: Rule #: 100 Type: All TCP Port: 0-65535</p>	<p>Inbound: Type: RDP Port: 3389 Source: 70.181.111.153/32 (TRG Office)</p> <p>Type: RDP Port: 3389 Source: 184.179.107.206/32 (TRG Office)</p> <p>Outbound: Type: All traffic Port: All Destination: 0.0.0.0/0</p>

Subnet Name	Route Table	Network ACLs	Security Group Rules
		Destination: 0.0.0.0/0 ALLOW Rule #: * Type: All Traffic Port Range: All Destination: 0.0.0.0/0 DENY	

Table 3 - Subnet Network and Security ACLs

Internet Gateway

An internet gateway within an AWS VPC is a horizontally scaled, redundant, and highly available component that allows communication between instances in the VPC and the internet. It imposes no availability risks or bandwidth constraints on VPC network traffic. An internet gateway serves two purposes: to provide a target within VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

AWS Elastic Beanstalk

AWS Elastic Beanstalk makes it easy to quickly deploy and manage applications in the AWS Cloud. The service allows developers to upload an application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. AWS Elastic Beanstalk uses proven AWS features and services, such as Amazon EC2, Amazon RDS, Elastic Load Balancing, Auto Scaling, Amazon S3, and Amazon SNS, to create an environment that runs your application.

Within the LA Cyber Lab’s AWS environment, Elastic Beanstalk is used to deploy and manage the APIs that support the mobile application. The APIs are written in NodeJS and are managed collectively as a single project. The API code is managed within a GitLab repository across development and master branches. All code commits successfully tested and approved within the development branch are merged into the master branch. Elastic Beanstalk deployments are sourced from the master branch and are invoked using the Elastic Beanstalk Command Line Interface (CLI). The CLI command used to initiate the deployment leverages a set of configurations (also version controlled). The configurations define the environment, thresholds for scaling, as well as the runtime environment variables.

The configurations are detailed below. Note that any secrets or sensitive settings have been omitted (listed as <omitted>) and are made available in a separate protected document.

.elasticbeanstalk/config.yml

```
global:
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
application_name: lacl-api
branch: null
default_ec2_keyname: ec2
default_platform: Node.js
default_region: us-west-2
include_git_submodules: true
instance_profile: null
platform_name: null
platform_version: null
profile: eb-cli
repository: null
sc: git
```

.ebextensions/options.config

```
option_settings:
aws:elasticbeanstalk:application:environment:
  JWT_SECRET: <omitted>
  NODE_ENV: production
  AUTHORIZATION_TOKEN: <omitted>
  SMTP_USER: 'AKIAQPAW3PMGNSXR7AIG'
  SMTP_PASSWORD: <omitted>
  SMTP_EMAIL_FROM: 'LA Cyber Lab <noreply@lacyberlab.net>'
  SMTP_PORT: 465
  SMTP_HOST: 'email-smtp.us-east-1.amazonaws.com'
  SMTP_SECURE: true
  EMAIL_ERROR_LEVEL: WARN
  DEFAULT_ERROR_LEVEL: DEBUG
  REPORT_AGE_MINUTES: 60
  PROFILE_EMAIL_DAYS: 30
  EXPIRY_MINUTES: 10
  LACL_BASE_URL: https://api.rosslyn.group
  APP_REDIRECT_VERIFY_LINK: 'com.lacyberlab.lacyberlab://verify/email'
  APP_REDIRECT_VERIFY_PASSWORD: 'com.lacyberlab.lacyberlab://verify/password'
  TRUSTAR_API_KEY_0: b8179861-1da4-4c1d-b9c4-6a0fec19e626
  TRUSTAR_API_SECRET_0: <omitted>
  TRUSTAR_API_KEY_1: 2d2ae209-2eb7-4dde-9567-954ff0b7d9db
  TRUSTAR_API_SECRET_1: <omitted>
  TRUSTAR_API_KEY_2: 5d89ed86-39d6-4495-abab-569dff8bd9f1
  TRUSTAR_API_SECRET_2: <omitted>
  TRUSTAR_API_KEY_3: 066b7eab-4861-4640-8695-fc4267122861
  TRUSTAR_API_SECRET_3: <omitted>
  TRUSTAR_API_KEY_4: 833aee9f-cd34-4664-8fae-6fedf4843ac5
  TRUSTAR_API_SECRET_4: <omitted>
  TRUSTAR_BASE_URL: https://api.trustar.co
  TRUSTAR_ENCLAVE_ID: 08d99eac-d197-4193-86d9-b637a70df1cb
  TRUSTAR_XFORCE_ID: cfa7b4ef-f30b-4773-92d7-c33a70af1e8e
  TRUSTAR_SCORE_STD_ID: 1
  MYSQL_HOST: lacl-prod.cluster-cbjapnqaevbe.us-west-2.rds.amazonaws.com
  MYSQL_USER: apiuser
  MYSQL_PASSWORD: <omitted>
  MYSQL_DATABASE: lacldb
  MYSQL_PORT: 3306
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
MYSQL_CONNECTION_LIMIT: 100
CIS_URL: https://www.cisecurity.org/cybersecurity-threats/
CIS_ALERT_LEVEL_HTML_CLASS: .col-lg-3.col-lg-offset-1.col-md-4.col-sm-3.col-xs-12.alert-level.text-
white.popular-title
TRUSTAR_BATCH_REPORT_NOT_FOUND_EXPIRE_MIN: 120
aws:autoscaling:asg:
  MinSize: 1
  MaxSize: 5
aws:autoscaling:trigger:
  LowerThreshold: 20
  MeasureName: CPUUtilization
  Unit: Percent
  UpperThreshold: 60
aws:elasticbeanstalk:cloudwatch:logs:
  StreamLogs: true
  RetentionInDays: 14
aws:elasticbeanstalk:managedactions:
  ManagedActionsEnabled: true
  PreferredStartTime: "Sun:09:00"
aws:elasticbeanstalk:managedactions:platformupdate:
  UpdateLevel: minor
  InstanceRefreshEnabled: true
aws:elbv2:listener:443:
  DefaultProcess: default
  ListenerEnabled: true
  Protocol: HTTPS
  SSLCertificateArns: 'arn:aws:acm:us-west-2:032260193036:certificate/221aedf3-98d5-4147-a0f6-8072dc09ca5b'
  SSLPolicy: 'ELBSecurityPolicy-TLS-1-2-Ext-2018-06'
aws:elbv2:loadbalancer:
  ManagedSecurityGroup: sg-0cd1b2d6de6dce246
  SecurityGroups: sg-0cd1b2d6de6dce246
aws:ec2:vpc:
  ELBScheme: public
```

To build the environment for the first time, the following Elastic Beanstalk CLI command is run from the local project directory. Note that the user API access key and secret key must be configured within the CLI or available in environment variables in order to authorize access to the LACL AWS environment.

```
eb create lacl-prod -d -c lacl-api --elb-type application --instance_type t3.large --keyname ec2 --platform node.js --
region us-west-2 --scale 2 --vpc.id vpc-0de3230b38586ed27 --vpc.ec2subnets subnet-09fe826fe15eaacec,subnet-
00f04cc1b0274a8e5,subnet-0327d4671f7f4fa9d --vpc.publicip --vpc.elbsubnets subnet-
05dc458609d0a056e,subnet-01d8b296023e7e926,subnet-0f8fc5d43b02871df --vpc.elbpublic --vpc.securitygroups
sg-0ac97a78b530b5584 --debug
```

Once the environment is built, any API code updates can be deployed by simply running the following command from the local project directory:

```
eb-deploy
```


Los Angeles Cyber Lab – InfoSec Mobile Application

Elastic Beanstalk Environment Details

The Elastic Beanstalk environment that is created during the initial build is as follows:

- 2 t3.large EC2 instances that auto scale up to a maximum of 5 instances based on CPU usage
 - Deployed across the API Subnets within the LACL Production VPC
- 2 application load balancers
 - Deployed across the Load Balancer subnets within the LACL Production VPC
 - Leverages SSL certificate issued by Amazon certificate authority
- Amazon Linux, NodeJS 10.17.0 runtime, and LACL API deployed on EC2 instances
- Security groups defined within the LACL VPC are applied to the EC2 instances and load balancers
- Cloudwatch configured to ingest LACL API logs
- Cloudwatch configured to monitor autoscaling metrics

AWS Relational Database Service

Amazon Relational Database Service (Amazon RDS) is a managed service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity, while managing time-consuming database administration tasks, freeing up teams to focus on applications and business. Amazon RDS manages the work involved in setting up a relational database: from provisioning the infrastructure capacity requested to installing the database software. Once the database is up and running, Amazon RDS automates common administrative tasks such as performing backups and patching the software that powers the database. With LACL AWS Environment Multi-AZ deployments are configured and therefore Amazon RDS manages synchronous data replication across Availability Zones with automatic failover.

AWS RDS Environment Details

The AWS RDS environment that is created to support the LACL Middleware is as follows:

- 2 db.r4.large instance classes
 - 2 vCPUs and 15.25 GB of memory each
- Amazon Aurora MySQL 5.7.12 compliant databases
- Encryption is enabled
- The database is clustered across availability zones

Functions and stored procedures have been created in the database to support the functionality of the APIs. No API code make direct queries to the database, rather it prepared statements to execute stored procedures and functions. Below is the schema create statements for reference. All DB table, stored procedure and function definitions are stored in version control.

Los Angeles Cyber Lab – InfoSec Mobile Application

```
CREATE TABLE becExtSource
(
    becExtSourceId SMALLINT NOT NULL,
    sourceDescription VARCHAR(100) NULL,
    createdAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becExtSource
ADD CONSTRAINT becExtSource_PK PRIMARY KEY (becExtSourceId);

CREATE TABLE becIndicator
(
    becIndicatorId BINARY(16) NOT NULL,
    becIndicatorTypeId SMALLINT NOT NULL,
    indicatorValue VARCHAR(500) NOT NULL,
    createdAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    becScoreStdId SMALLINT NOT NULL,
    indicatorScore NUMERIC(5,2) NOT NULL,
    indicatorNotes VARCHAR(1000) NULL
);

ALTER TABLE becIndicator
ADD CONSTRAINT becIndicator_PK PRIMARY KEY (becIndicatorId);

CREATE UNIQUE INDEX becIndicator_AK1 ON becIndicator
(
    becScoreStdId ASC,
    becIndicatorTypeId ASC,
    indicatorValue ASC
);

CREATE TABLE becIndicatorType
(
    becIndicatorTypeId SMALLINT NOT NULL,
    indicatorDescription VARCHAR(100) NOT NULL,
    createdAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    indicatorTextId VARCHAR(20) NOT NULL
);

ALTER TABLE becIndicatorType
ADD CONSTRAINT becIndicatorType_PK PRIMARY KEY (becIndicatorTypeId);

CREATE UNIQUE INDEX becIndicatorType_AK1 ON becIndicatorType
(
    indicatorTextId ASC
);

CREATE TABLE becNotificationHistory
(
    becNotificationHistoryID BINARY(16) NOT NULL,
    IsNotified TINYINT NULL,
    createdAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    becReportId BINARY(16) NOT NULL,
    becStatusId SMALLINT NOT NULL,
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
notificationMessage VARCHAR(255) NOT NULL
);

ALTER TABLE becNotificationHistory
ADD CONSTRAINT becNotificationHistory_PK PRIMARY KEY (becNotificationHistoryID);

CREATE TABLE becReport
(
    becReportId      BINARY(16) NOT NULL,
    userProfileId    BINARY(16) NOT NULL,
    eMail            VARCHAR(100) NOT NULL,
    postalCode       VARCHAR(50) NOT NULL,
    reportTitle      VARCHAR(200) NOT NULL,
    externalId       VARCHAR(50) NULL,
    reportDate       TIMESTAMP NOT NULL,
    reportDetails    VARCHAR(1000) NULL,
    becStatusId      SMALLINT NOT NULL,
    becExtSourceId   SMALLINT NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    becScoreStdId    SMALLINT NOT NULL,
    reportScore      NUMERIC(5,2) NOT NULL
);

ALTER TABLE becReport
ADD CONSTRAINT becReport_PK PRIMARY KEY (becReportId);

CREATE INDEX becReport_IE1 ON becReport
(
    reportDate ASC
);

CREATE INDEX becReport_IE2 ON becReport
(
    becExtSourceId ASC,
    externalId ASC
);

CREATE TABLE becReportIndicator
(
    becReportId      BINARY(16) NOT NULL,
    becIndicatorId   BINARY(16) NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becReportIndicator
ADD CONSTRAINT becReportIndicator_PK PRIMARY KEY (becReportId,becIndicatorId);

CREATE TABLE becReportSector
(
    becReportId      BINARY(16) NOT NULL,
    userSectorId     SMALLINT NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becReportSector
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
ADD CONSTRAINT becReportSector_PK PRIMARY KEY (becReportId,userSectorId);

CREATE TABLE becScoreRisk
(
    riskDescription    VARCHAR(100) NOT NULL,
    recommendedActions VARCHAR(1000) NULL,
    scoreRiskFrom      NUMERIC(5,2) NOT NULL,
    scoreRiskTo        NUMERIC(5,2) NOT NULL,
    becScoreRiskId     SMALLINT NOT NULL,
    becScoreStdId      SMALLINT NOT NULL,
    createdAt          TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt          TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    riskScore          NUMERIC(5,2) NOT NULL
);

ALTER TABLE becScoreRisk
ADD CONSTRAINT becScoreRisk_PK PRIMARY KEY (becScoreRiskId);

CREATE TABLE becScoreStd
(
    becScoreStdId     SMALLINT NOT NULL,
    scoreStdDescription VARCHAR(100) NOT NULL,
    createdAt         TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt         TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becScoreStd
ADD CONSTRAINT becScoreStd_PK PRIMARY KEY (becScoreStdId);

CREATE TABLE becStatus
(
    becStatusId      SMALLINT NOT NULL,
    statusDescription VARCHAR(100) NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becStatus
ADD CONSTRAINT becStatus_PK PRIMARY KEY (becStatusId);

CREATE TABLE systemConfigGroup
(
    systemConfigGroupId SMALLINT NOT NULL,
    groupName           VARCHAR(100) NOT NULL,
    createdAt           TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt           TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE systemConfigGroup
ADD CONSTRAINT systemConfigGroup_PK PRIMARY KEY (systemConfigGroupId);

CREATE TABLE systemConfigValue
(
    configName        VARCHAR(100) NOT NULL,
    configValue       VARCHAR(100) NOT NULL,
    systemConfigGroupId SMALLINT NOT NULL,
    createdAt         TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt         TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
);

ALTER TABLE systemConfigValue
ADD CONSTRAINT systemConfigValue_PK PRIMARY KEY (configName);

CREATE TABLE userDevice
(
    userDeviceId    BINARY(16) NOT NULL,
    userProfileId    BINARY(16) NOT NULL,
    deviceId         VARCHAR(100) NULL,
    allowPushNotification TINYINT NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    fcmToken         VARCHAR(255) NULL
);

ALTER TABLE userDevice
ADD CONSTRAINT userDevice_PK PRIMARY KEY (userDeviceId);

CREATE TABLE userEmail
(
    userEmailId    BINARY(16) NOT NULL,
    userProfileId    BINARY(16) NOT NULL,
    registeredEmail VARCHAR(100) NULL,
    verified        TINYINT NOT NULL,
    isProfileEmail  tinyint NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    verifyToken     VARCHAR(500) NULL,
    verifyExpiry    TIMESTAMP NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE userEmail
ADD CONSTRAINT userEmail_PK PRIMARY KEY (userEmailId);

CREATE UNIQUE INDEX userEmail_AK1 ON userEmail
(
    registeredEmail ASC
);

CREATE TABLE userProfile
(
    userProfileId    BINARY(16) NOT NULL,
    password         VARCHAR(500) NULL,
    postalCode       VARCHAR(50) NOT NULL,
    roleId           SMALLINT NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    passwordResetToken VARCHAR(500) NULL,
    passwordResetExpiry TIMESTAMP NULL DEFAULT CURRENT_TIMESTAMP,
    firstName        VARCHAR(32) NOT NULL,
    lastName         VARCHAR(32) NOT NULL
);

ALTER TABLE userProfile
ADD CONSTRAINT userProfile_PK PRIMARY KEY (userProfileId);

CREATE TABLE userProfileSector
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
(
    userProfileId    BINARY(16) NOT NULL,
    userSectorId     SMALLINT NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE userProfileSector
ADD CONSTRAINT userProfileSector_PK PRIMARY KEY (userProfileId,userSectorId);

CREATE TABLE userRole
(
    roleId           SMALLINT NOT NULL,
    roleDescription  VARCHAR(100) NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE userRole
ADD CONSTRAINT userRole_PK PRIMARY KEY (roleId);

CREATE TABLE userSector
(
    userSectorId     SMALLINT NOT NULL,
    sectorDescription VARCHAR(100) NOT NULL,
    createdAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP,
    updatedAt        TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

CREATE TABLE becReportUpdateHistory
(
    becReportUpdateHistoryId BINARY(16) NOT NULL,
    becReportId             BINARY(16) NOT NULL,
    becStatusId             SMALLINT NOT NULL,
    createdAt               TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE becReportUpdateHistory
ADD CONSTRAINT becReportUpdateHistory_PK PRIMARY KEY (becReportUpdateHistoryId);

ALTER TABLE userSector
ADD CONSTRAINT userSector_PK PRIMARY KEY (userSectorId);

ALTER TABLE becIndicator
ADD CONSTRAINT becIndicatorType_becIndicator FOREIGN KEY (becIndicatorTypeId) REFERENCES becIndicatorType
(becIndicatorTypeId);

ALTER TABLE becIndicator
ADD CONSTRAINT becScoreStd_becIndicator FOREIGN KEY (becScoreStdId) REFERENCES becScoreStd (becScoreStdId);

ALTER TABLE becNotificationHistory
ADD CONSTRAINT becReport_becNotificationHistory FOREIGN KEY (becReportId) REFERENCES becReport (becReportId);

ALTER TABLE becNotificationHistory
ADD CONSTRAINT becStatus_becNotificationHistory FOREIGN KEY (becStatusId) REFERENCES becStatus (becStatusId);

ALTER TABLE becReport
ADD CONSTRAINT userProfile_becReport FOREIGN KEY (userProfileId) REFERENCES userProfile (userProfileId);
```

Los Angeles Cyber Lab – InfoSec Mobile Application

```
ALTER TABLE becReport
ADD CONSTRAINT becStatus_becReport FOREIGN KEY (becStatusId) REFERENCES becStatus (becStatusId);

ALTER TABLE becReport
ADD CONSTRAINT becExtSource_becReport FOREIGN KEY (becExtSourceId) REFERENCES becExtSource (becExtSourceId);

ALTER TABLE becReport
ADD CONSTRAINT becScoreStd_becReport FOREIGN KEY (becScoreStdId) REFERENCES becScoreStd (becScoreStdId);

ALTER TABLE becReportIndicator
ADD CONSTRAINT becIndicator_becReportIndicator FOREIGN KEY (becIndicatorId) REFERENCES becIndicator (becIndicatorId);

ALTER TABLE becReportSector
ADD CONSTRAINT becReport_becReportSector FOREIGN KEY (becReportId) REFERENCES becReport (becReportId);

ALTER TABLE becReportSector
ADD CONSTRAINT userSector_becReportSector FOREIGN KEY (userSectorId) REFERENCES userSector (userSectorId);

ALTER TABLE becScoreRisk
ADD CONSTRAINT becScoreStd_becScoreRisk FOREIGN KEY (becScoreStdId) REFERENCES becScoreStd (becScoreStdId);

ALTER TABLE systemConfigValue
ADD CONSTRAINT systemConfigGroup_systemConfigValue FOREIGN KEY (systemConfigGroupId) REFERENCES
systemConfigGroup (systemConfigGroupId);

ALTER TABLE userDevice
ADD CONSTRAINT userProfile_userDevice FOREIGN KEY (userProfileId) REFERENCES userProfile (userProfileId);

ALTER TABLE userEmail
ADD CONSTRAINT userProfile_userEmail FOREIGN KEY (userProfileId) REFERENCES userProfile (userProfileId);

ALTER TABLE userProfile
ADD CONSTRAINT userRole_userProfile FOREIGN KEY (userRoleId) REFERENCES userRole (userRoleId);

ALTER TABLE userProfileSector
ADD CONSTRAINT userSector_userProfileSector FOREIGN KEY (userSectorId) REFERENCES userSector (userSectorId);

ALTER TABLE becReportUpdateHistory
ADD CONSTRAINT becReport_becReportUpdateHistory FOREIGN KEY (becReportId) REFERENCES becReport (becReportId);

ALTER TABLE becReportUpdateHistory
ADD CONSTRAINT becStatus_becReportUpdateHistory FOREIGN KEY (becStatusId) REFERENCES becStatus (becStatusId);
```



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP) Mobile Application

LACL TISP Mobile Application Responsiveness

July 31, 2019

Contents

Overview.....	2
Terms	3
TRG – The Rosslyn Group.....	3
UX/UI – User Design/User Interface.....	3
LA Cyber Lab Mobile Application Responsiveness	4
1. Scope.....	4
2. Strategy & Testing.....	4
3. Revision History	5

Overview

The LACL Mobile Application was developed in an agile capacity over a 90-day timeline in the summer of 2019. The mobile app was designed, tested, released and beta tested to validate and prove design logic. The application is a light middleware interfacing between the user and the LACL's TISP data lake.

The mobile app is the primary means by which the LACL engages SMBs and individuals. Functionality of the mobile app was designed through a series of small SMB focus groups in conjunction with the LACL team.

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

TISP – Threat Intelligence Sharing Platform

TRG – The Rosslyn Group

UX/UI – User Design/User Interface

LA Cyber Lab Mobile Application Responsiveness

1. Scope

The LACL TISP and mobile application testing and development strategy are outlined within this document.

2. Strategy & Testing

With respect to Mobile Responsiveness Design and testing, TRG's UX/UI design team focused their approach on implementing an application that renders correctly across different devices, operating systems and screen sizes. TRG implemented the React framework to develop a modular, adaptable and fluid front-end design and user experience. Along with implementing React, The TRG UX/UI design team followed three development principles to ensure a responsive mobile application:

#1) The use of fluid Grids – This approach is based on the percentage of mobile real estate and not the historic pixel-based approach.

#2) Media Queries – This is used to apply different styles based on the device screen size.

#3) Flexible images and media – This helps to show the images and media differently in different sizes by using scaling or CSS.

Along with the development approach, it is equally important to test the application to ensure it is showing up as expected on all devices. A responsive application needs to give the same experience to the users across mobile operating systems and devices. It needs to be tested for device versions, different screen sizes, modes – landscape or portrait, etc. The content, videos, images, links, etc. all need to be tested for their appearance before releasing the application. For example, plotting on a map may look a little different on Android when compared to iOS. TRG executed the following test cases to ensure responsiveness of the mobile application across a variety of IOS and Android devices:

- 1) Verify whether the content fits on the screen and is not cut out or distorted.
- 2) Verify whether the feeds are loading and do not have broken links in them.
- 3) Verify whether the text color, the font etc, remain the same across devices.
- 4) Verify whether zooming in/out doesn't distort the map.
- 5) Verify whether fast scrolling doesn't distort the content.

- 6) Verify whether the links are working well and if they take the user to the appropriate page.
- 7) Verify whether the application back end calls are not timing out or taking too long to load.
- 8) Verify whether locking of portrait mode so content remains in the most optimum layout.
- 9) Verify whether the images of different types are shown as expected.
- 10) Verify whether navigating between cards in the mobile application doesn't distort the content etc.
- 11) Verify speed and responsiveness to query changes.

With regards to test case 11, TRG UX/UI design team calculated the impact of code and design choices on user experience. For example, typically, people get very frustrated if they have to wait more than one to two seconds for any UI feedback and therefore our mobile design aimed to load data dynamically to reduce the time to content access. For each iteration of the application, TRG measured timing differentials in already-deployed features so to ensure that future iterations didn't impact performance expectations.

3. Revision History

Date of Change	Responsible Party	Summary of Change
July 31, 2019	TRG	Original Draft
Oct. 18, 2019	LACL	Final Formatting and Content Update



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)

Supported by the U.S. Department of Homeland Security

Information Security and Management

LACL Data Retention Policy

November 12, 2019

Contents

Overview 2

Terms 3

LA Cyber Lab Data Retention Policy 4

Purpose 4

Scope 4

Policy 4

Figure 1. Data Retention Policy..... 5

Policy Compliance 6

Related Standards, Policies and Processes 6

Revision History 6

Overview

The LACL maintains several types of data including partner provided threat data, data received from the mobile application and member data. Data retention is based upon the type of data and the security controls associated with the data. Currently, the LACL is unaware of any data retention compliance requirements.

Terms

AWS – Amazon Web Services

BEC – Business Email Compromise

CTI – Cyber Threat Intelligence

IOC – Indicator of Compromise

LACL – Los Angeles Cyber Lab, LA Cyber Lab

TISP – Threat Intelligence Sharing Platform

LA Cyber Lab Data Retention Policy

1. Purpose

This policy establishes the retention period of data within systems owned by the LACL and for which the LACL is responsible for the disposition of deleted data. This includes system and log files that are a routine record of events on systems.

This policy outlines how long data and documents will or must be retained and provides a policy for when and how to dispose of data and documents that are eligible to be destroyed.

2. Scope

Sources of data for the LACL are:

- 1) Names, email addresses, contact information, etc. voluntarily provided by partners, members, event attendees, mobile application registration, and through social media;
- 2) IOCs from OSINT, closed networks, and partners;
- 3) Emails forwarded to the LACL TISP via the mobile application user;
- 4) Reports within the TISP which may or may not represent the collaboration of LACL and its partners;
- 5) Internal business information.

Data that has been exchanged and voluntarily shared with the LACL, data that has been deleted by the user from the system as well as system and log files that provide hardware or operating system event data used for compliance purposes or to diagnose problems will be retained in accordance with this policy.

For user generated and exchanged data, *retention* refers to the length of time a data file or document is stored in the system for reporting, compliance or business reasons.

3. Policy

3.1. Data Retention Roles

The retention of data and determination of useful retention of data and system logs is determined by system administrators under the direction of the Executive Director of the LACL. System administrators and database administrators are responsible for the execution of retention and adherence to the schedule.

3.2. Data Record Types

This policy addresses electronic data exchanged with, shared with and generated by LACL systems in various formats (e.g. .txt, .csv, STIX/TAXII,

RESTful API etc.), employee and staff saved and deleted email in Microsoft Exchange and Gmail, data stored in the general TISP Enclave or the BEC Enclave, data stored in the LACL mobile app middleware platform, data stored in any Amazon Web Services (AWS) cloud-based systems and all LACL systems provided for the use and the storage of LACL Cyber Threat Intelligence (CTI) data.

3.3. Record Retention - TISP

The data within the TISP will be retained indefinitely and will allow for searchable queries of IOCs. The data will be reviewed periodically, not to exceed one year, for retention purposes. At a minimum, data will be retained for 90 days to allow for trending, reporting and feeding dashboards used by the LACL partners.

3.4. Record Retention – Mobile App

The LACL Mobile App middleware architecture includes a cloud hosted (AWS) database which stores the user provided information. This information includes the user’s first name, last name, zip code and email addresses. Additionally, this database stores the first 1000 characters of the email subject submitted by the user. The data is retained indefinitely in the database, with the option to purge data upon user request. The mobile application only displays the last 30 days of data related to email submissions.

3.5. Record Retention – LACL Gmail and Shared Files

For the purpose of this document, employee and contractor data stored in LACL share-drives, shall be retained for one year or until no longer necessary. Procurement data will be retained for three years or until no longer necessary.

Figure 1. Data Retention Policy

RETENTION POLICY			
Data Type	Retention Period	Deletion Time Period	
TISP BEC Emails	PII – 30 days, once identified	Upon User Request	Up to 1 year
TISP LACL IOCs	Indefinite; minimum of 90 days	Upon Partner Request	When AWS storage is exhausted; oldest data will be purged
Mobile App User	Indefinite	Upon User Request	When AWS storage is exhausted; oldest data will be purged
Internal Data/Records	Minimum <3 years	When no longer necessary	When storage is exhausted; oldest data will be purged
Proprietary Data	Indefinite	When no longer necessary	Upon obsolescence

4. Policy Compliance

4.1. Compliance Measurement

The LACL team will verify compliance to this policy through various methods, including but not limited to, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

Any exception to the policy must be approved in writing by the Executive Director of the LACL in advance.

4.3. Non-Compliance

Any employees, contractors, consultants, temporary and other workers, Partners or Members found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

5.1. None

6. Revision History

Date of Change	Responsible Party	Summary of Change
Sept. 1, 2019	Rob Velasco	Original Draft
Sept. 24, 2019	Rob Velasco	Updated Content
Oct. 28, 2019	The Rosslyn Group	Updated Content
Nov. 12, 2019	LACL	Final Edits and Formatting



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Privacy Policy:

The purpose of this statement is to define the Los Angeles Cyber Lab, Inc.'s (LACL) policy with regards to the collection and use of personally identifiable information (PII – any information relating to an identified or identifiable individual who is the subject of the information).

Information Collected:

The LACL collects two kinds of user information – Anonymous Information and Personally Identifiable Information (PII).

Anonymous information is

information that does not identify specific individuals and is automatically transmitted by your browser. This information can consist of:

- The URL (Uniform Resource Locator or address) of the web page you previously visited
- The domain names and/or IP addresses which are numbers that are automatically assigned to your computer whenever you are connected to the Internet or World Wide Web
- The browser version you are using to access the site

This information is used to help improve our web site. None of the information can be linked to any individual.

Personally Identifiable Information (PII) is

information that could include:

- Name
- Address
- Email address
- Telephone number
- Credit/debit card information

The LACL will make every reasonable effort to protect your privacy. It restricts access to your personal identifiable information to those employees that will respond to your request. The LACL does not



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

intentionally disclose any personal information about our users to any third parties inside or outside the LACL except as required by law.

The LACL only collects personally identifiable information that is required to provide service. You can decline to provide us with any personal information on any site on the Internet at any time. However, if you should choose to withhold requested information, we may not be able to provide you with the online services dependent upon the collection of that information.

Access to Personally Identifiable Information

Access to personally identifiable information in public records at state and local levels of government in Los Angeles is controlled primarily by the California Public Records Act (Government Code Section 6250, et seq.). Information that is generally available under the Public Records Act may be posted for electronic access through the LACL's web site. While the Public Records Act sets the general policies for access to LACL records, other sections of California code as well as federal laws also deal with confidentiality issues.

E-mail Addresses

E-mail addresses obtained through the web site will not be sold or given to other private companies for marketing purposes. The information collected is subject to the access and confidentiality provisions of the Public Records Act, other applicable sections of the California code as well as federal laws. E-mail or other information requests sent to the LACL web site may be maintained in order to respond to the request, forward that request to the appropriate agency within the LACL, communicate updates to the LACL page that may be of interest to citizens, or to provide the LACL web designer with valuable customer feedback to assist in improving the site. Individuals can cancel any communications regarding new service updates at any time.

Cookies

Some LACL applications use "cookies." A cookie is a small data file that certain web sites write to your hard drive when you visit them. A cookie file can contain information such as a user id that the site uses to track the pages you have visited. But the only personal information a cookie can contain is information you supply yourself. A cookie is only a text file and cannot read data off your hard disk or read cookie files created by other sites. Cookies can track user traffic patterns, recognize your computer's browser when you return, and could provide personalized content without requiring sign-in.



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

You can refuse cookies by turning them off in your browser. However, they may be required to use some of the web applications on the LACL's site.

Google Analytics Cookie Tracking

Some LACL applications use Google Analytics cookies to log user sessions and help us understand traffic and behavior. This helps us analyze data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes.

Some LACL applications include the Google Analytics Display Advertising feature used to provide Demographics and Interest Reporting. This feature uses a third party DoubleClick Cookie.

To provide website visitors the ability to prevent their data from being used by Google Analytics, Google has developed the Google Analytics opt-out browser add-on for the Google Analytics JavaScript (ga.js, analytics.js, dc.js). This add-on instructs the Google Analytics JavaScript (ga.js, analytics.js, and dc.js) running on websites to prohibit sending information to Google Analytics. However, the Google Analytics opt-out browser add-on does not prevent data from being sent to the LACL's site. Visit <https://tools.google.com/dlpage/gaoptout/> for more info on how to opt out.

Please note that updates to your browser or operating system may affect the functionality of the opt-out add-on. The latest versions of Internet Explorer sometimes load the Google Analytics opt-out add-on after sending data to Google Analytics. Therefore, if you are using Internet Explorer, the add-on will set cookies on your computer. These cookies ensure that any collected data is immediately deleted from the collection server. Please make sure that third party cookies aren't disabled for your Internet Explorer browser. If you delete your cookies, the add-on will, within a short timeframe, reset these cookies to ensure that your Google Analytics browser add-on remains fully functional.

The following chart is a detailed list of Google Analytics cookies that would be used.

Cookie Name	Default Expiration Time	Description
ga	2 years	Used to distinguish users.



Los Angeles Cyber Lab, Inc.
 An Internet Security - Information Sharing & Analysis Organization

Cookie Name	Default Expiration Time	Description
gat	10 minutes	Used to throttle request rate.
utma	2 years from set/update	Used to distinguish users and sessions. The cookie is created when the javascript library executes and no existing __utma cookies exists. The cookie is updated every time data is sent to Google Analytics.
utmt	10 minutes	Used to throttle request rate.
utmb	30 mins from set/update	Used to determine new sessions/visits. The cookie is created when the javascript library executes and no existing __utmb cookies exists. The cookie is updated every time data is sent to Google Analytics.
utmz	6 months from set/update	Stores the traffic source or campaign that explains how the user reached your site. The cookie is created when the javascript library executes and is updated every time data is sent to Google Analytics.
utmc	End of browser session	Not used in ga.js. Set for interoperability with urchin.js. Historically, this cookie operated in conjunction with the __utmb cookie to determine whether the user was in a new session/visit.
utmv	2 years from set/update	Used to store visitor-level custom variable data. This cookie is created when a developer uses the _setCustomVar method with a visitor level custom variable. This cookie was also used for the deprecated _setVar method. The cookie is updated every time data is sent to Google Analytics.
DoubleClick		Google Analytics Demographics and Interest Reporting



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Cookie Name	Default Expiration Time	Description
Cookie Name	Default Expiration Time	Description
ga	2 years	Used to distinguish users.
gat	10 minutes	Used to throttle request rate.
utma	2 years from set/update	Used to distinguish users and sessions. The cookie is created when the javascript library executes and no existing __utma cookies exists. The cookie is updated every time data is sent to Google Analytics.
utmt	10 minutes	Used to throttle request rate.
utmb	30 mins from set/update	Used to determine new sessions/visits. The cookie is created when the javascript library executes and no existing __utmb cookies exists. The cookie is updated every time data is sent to Google Analytics.
utmc	End of browser session	Not used in ga.js. Set for interoperability with urchin.js. Historically, this cookie operated in conjunction with the __utmb cookie to determine whether the user was in a new session/visit.
utmz	6 months from set/update	Stores the traffic source or campaign that explains how the user reached your site. The cookie is created when the javascript library executes and is updated every time data is sent to Google Analytics.
utmv	2 years from set/update	Used to store visitor-level custom variable data. This cookie is created when a developer uses the _setCustomVar method with a visitor level custom variable. This cookie was also used for the deprecated _setVar



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

Cookie Name	Default Expiration Time	Description
		method. The cookie is updated every time data is sent to Google Analytics.
DoubleClick		Google Analytics Demographics and Interest Reporting

Minor's Privacy Policy

Any information collected by any LACL site from children under 13 are subject to the same guidelines as the general LACL privacy policy. In addition, the following guidelines will be followed for any information collected by or for any child under 13:

- Information that could be collected from or for a minor includes but might not be limited to name, address, telephone number, e-mail address, school, and hobbies.
- Parental (including legal guardian) Consent
- Parental consent will be obtained before collecting, using or disclosing personal information about a child.
- If any information practices change in a “material” way, new consent will be obtained from the parents. This includes changes in the kinds of material being collected, a change in how that information is being used, or if there is a change in the third parties that have access to that information.
- Parents will be able to review the personal information collected from their children which includes verification of the identity of the requesting parent. See individual requests for information for specifics.
- Parents will be allowed to revoke their consent and delete information collected from or for their children on request. When consent is revoked, the website will stop collecting, using or disclosing information from or for that child. Revocation may end a child’s participation in an activity if the information collected was necessary for participation on the website.
- Additional information can be obtained at the FTC’s Consumer Response Center (<http://www.ftc.gov/privacy/index.html>) and the Children’s Privacy (<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy1>) websites.

Security

Los Angeles Cyber Lab, Inc.
200 N. Spring Street, Suite 303 | Los Angeles, CA 90012-3239
www.lacyberlab.org



Los Angeles Cyber Lab, Inc.
An Internet Security - Information Sharing & Analysis Organization

The LACL is committed to data security and the data quality of personally identifiable information that is either available from or collected by our web site and has taken reasonable precautions to protect such information from loss, misuse or alteration.

The LACL operates “secure data networks” protected by industry standard firewalls and password protection systems. Only authorized individuals have access to the information provided by our users.

When a LACL application accepts credit cards or any other particularly sensitive information for any of its services, it encrypts all ordering information, such as your name and credit card number, in order to protect its confidentiality.

Access to Your Information

Unless otherwise prohibited by state or federal law, rule or regulation you will be granted the ability to access and correct any personally identifiable information. We will take reasonable steps to verify your identity before granting access to review or make corrections to your information. Each LACL service that collects personally identifiable information will allow for review and update of that information. See individual requests for information for specifics.

Non LACL Web Sites

Non-LACL web sites may be linked through the LACL’s web site. Many non-LACL sites may or may not be subject to the Public Records Act and may or may not be subject to other sections of California Code or federal law. Visitors to such sites are advised to check the privacy statements of such sites and to be cautious about providing personally identifiable information without a clear understanding of how the information will be used. Visitors may also wish to consult privacy guidelines such as those recommended by the Online Privacy Alliance (<http://www.privacyalliance.org/resources/ppguidelines.shtml>).

How to Contact Us

If you have any questions or concerns about this privacy policy, please send us an email at dev@lacyberlab.org.

Date last modified: September 5, 2019



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP) Mobile Application

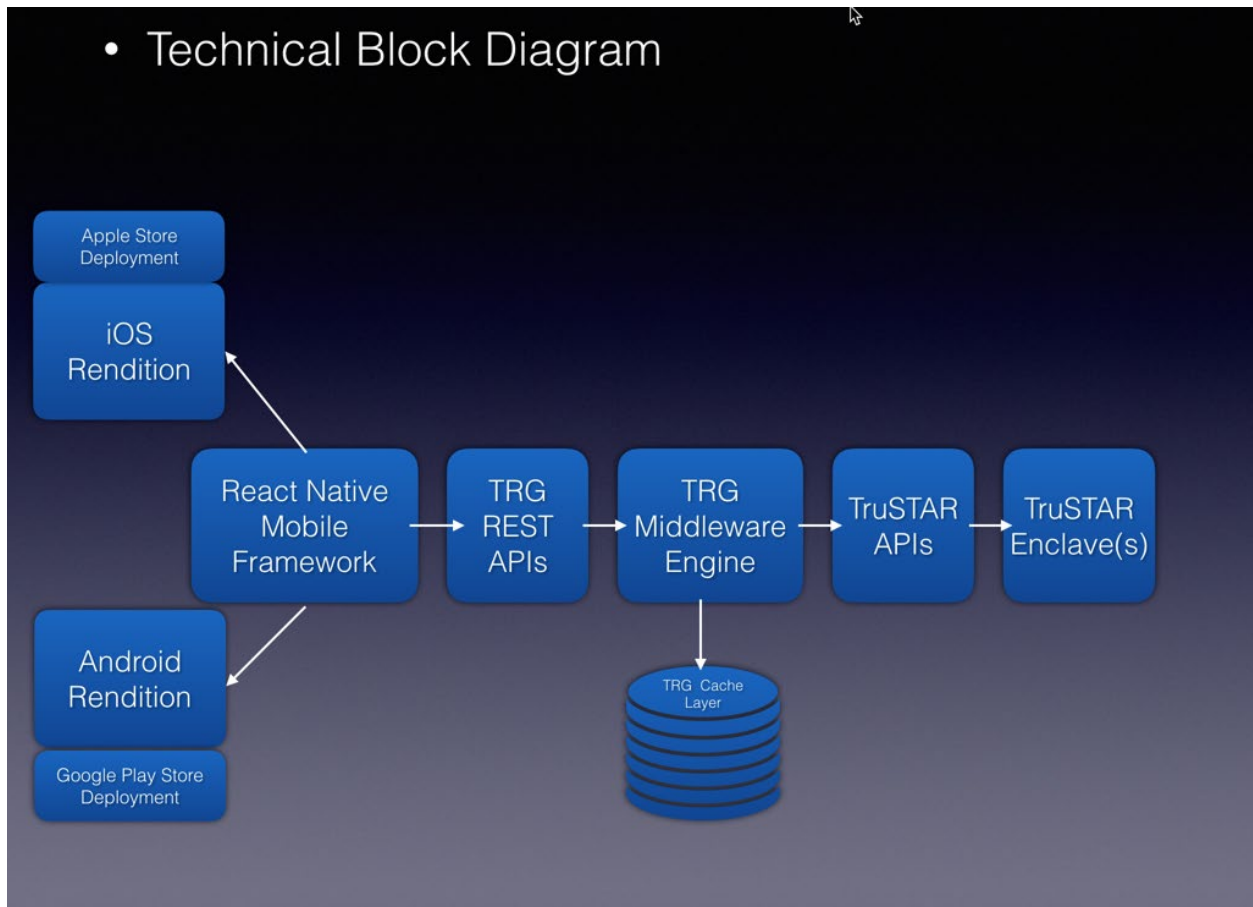
LACL Middleware Technical Documentation

September 30, 2019

Contents

Overview Technical Diagram	2
Terms	3
eMail Process.....	4
TruSTAR BEC Score Update Process	6
TruSTAR Process Diagram.....	7
Enclave Ids	8
Get BEC Reports API	8
Get BEC Reports Indicators API.....	8
Get X-Force Indicator Correlating Reports API	8
Get X-Force Report Score API.....	9

Overview Technical Diagram



The LACL mobile application is designed as a middleware application which wraps around the API of an existing threat intelligence sharing portal; in this instance the TISP is maintained and managed by TruSTAR. The mobile application created, by The Rosslyn Group (TRG), operates on Apple iOS and Android platforms. The mobile application is available for download in Google and Apple app stores.

TRG designed the middleware to be interchangeable with other APIs. The initial most viable product (VMP) was created to provide the following:

- Ingest an email from a known user with a validated account and provide a response via the mobile application regarding the malicious content of the email
- Provide trending data for users in the Los Angeles region about the threats
- Provide cybersecurity awareness through various news feeds

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

MU – Mobile Users

MW – LACL Middleware Tier

MWDB – LACL Middleware Relational Database

MVP – Most Viable Product

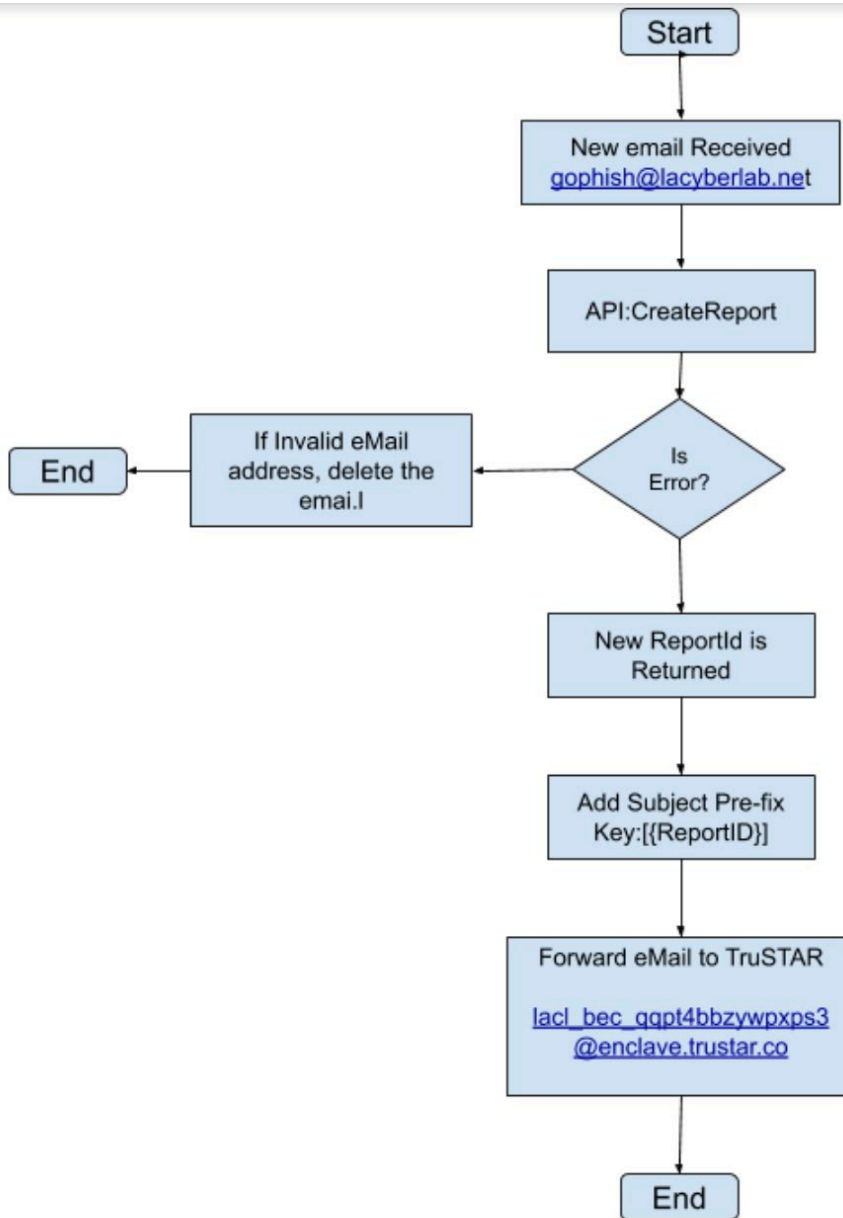
TISP – Threat Intelligence Sharing Platform

TRG – The Rosslyn Group

UUID - Universally Unique Identifier

eMail Process

The MU will forward any suspicious emails to the LACL inbox (gophish@lacyberlab.net). This event will trigger the MW to perform the following tasks.



Los Angeles Cyber Lab – TISP Mobile Application

- The mobile user will forward all suspicious emails to the LA Cyber Lab email address gophish@lacyberlab.net and gophishtest@lacyberlab.net
- The email inbox is hosted in AWS SES (Simple Email Services)
- Upon receiving an email, SES will trigger an API call to CreateReport.
- The sender's email address against MWDB registered emails.
- If the email is not registered or validated, an error is raised. The email will be deleted and ignored.
- If the email comes from a valid registered user, it will perform the following tasks:
 - It will create a new record in the MWDB using the API
 - The new record will be created with a status of 1-new.
 - The API will return the UUID for the newly created record.
 - The new UUID will be appended to the email subject line prefix:
Key:[UUID]
- The email is forwarded in its entirety to the TruSTAR inbox email address: lacl_bec_sizpvp2vfrnynvq@enclave.trustar.co
- A push notification is sent to the mobile user confirming the email receipt.
- AWS is event trigger is responsible for handling and retrying all other errors.

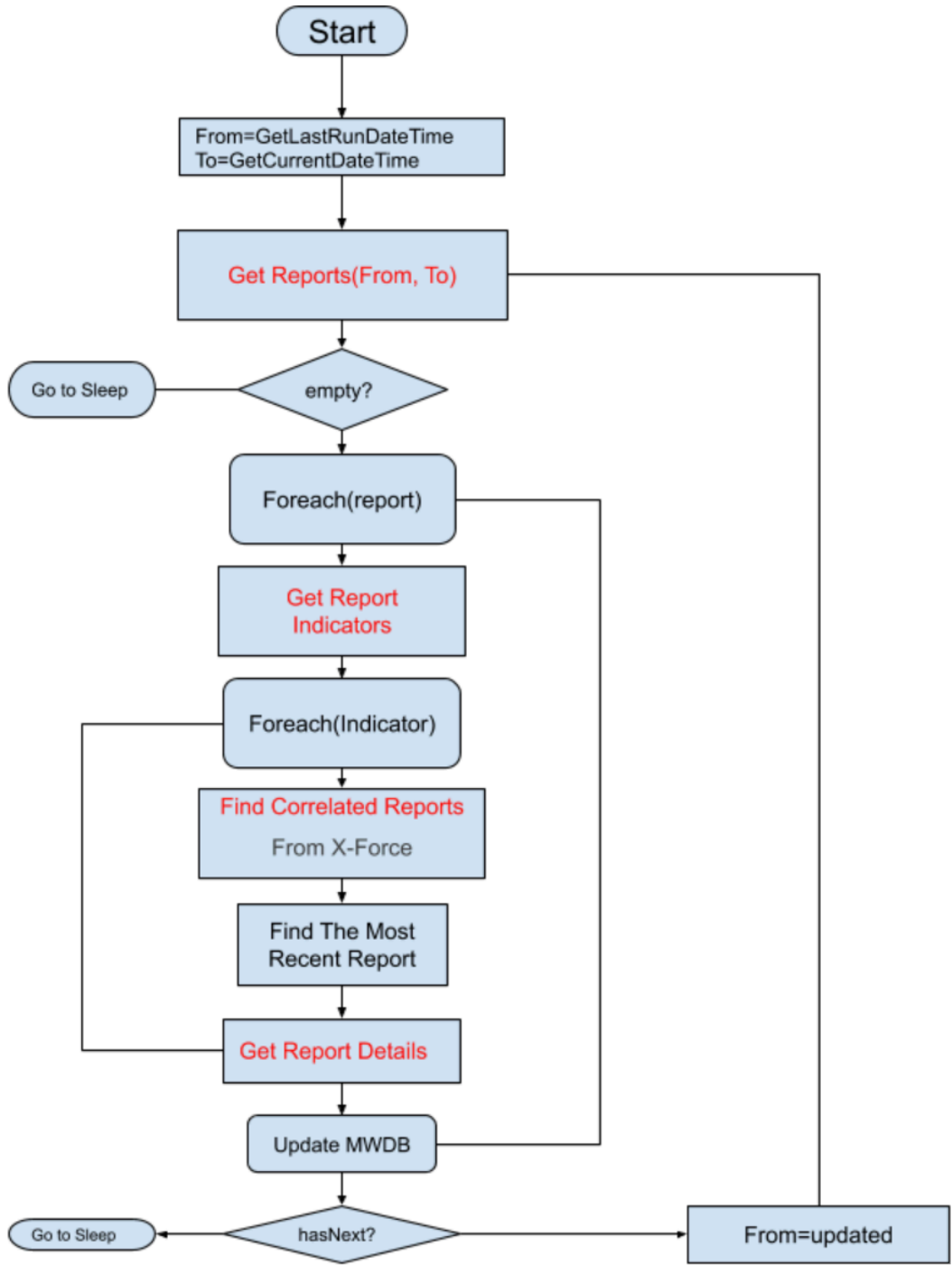
TruSTAR BEC Score Update Process

The BEC data is initially submitted to the LACL enclave through the TruSTAR email inbox. Using an asynchronous process, TruSTAR parses the emails to extract the relevant data. The parsed data is ingested into the BEC enclave to be scored. As the data is ingested into the enclave, TruSTAR starts the next phase of its internal process which is responsible for identifying the relevant indicators. Each indicator is then assessed and scored according to its risk and malicious relevance on the scale of 1-10.

The MW is responsible for reading the resulting indicators and their scores back into the MWDB. MW performs the following tasks:

- Query TruSTAR to retrieve the most recent updated data based on the updated date timestamp.
- MW will keep track of the last time it asked TruSTAR for data in a configuration table (LastQueryDateTimeStamp).
- When the data is read successfully, MW will update the (LastQueryDateTimeStamp) configuration value to the new timestamp.
- MW will wait a configurable period of time to start reading process over again.

TruSTAR Process Diagram



Enclave Ids

Enclave Name	Enclave ID	Notes
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb	
IBM X-Force	cfa7b4ef-f30b-4773-92d7-c33a70af1e8e	

Get BEC Reports API

<https://api.trustar.co/api/1.3/reports?enclaveid=08d99eac-d197-4193-86d9-b637a70df1cb&from=1563390000000&to=1563465245297>

Parameter name	Data Type	Description
enclaveid	UUID	LACL BEC UUID
from	Epoch timestamp	Start date in milisecond
to	Epoch timestamp	End date in milisecond

More information: https://docs.trustar.co/api/v13/reports/get_reports.html

Get BEC Reports Indicators API

["https://api.trustar.co/api/1.3/reports/{fid}/indicators?idType=internal"](https://api.trustar.co/api/1.3/reports/{fid}/indicators?idType=internal)

Parameter name	Data Type	Description
id	UUID	Report ID
idType	string	internal or external

More information: https://docs.trustar.co/api/v13/indicators/get_indicators_for_report.html

Get X-Force Indicator Correlating Reports API

<https://api.trustar.co/api/1.3/reports/correlated?indicators=WANNACRY&enclaveids=cfa7b4ef-f30b-4773-92d7-c33a70af1e8e>

Parameter name	Data Type	Description
----------------	-----------	-------------

Los Angeles Cyber Lab – TISP Mobile Application

indicators	string	indicator value of any type; i.e. an IP address, email address, URL, MD5, SHA1, SHA256, Registry Key, Malware name, etc.
enclavelds	uuid	X-force: (cfa7b4ef-f30b-4773-92d7-c33a70af1e8e)

More information: https://docs.trustar.co/api/v13/reports/find_correlated_reports.html

Get X-Force Report Score API

<https://api.trustar.co/api/1.3/reports/{id}>

Parameter name	Data Type	Description
id	string	Report id

More information: https://docs.trustar.co/api/v13/reports/get_report_details.html



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)

Supported by the U.S. Department of Homeland Security

Information & Data Security

LACL Configuration Management Policy – Mobile Application

January 21, 2020

Contents

Overview	2
Terms	3
Configuration Management Policy	4
1. 4	
2. 4	
3. 4	
3.4.1 Policy “Establish/maintain baseline configurations/inventories of information systems”	5
3.4.2 Policy “Establish and enforce security configurations for information technologies”	6
3.4.3 Policy “Track, review and approve configuration changes to information systems”	7
3.4.4 Policy “Analyze the security impact of changes prior to implementation”	8
3.4.5 Policy “Define, document, approve and enforce physical & logical access restrictions”	9
3.4.6 Policy “Employ principle of least functionality”	9
3.4.7 Policy “Restrict, disable and prevent the use of nonessential functions”	10
3.4.8 Policy “Apply Blacklisting and Whitelisting technologies”	11
3.4.9 Policy “Control and monitor user installed software”	11
4. 12	
5. 12	
6. 14	
7. 14	

Overview

The LA Cyber Lab maintains the configuration and change management processes for the *LACL Mobile App*. The configuration management process is essential to maintaining a chain of custody in the decision making and approvals of changes to the mobile app. The mobile app has been configured in such a manner as to meet the specifications of the LACL's user interface and business email compromise use cases as part of its "Connecting the Community" initiatives.

Terms

Build is an operational version of a system or component that incorporates a specified subset of the capabilities that the final product shall provide.

Configuration Baseline is configuration information formally designated at a specific time during a product's or product component's life. Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.

Configuration is the functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

Configuration Item is an aggregation of work products that is designated for configuration management and treated as a single entity in the configuration management process. This aggregation consists of all required components: hardware, software, and other items that comprise a baseline.

Configuration Management is a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

Information System (IS) and Information Technology (IT) applies within the context of supporting LA Cyber Lab IT systems.

LACL – Los Angeles Cyber Lab, LA Cyber Lab

Local Security Policy (LSP) in Microsoft Windows allows the enforcing of many system, user, and security related settings, such as password policy, audit policy, and user permissions.

Operating System (OS) means the software on the hard drive that enables the computer hardware and software resources to communicate and operate with the computer software.

Production Data is data that belongs to an individual, or can identify an individual, or that is otherwise considered Regulatory Protected Information.

TISP – Threat Intelligence Sharing Platform

TRG – The Rosslyn Group

Configuration Management Policy

1. PURPOSE

This policy and supporting procedures are designed to provide a documented and formalized Configuration Management policy that is to be adhered to at all times. Compliance with the stated policy and supporting procedures helps ensure the security, resiliency, and function of the systems that support and serve the LA Cyber Lab mission.

2. SYSTEM SCOPE

This policy and supporting procedures encompass all system resources that are owned, operated, maintained, and controlled by the LA Cyber Lab and all other system resources, both internally and externally, that interact with LA Cyber Lab systems, which include:

- Internal production and development system resources owned, operated, maintained, and controlled by the LA Cyber Lab. Including all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.
- Externally hosted system resources are those owned, operated, maintained, and controlled by any entity other than LA Cyber Lab, but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of internal system resources.
- When referencing the term “users”, this includes any individual that has been granted remote access rights by LA Cyber Lab and has went through all required provisioning steps.

For purpose of this policy, Configuration Management is defined as the following: the method and discipline for evaluating, coordinating, approving or disapproving, or implementing changes in artifacts; an artifact may be a piece of hardware, software, or documentation.

3. POLICY DEFINITIONS

The LA Cyber Lab shall ensure that the Configuration Management policy adheres to the following conditions for purposes of complying with security requirements set forth by NIST SP 800-171 and NIST 800-53 and approved by management. All requirements governed by this policy apply to the **LA Cyber Lab Mobile Application and Threat Intelligence Sharing Platform (TISP)** production environments.

- 3.4.1 Establish and maintain baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- 3.4.2 Establish and enforce security configuration settings for information technology products employed in information systems.
- 3.4.3 Track, review, approve/disapprove, and audit changes to information systems.
- 3.4.4 Analyze the security impact of changes prior to implementation.
- 3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- 3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities.
- 3.4.7 Restrict, disable, and prevent the use of nonessential functions, ports, protocols, and services.
- 3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- 3.4.9 Control and monitor user-installed software.

POLICY

3.4.1 Policy “Establish and maintain baseline configurations and inventories of information systems”

Baseline configurations serve as a foundation for future builds, releases, and/or changes to information systems. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current architecture. Industry standard configuration baselines for commonly used operating platforms shall be leveraged to ensure security settings are appropriate.

LA Cyber Lab shall develop, document, and maintain a current baseline configuration for information systems, which may include the following:

- Baseline configurations about information system components
 - Standard software packages installed on workstations notebook computers, servers, network components, or mobile devices.
 - Current version numbers and patch information on operating systems and applications; and configuration settings/parameters)
- Network topology and the logical placement of those components within the system architecture.

INVENTORIES

Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

LA Cyber Lab shall develop and document an inventory of information system components that:

- Accurately reflects the current information system
 - Hardware
 - Software
 - Criticality rating
- Includes all components within the authorization boundary of the information system
- Provides granularity necessary for tracking and reporting
- Updates the inventory of components as part of component installations, removals, and updates.

3.4.2 Policy “Establish and enforce security configurations for information technologies”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth that apply to “Configuration and hardening management”:

Background

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

LA Cyber Lab manages security-related parameters, which are parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example:

- Account, file and directory permission settings
- Settings for functions, ports, protocols, services, and remote connections

LA Cyber Lab shall establish organization-wide configuration settings to subsequently manage specific settings for information systems. The established settings are part of the systems configuration baseline. Common secure configuration guides provide recognized, standardized, and established benchmarks that validate secure configuration settings for specific information technology platforms, products, and instructions.

LA Cyber Lab shall establish and document configuration settings for information technology products employed within the information system using:

- Security configuration guides that reflect the most restrictive mode consistent with operational requirements.
- Identifies, documents, and approves any deviations from established configuration settings.

3.4.3 Policy “Track, review and approve configuration changes to information systems”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth and approved by management that apply to “Configuration review and approval”:

Background

Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

LA Cyber Lab shall implement processes for managing configuration changes to information systems that include:

- For new development information systems or upgrades, a change control meeting shall be conducted including representatives from respective development organizations and management.
- Tracking changes includes activities before and after changes are made to information systems.
- Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.

An active "implement or defer" process is currently in place in which "fixes" are accepted and "deferrals" are dispositioned appropriately.

3.4.4 Policy “Analyze the security impact of changes prior to implementation”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth and approved by management that apply to “Change impact”:

Background

Organizational personnel with information security responsibilities (e.g., Information System Administrators, Product Owners, Development Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analyses are scaled in accordance with the security categories of the information systems.

LA Cyber Lab analyzes changes to the information system to determine potential security impacts prior to change implementation by:

- Conducting security impact analysis, which includes, reviewing security plans to understand security control requirements and reviewing system design

documentation to understand control implementation and how specific changes might affect the controls.

- Conducting security impact analyses, which also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required.
- Before implementation, changes are tested in development environment.

3.4.5 Policy “Define, document, approve and enforce physical and logical access restrictions”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth that apply to “Physical and logical access restrictions”:

Background

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems.

Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3 in NIST 800-53), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

LA Cyber Lab shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system by:

- Permitting only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications.
- Maintaining records of access to ensure that configuration change control is implemented and to support after-the-fact actions shall organizations discover any unauthorized changes.

3.4.6 Policy “Employ principle of least functionality”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth that apply to “The principle of least functionality”:

Background

Information systems provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). It is sometimes convenient to provide multiple services from single information system components,

but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing).

Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

LA Cyber Lab shall employ least functionality principles by configuring the information system to provide only essential capabilities by:

- Prohibiting or restricting the use of the following functions, ports, protocols, and/or services for applications and software services.
- Disabling unused or unnecessary physical and logical ports/protocols on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.
- Using scanning tools to detect and remediate unnecessary services and systems.

3.4.7 Policy “Restrict, disable and prevent the use of nonessential functions”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth that apply to “Use of nonessential functions”:

Background

The organization shall make a determination for the relative security of the function, port, protocol, and/or service, or base the security decision on the assessment by third parties.

LA Cyber Lab reviews the information system before a major software release to identify unnecessary and/or non-secure functions, ports, protocols, and services by:

- Disabling specific functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.
- Preventing program execution in accordance with approved technology lists and software program usage guidelines.
- Providing a list of approved software to personnel.

3.4.8 Policy “Apply Blacklisting and Whitelisting technologies”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth and approved by management that apply to “Whitelist and blacklist technologies”:

Background

The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

LA Cyber Lab identifies software programs authorized to execute on the information system by:

- Employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.
- Reviewing and updating LA Cyber Lab’s list of authorized software programs before a major software release.

The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. If adopted, blacklisting rules shall include:

- Employing an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.
- Reviewing and updating LA Cyber Lab’s list of unauthorized blacklisted software program before a major software release.

3.4.9 Policy “Control and monitor user installed software”

LA Cyber Lab has defined its Configuration Management policy to adhere to the following conditions set forth that apply to “User installation of software”:

Background

If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved app stores.

Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The

policies organizations select governing user-installed software may be organization-developed or provided by a third-party entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

LA Cyber Lab shall establish govern the installation of software by users by:

- Manually enforce software installation through local security policy.
- Monitor policy compliance by monthly scanning technologies (i.e. vulnerability scans).

4. POLICY MAINTENANCE

The LA Cyber Lab is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with mandated organizational security requirements set forth and approved by management.

5. CONFIGURATION MANAGEMENT PLAN CHECKLIST (BASED ON NIST 800-171)

Overview

The **Configuration Management Checklist** provides a review of the objectives established in the LA Cyber Lab Configuration Management Policy. In addition, this checklist serves as a guide to assist in the identification of required Configuration Management procedures, and to provide a high-level outline of the LA Cyber Lab Configuration Management Plan.

Purpose

This policy addresses the establishment of configuration management policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

When developing a Configuration Management process, the process shall be designed with best practices in mind and verifying they meet or exceed the security requirements in NIST SP 800-171 which are outlined below.

Basic Security Requirements

- **CM-2 (Baseline Configuration)** - The organization defines and updates the baseline configuration as an integral part of information system component installations.
- **CM-6 (Configuration Settings)** - The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.
- **CM-8 (Information Systems Component Inventory)** - The organization develops and documents an inventory of information system components that accurately reflects the current information system; and Includes all components within the authorization boundary of the information system;
- **CM-8 (1) (Information Systems Component Inventory - Updates)** - The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Derived Security Requirements

- **CM-3 (Configuration Change Control)** - The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.
- **CM-4 (Security Impact Analysis)** The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
- **CM-5 (Access Restrictions for Change)** The organization enforces access restrictions associated with changes to the information system.
- **CM-7 (Least Functionality)** The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].
- **CM-7 (1) (Least Functionality – Periodic Review)** The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.

- **CM-7 (2) (Least Functionality – Prevent program execution)** The information system prevents program execution in accordance with Selection (one or more): Assignment: organization-defined policies regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- **CM-7 (4) (Least Functionality – Blacklisting)** The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.

- **CM-7 (5) (Least Functionality – Whitelisting)** The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

- **CM-11 (User Installed Software)** The organization establishes [Assignment: organization-defined policies] governing the installation of software by users.

6. REFERENCES

NIST 800- 66 (HIPAA Security Rule)

NIST 800-171 (Protecting Controlled Information in Information Systems)

7. REVISIONS HISTORY

Date of Change	Responsible Party	Summary of Change
Oct. 14, 2019	TRG	Original Draft
January 21, 2020	LACL	Final Formatting and Content Update



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)

Supported by the U.S. Department of Homeland Security

Information Protection & Security

LACL Change Management Policy

November 1, 2019

Contents

- Overview 2
- Terms 3
- Change Management Policy 4
 - Purpose 4
 - Scope 4
 - Policy 4
 - Policy Compliance 5
- Appendix A – Types of Changes 6
 - Types of Changes 6

Overview

Changes to IT systems can be a major root cause of attack vectors inside and outside of an organization. It is crucial that any change to any major IT system be assessed for both expected functionality and vulnerabilities and unplanned or unexpected discoveries be remediated prior to production deployment.

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

CA – Change Authority

CRF – Change Request Form

Change Management Policy

1. Purpose

Change Management refers to a formal process for making changes to IT systems. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimizes negative impact to services and customers.

This policy establishes the change management process and associated approvals for systems owned by the LACL and for which the LACL is responsible for. This policy outlines documentation, information and signatures required to make a change to an IT system.

2. Scope

This policy applies to all changes to architectures, tools and IT Services provided by the LACL after acceptance of a system and it is placed into production. Modifications made to non-production systems (such as testing environments with no impact on production IT Services) are outside the scope of this policy.

3. Policy

All Changes to IT services must follow a structured process to ensure appropriate planning and execution.

By ITIL definition there are three types of changes: (a) a Standard Change, (b) a Normal Change (of low, medium, or high risk), and (c) an Emergency Change. See “Appendix A – Types of Changes for more detailed definitions. Each Change Authority must establish an appropriate complete change management process commensurate with the type of change being authorized.

- 3.1. All Changes must follow a process of planning, evaluation, review, approval, and documentation.
- 3.2. The LACL Executive Director serves as the default Change Authority (CA) for changes to IT systems and has the authority to determine change type and risk level. If in doubt, a higher level of risk should be assumed and additional review and approval should be sought by the Board.
- 3.3. All changes must have documented procedures in place that have been approved by the CA.
- 3.4. All Emergency Changes must be authorized by the CA and submitted for review by the Board in retrospect to ensure that effective oversight was maintained and proper communication and coordination occurred.
- 3.5. Documentation of Standard, Normal and Emergency Changes must be made in a process log that is stored in a common location so that coordination of changes across the organization can be managed appropriately. They should also be logged in a manner that can be audited for process improvement and root cause diagnosis as part of Problem

Management.

- 3.6. All proposed changes will be submitted by the **Requestor**. Change Management responsibilities for the Requestor include the following tasks:
 - 3.6.1. Prepare the **LACL Change Request Form (CRF)** and submit to the LACL Executive Director for review and consideration.
 - 3.6.2. If appropriate, incorporate feedback from the LACL Executive Director into the CRF
 - 3.6.3. Document the outcome of the change
- 3.7. Proposed changes and associated CRFs will be approved by the **Change Authority**.
- 3.8. Change Management responsibilities for the Change Authority include the following tasks:
 - 3.8.1. Provide advisory input to the Requestor on any needed changes to the CRF prior to approval, including any follow up communication necessary for clarification during the change process
 - 3.8.2. Review and approve CRFs
 - 3.8.3. Review change outcomes and make process changes appropriate to increase service availability and service quality.

4. Policy Compliance

- 4.1. Compliance Measurement
 - 4.1.1. The LACL will verify compliance to this policy through various methods, including but not limited to, periodic reviews, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
- 4.2. Exceptions
 - 4.2.1. Any exception to the policy must be approved in writing by the Executive Director of the LACL in advance.
- 4.3. Non-Compliance
 - 4.3.1. Any employees, contractors, consultants, temporary and other workers, Partners or Members found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

- 5.1. LACL Change Request Form (CRF)

6. Revision History

Date of Change	Responsible Party	Summary of Change
Sept. 26, 2019	Rob Velasco	Original Draft
Nov.1, 2019	LACL	Formatting & Final Updates

Appendix A – Types of Changes

Types of Changes

There are three types of changes:

1. **Standard Change** – A repeatable change that has been pre-authorized by the Change Authority by means of a documented procedure that controls risk and has predictable outcomes (e.g. routine patching, maintenance, etc.).
2. **Normal Change** – A change that is not an Emergency change or a Standard change. Normal changes follow the defined steps of the change management process.
3. **Emergency Change** – A change that must be introduced as soon as possible due to likely negative service impacts. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps due to the urgent nature of the issue; however, any Emergency Change must still be authorized by the Executive Director and reviewed by the Board retroactively.



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)

Supported by the U.S. Department of Homeland Security

Information Protection & Security

LACL Password Policy

September 30, 2019

Contents

Overview.....	2
Terms	3
Password Policy.....	4
1. Purpose.....	4
2. Scope	4
3. Policy	4
3.1. Strong Passwords.....	4
3.2. Weak Passwords	5
3.3. Password Creation.....	5
3.4. Password Change.....	5
3.5. Password Protection	5
3.6. Application Development	5
3.7. Additional Requirements	6
4. Policy Compliance	6
5. Related Standards, Policies and Processes	6
6. Revision History	6

Overview

Information protection and security are critical to the success of every ISAO; the LA Cyber Lab is successful based upon its ability to maintain trust amongst its partners and members. Therefore, it is necessary to implement certain controls to protect the information of the LA Cyber Lab and the information shared to the LA Cyber Lab. Every good security program implements education around access control and credentials which are the two primary means for compromising or gaining unauthorized access to an organization's information.

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise or unauthorized access of an individual systems, data, or network. This policy provides best practices for creating secure passwords. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to LACL information systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

Partner – An entity which shares information to the LACL

Member – An entity or individual which receives information from the LACL

TISP – Threat Intelligence Sharing Platform

Password Policy

1. Purpose

The purpose of this policy is to provide best practices for the creation of strong passwords and guidance in protecting LACL information.

2. Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

3. Policy

3.1. Strong Passwords: are long, the more characters you have the stronger the password, and often contain special characters. Below are the minimum requirements for LACL Password Construction:

- 3.1.1. Include a minimum of 8 characters
- 3.1.2. Include at least one symbols: (e.g. @#\$%)
- 3.1.3. Include at least one numbers: (e.g. 123456)
- 3.1.4. Include at least one lowercase character: (e.g. abcdefgh)
- 3.1.5. Include at least one uppercase characters: (e.g. ABCDEFGH)

GOOD PASSWORD PRACTICES

- Use pass-phrases or complex passwords with more than 8 characters (*complex passwords include*)
 - Randomize the use of capital and lowercase characters
 - Use special symbols such as #, &, %, \$
 - Include a number in your password
- Change passwords every 6 months and anytime you suspect a potential compromise
- Educate employees & family members
- Change the default password for devices and accounts
- Consider the use of password managers

BAD PASSWORD PRACTICES

- Don't use *password* or any other form of *passw0rd* as your password or any of the worst passwords listed above
- Don't use common information that can be easily guessed (such as first/middle/last names or birthdays)
- Don't use the same password for multiple accounts (admin and user accounts need different passwords; HR and Financial records systems need different passwords, too)
- Don't write down passwords and leave them in an easy to find places (like under your keyboard)
- Don't share passwords with untrusted sites, sources or personnel

- 3.2. Weak Passwords: are simple and may be quickly compromised by hackers and:
 - 3.2.1. Contain less than eight characters.
 - 3.2.2. Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
 - 3.2.3. Contain number patterns or easily guessed words such as: aaabbb, qwerty, zyxwvuts, 123321, password123, adminadmin. *See a complete list of passwords to avoid documented in the [LACL PSA #1 Passwords](#).*
- 3.3. Password Creation
 - 3.3.1. All user-level and system-level passwords must conform to paragraphs 3.1.-3.3.
 - 3.3.2. Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.
 - 3.3.3. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.
 - 3.3.4. Multi-factor authentication is highly recommended for any privileged access accounts.
- 3.4. Password Change
 - 3.4.1. Passwords should be changed only when there is reason to believe a password has been compromised.
 - 3.4.2. Password cracking or guessing may be performed on a periodic or random basis by the LACL technical support team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with this policy.
- 3.5. Password Protection
 - 3.5.1. Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential LACL information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
 - 3.5.2. Passwords must not be inserted into email messages, support cases or other forms of electronic communication, nor revealed over the phone to anyone.
 - 3.5.3. Passwords may be stored in “password managers” authorized by the organization.
 - 3.5.4. Do not use the "Remember Password" feature of applications (for example, web browsers) for privileged access accounts.
 - 3.5.5. Any user suspecting that his/her password may have been compromised must report the incident to a Director and change the password(s) of affected accounts.
- 3.6. Application Development
 - 3.6.1. Application developers must ensure that their programs contain the following security precautions:

- 3.6.1.1. Applications must support authentication of individual users, not groups.
 - 3.6.1.2. Applications must not store passwords in clear text or in any easily reversible form.
 - 3.6.1.3. Applications must not transmit passwords in clear text over the network.
 - 3.6.1.4. Applications must provide for some sort of role-based access control and management, such that one user cannot take over the functions of another without having to know the other's password.
- 3.7. Additional Requirements
- 3.7.1. Every work account should have a different, unique password.
 - 3.7.2. To enable users to maintain multiple passwords, the use of 'password manager' software that is authorized and provided by the LACL is encouraged.
 - 3.7.3. Whenever possible, it is recommended to enable the use of multi-factor authentication.

4. Policy Compliance

- 4.1. Compliance Measurement
 - 4.1.1. The LACL will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
- 4.2. Exceptions
 - 4.2.1. Any exception to the policy must be approved in writing by the Executive Director of the LACL in advance.
- 4.3. Non-Compliance
 - 4.3.1. Any employees, contractors, consultants, temporary and other workers, Partners or Members found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

- 5.1. [PSA #1 Passwords](#) (February 2019); *Posted on the LACL website.*

6. Revision History

Date of Change	Responsible Party	Summary of Change
Sept. 1, 2019	Rob Velasco	Original Draft
Sept. 24, 2019	Rob Velasco	Updated Content
Oct. 14, 2019	Joshua Belk	Final Formatting and Content Update



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP) Mobile Application

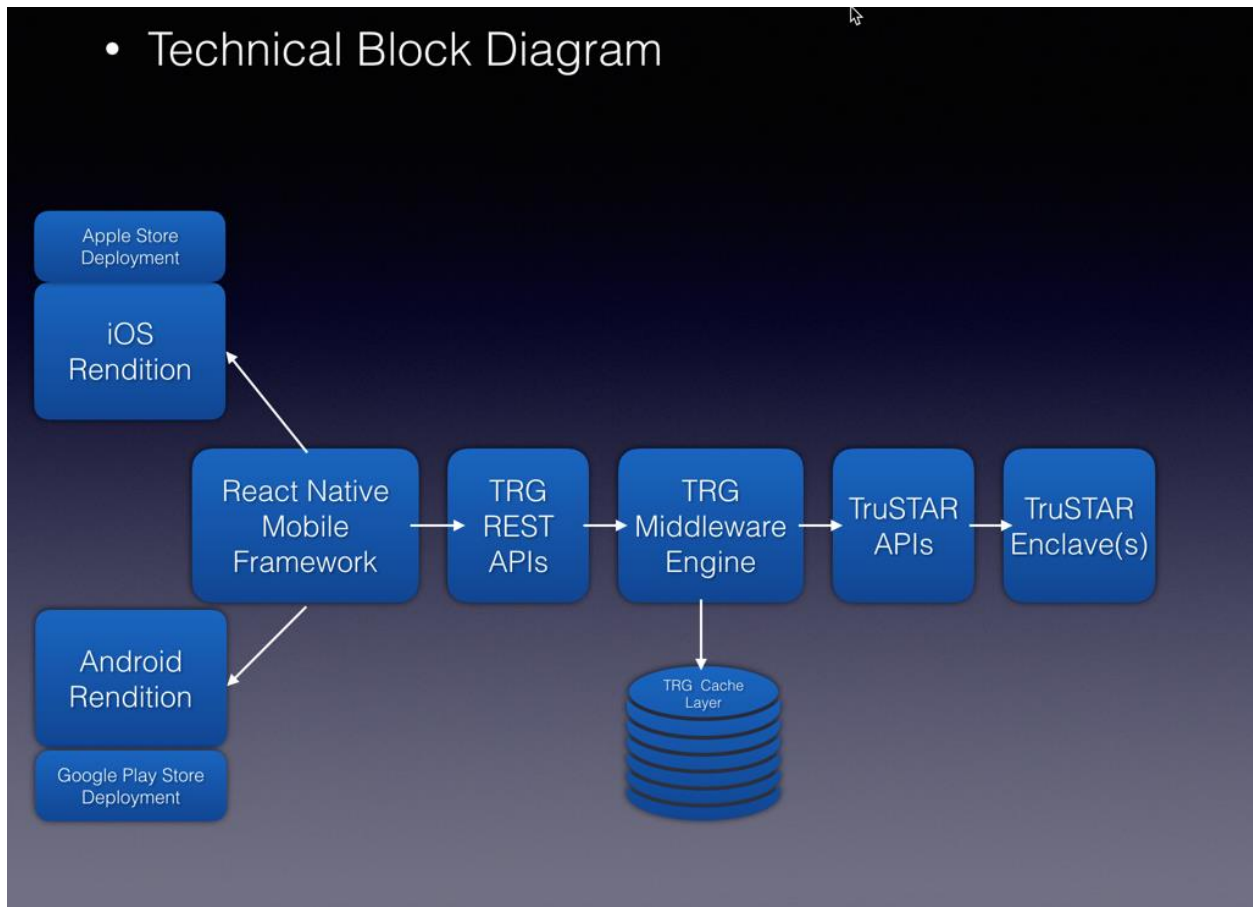
LACL Middleware Technical Documentation

September 30, 2019

Contents

Overview Technical Diagram	2
Terms	3
eMail Process.....	4
TruSTAR BEC Score Update Process	6
TruSTAR Process Diagram.....	7
Enclave Ids	8
Get BEC Reports API	8
Get BEC Reports Indicators API.....	8
Get X-Force Indicator Correlating Reports API	8
Get X-Force Report Score API.....	9

Overview Technical Diagram



The LACL mobile application is designed as a middleware application which wraps around the API of an existing threat intelligence sharing portal; in this instance the TISP is maintained and managed by TruSTAR. The mobile application created, by The Rosslyn Group (TRG), operates on Apple iOS and Android platforms. The mobile application is available for download in Google and Apple app stores.

TRG designed the middleware to be interchangeable with other APIs. The initial most viable product (VMP) was created to provide the following:

- Ingest an email from a known user with a validated account and provide a response via the mobile application regarding the malicious content of the email
- Provide trending data for users in the Los Angeles region about the threats
- Provide cybersecurity awareness through various news feeds

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

MU – Mobile Users

MW – LACL Middleware Tier

MWDB – LACL Middleware Relational Database

MVP – Most Viable Product

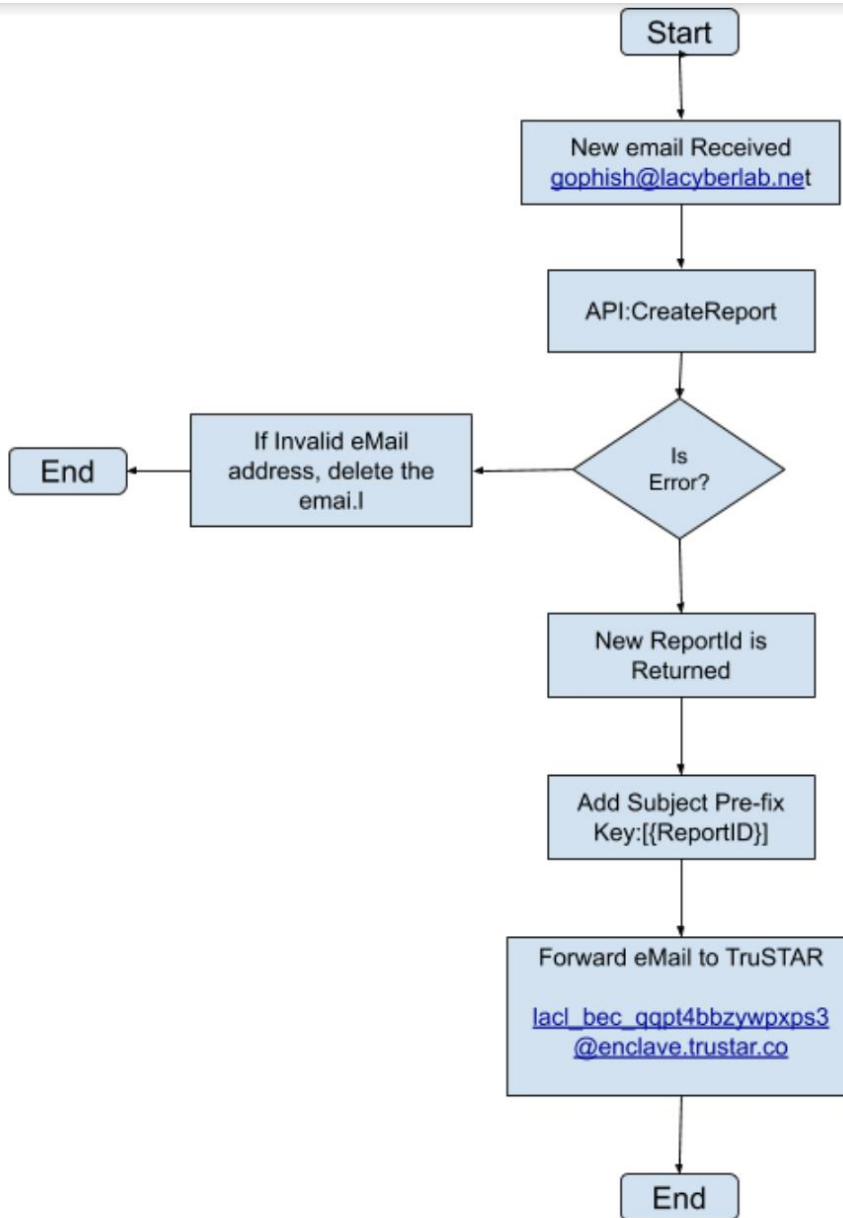
TISP – Threat Intelligence Sharing Platform

TRG – The Rosslyn Group

UUID - Universally Unique Identifier

eMail Process

The MU will forward any suspicious emails to the LACL inbox (gophish@lacyberlab.net). This event will trigger the MW to perform the following tasks.



Los Angeles Cyber Lab – TISP Mobile Application

- The mobile user will forward all suspicious emails to the LA Cyber Lab email address gophish@lacyberlab.net and gophishtest@lacyberlab.net
- The email inbox is hosted in AWS SES (Simple Email Services)
- Upon receiving an email, SES will trigger an API call to CreateReport.
- The sender's email address against MWDB registered emails.
- If the email is not registered or validated, an error is raised. The email will be deleted and ignored.
- If the email comes from a valid registered user, it will perform the following tasks:
 - It will create a new record in the MWDB using the API
 - The new record will be created with a status of 1-new.
 - The API will return the UUID for the newly created record.
 - The new UUID will be appended to the email subject line prefix:
Key:[UUID]
- The email is forwarded in its entirety to the TruSTAR inbox email address:
lacl_bec_sizpvp2vfrnynvq@enclave.trustar.co
- A push notification is sent to the mobile user confirming the email receipt.
- AWS is event trigger is responsible for handling and retrying all other errors.

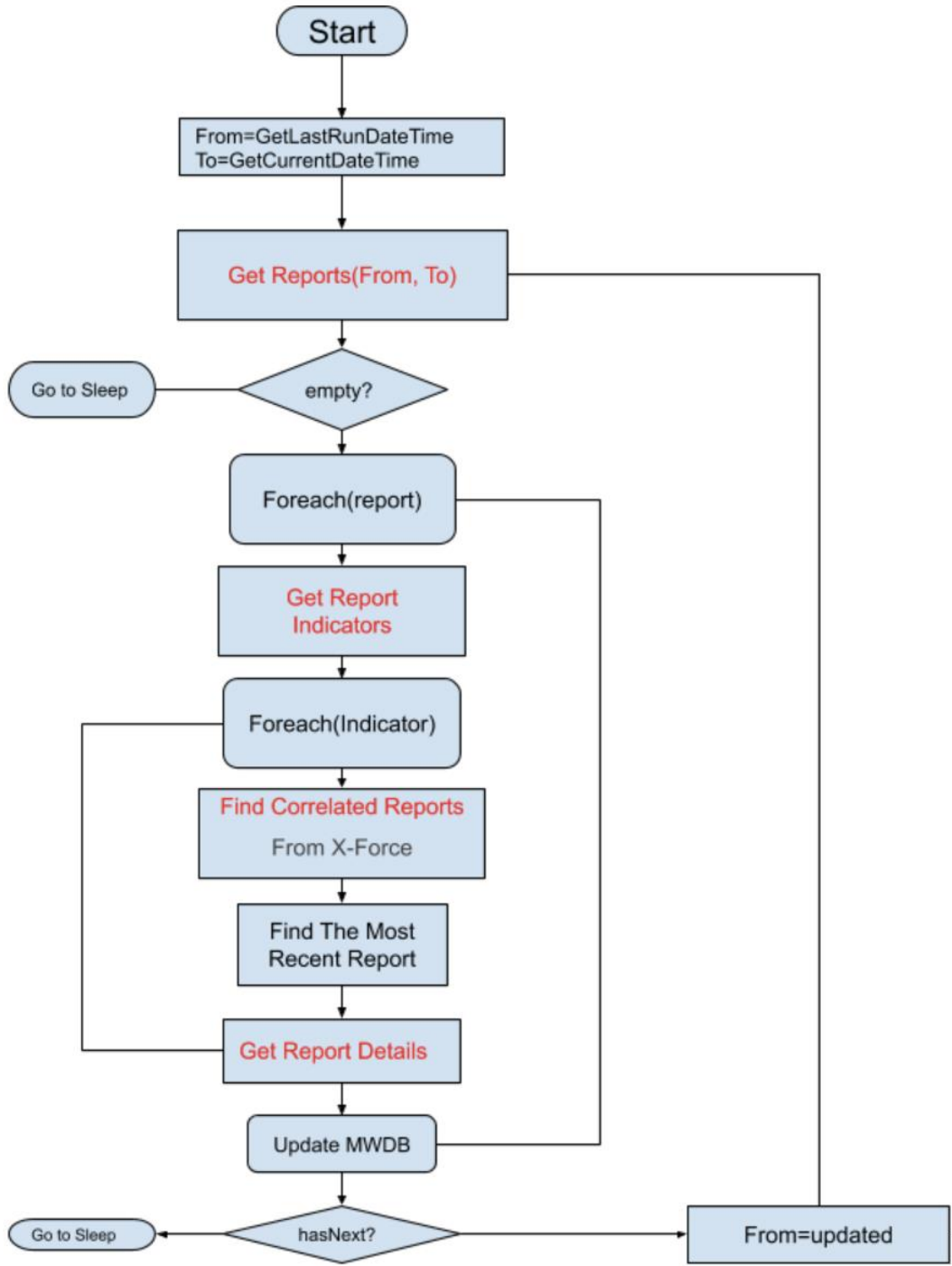
TruSTAR BEC Score Update Process

The BEC data is initially submitted to the LACL enclave through the TruSTAR email inbox. Using an asynchronous process, TruSTAR parses the emails to extract the relevant data. The parsed data is ingested into the BEC enclave to be scored. As the data is ingested into the enclave, TruSTAR starts the next phase of its internal process which is responsible for identifying the relevant indicators. Each indicator is then assessed and scored according to its risk and malicious relevance on the scale of 1-10.

The MW is responsible for reading the resulting indicators and their scores back into the MWDB. MW performs the following tasks:

- Query TruSTAR to retrieve the most recent updated data based on the updated date timestamp.
- MW will keep track of the last time it asked TruSTAR for data in a configuration table (LastQueryDateTimeStamp).
- When the data is read successfully, MW will update the (LastQueryDateTimeStamp) configuration value to the new timestamp.
- MW will wait a configurable period of time to start reading process over again.

TruSTAR Process Diagram



Enclave Ids

Enclave Name	Enclave ID	Notes
LACL BEC	08d99eac-d197-4193-86d9-b637a70df1cb	
IBM X-Force	cfa7b4ef-f30b-4773-92d7-c33a70af1e8e	

Get BEC Reports API

<https://api.trustar.co/api/1.3/reports?enclaveid=08d99eac-d197-4193-86d9-b637a70df1cb&from=1563390000000&to=1563465245297>

Parameter name	Data Type	Description
enclaveid	UUID	LACL BEC UUID
from	Epoch timestamp	Start date in milisecond
to	Epoch timestamp	End date in milisecond

More information: https://docs.trustar.co/api/v13/reports/get_reports.html

Get BEC Reports Indicators API

"<https://api.trustar.co/api/1.3/reports/{id}/indicators?idType=internal>"

Parameter name	Data Type	Description
id	UUID	Report ID
idType	string	internal or external

More information: https://docs.trustar.co/api/v13/indicators/get_indicators_for_report.html

Get X-Force Indicator Correlating Reports API

<https://api.trustar.co/api/1.3/reports/correlated?indicators=WANNACRY&enclaveids=cfa7b4ef-f30b-4773-92d7-c33a70af1e8e>

Parameter name	Data Type	Description
----------------	-----------	-------------

Los Angeles Cyber Lab – TISP Mobile Application

indicators	string	indicator value of any type; i.e. an IP address, email address, URL, MD5, SHA1, SHA256, Registry Key, Malware name, etc.
enclavelds	uuid	X-force: (cfa7b4ef-f30b-4773-92d7-c33a70af1e8e)

More information: https://docs.trustar.co/api/v13/reports/find_correlated_reports.html

Get X-Force Report Score API

<https://api.trustar.co/api/1.3/reports/{id}>

Parameter name	Data Type	Description
id	string	Report id

More information: https://docs.trustar.co/api/v13/reports/get_report_details.html



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Mobile Application Supporting Document

LA Cyber Lab Mobile Application Threat Language

January 19, 2020

LACL – Mobile Application

This document is a supplement to the existing LACL Mobile Application documentation.

The following are the specific language and guidance provided for critical and guarded threats within the LACL mobile application. The mobile application provides a response to users who have submitted an email for evaluation. When users open their inbox, one of the responses below will appear.

Security State Of Affairs - Threat Level

- **GREEN or LOW indicates a low risk.** No unusual activity exists beyond the normal concern for known hacking activities, known viruses, or other malicious activity.

Recommendations:

- Continue routine preventive measures, i.e. update antivirus, scan attachments
- Continue routine security monitoring
- Ensure personnel receive proper training on cybersecurity policies

For more detail please see <https://www.cisecurity.org/cybersecurity-threats/alert-level/>

- **BLUE or GUARDED indicates a general risk of increased hacking, virus, or other malicious activity.**

Recommendations:

- Continue routine preventative measures and security monitoring
- Identify vulnerable systems
- Implement countermeasures to protect vulnerable systems
- When available, test and implement patches, install anti-virus updates, etc., in the next regular cycle.

For more detail please see <https://www.cisecurity.org/cybersecurity-threats/alert-level/>

- **YELLOW or ELEVATED indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.**

Recommendations:

- Identify vulnerable systems
- Increase monitoring of critical systems.

LACL – Mobile Application

- Immediately implement appropriate countermeasures to protect vulnerable critical systems
- When available, test and implement patches, install anti-virus updates, etc., as soon as possible

For more detail please see <https://www.cisecurity.org/cybersecurity-threats/alert-level/>

- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets core/critical infrastructure to cause multiple service outages and system compromises

Recommendations:

- Closely monitor security mechanisms, including firewalls, web log files, anti-virus, etc., for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider the use of alternative methods of communication, such as phone, fax, or radio in lieu of email and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc., immediately.

For more detail please see <https://www.cisecurity.org/cybersecurity-threats/alert-level/>

- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems or critical infrastructure sectors.

Recommendations:

- Shut down connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternative methods of communication, such as phone, fax, or radio as necessary in lieu of email and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc., immediately.

For more detail please see <https://www.cisecurity.org/cybersecurity-threats/alert-level/>

Email Scoring - Threat Level

Guarded:

Overview - Even though we didn't find a direct malicious indicator in your message, always be mindful of potential compromises as they change on a regular basis. Follow our general tips below:

Tips:

- Verify sender address
- Exercise caution when opening email unexpected senders
- Scan attachments prior to opening
- Suspicious requests often indicate malicious intent
- Recognize poorly worded scams

Critical -

Overview - One or more indications of compromise was identified in your message. Follow our recommended actions below:

Tips:

- Delete email
- Do not open attachments
- Do not click on links
- Stop Cyber Crime – visit lacyberlab.org <href to stop cybercrime page on la cyber lab>

**Pro-Tips*

- Review email, server, and firewall logs
- Identify bad IPs, domains, and hashes
- Compare with free threat intelligence at LA Cyber Lab <href the tools for LA business>



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP)

LACL Mobile Application Security Policy

September 30, 2019

Contents

- Overview 2
- Terms 3
- Mobile Application Security Policy 4
 - 1. Purpose 4
 - 2. Scope 4
 - 3. Policy 4
 - 4. Policy Compliance 5
 - 5. Related Standards, Policies and Processes 6
 - 6. Revision History 6

Overview

The LA Cyber Lab's mobile application is the primary means for interacting with the SMB of the greater Los Angeles area. The mobile application supports the information sharing efforts of the LA Cyber Lab by allowing users to submit and receive information via the mobile application. Web and mobile application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web or mobile application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment. The LACL TISP mobile application was created and maintained by The Rosslyn Group (TRG).

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

Partner – An entity which shares information to the LACL

Member – An entity or individual which receives information from the LACL

OWASP – Open Web Application Security Project

TISP – Threat Intelligence Sharing Platform

TRG – The Rosslyn Group

Mobile Application Security Policy

1. Purpose

The purpose of this policy is to define web and mobile application security assessments within the LACL. Web and mobile application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of LACL services available both internally and externally as well as satisfy compliance with any relevant policies in place.

2. Scope

This policy covers all web and mobile application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at the LACL.

All web and mobile application security assessments will be performed by delegated security personnel either employed or contracted by the LACL. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of the LACL is strictly prohibited unless approved by the Executive Director of the LACL.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

3. Policy

3.1. Web and mobile applications are subject to security assessments based on the following criteria:

- 3.1.1. New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- 3.1.2. Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- 3.1.3. Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- 3.1.4. Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

- 3.1.5. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out.
- 3.1.6. Emergency releases will be designated as such by the Executive Director or an appropriate manager who has been delegated this authority.
- 3.2. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.
 - High – Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
 - Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
 - Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.
- 3.3. The following security assessment levels shall be established by the LACL or other designated organization that will be performing the assessments.
 - 3.3.1. Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on industry standards or OWASP testing guides. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
 - 3.3.2. Quick – A quick assessment will consist of a (typically) automated scan of an application for industry standard or OWASP Top Ten web application security risks at a minimum.
 - 3.3.3. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.
- 3.4. Industry standard tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the LACL leadership team.

4. Policy Compliance

4.1. Compliance Measurement

- 4.1.1. The LACL will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.2. Exceptions

4.2.1. Any exception to the policy must be approved in writing by the Executive Director of the LACL in advance.

4.3. Non-Compliance

4.3.1. Any employees, contractors, consultants, temporary and other workers, Partners or Members found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

5.1. LACL TISP Mobile Application Documentation

6. Revision History

Date of Change	Responsible Party	Summary of Change
Sept. 1, 2019	Rob Velasco	Original Draft
Sept. 24, 2019	Rob Velasco	Updated Content
Oct. 14, 2019	Joshua Belk	Final Formatting and Content Update



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISAO)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP)

LACL Partner Sharing Policy

September 30, 2019

Contents

Overview	3
Terms	4
Partner Sharing Policy	5
1.4	
2.4	
3.5	
4.7	
5.8	
6.9	
API Submissions	10
Request	11
Response	12
Python SDK Submissions	12

Overview

Sharing information with the LACL is a critical component of the TISP initiative. Partners must be able to define and identify information which is eligible to be shared, have the technical ability to share and be willing to share. Information sharing with the LACL IS-ISAO may include malicious indicators, indicators of compromise, known threats.

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

Partner – An entity which shares information to the LACL

Member – An entity or individual which receives information from the LACL

TISP – Threat Intelligence Sharing Platform

Partner Sharing Policy

1. Scope

The LACL IS-ISAO's value is in the threat information shared by its Partners to the Community. LACL IS-ISAO uses TruSTAR for its Cyber Threat Intelligence Sharing Platform (TISP). The TISP integrates Partner threat information in the following ways:

1. Enclave Email Inbox
2. SIEM, Orchestration or Case Management Tool
3. STIX/TAXII enabled Tools
4. TruSTAR API/SDK

2. Process Overview

The following figures show the start of the Partner threat information sharing process, TISP enrichment and how the results are viewed.

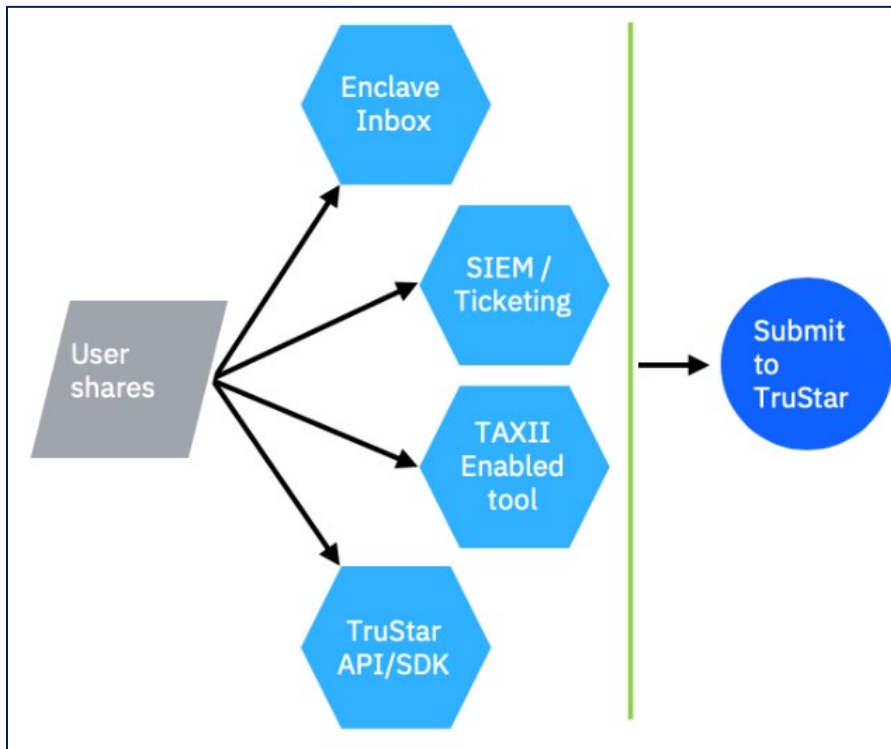


Figure 1: Integration process begins with Partners sharing threat information by email, SIEM/Ticketing Tool, TAXII enabled tool, or TruSTAR API/SDK

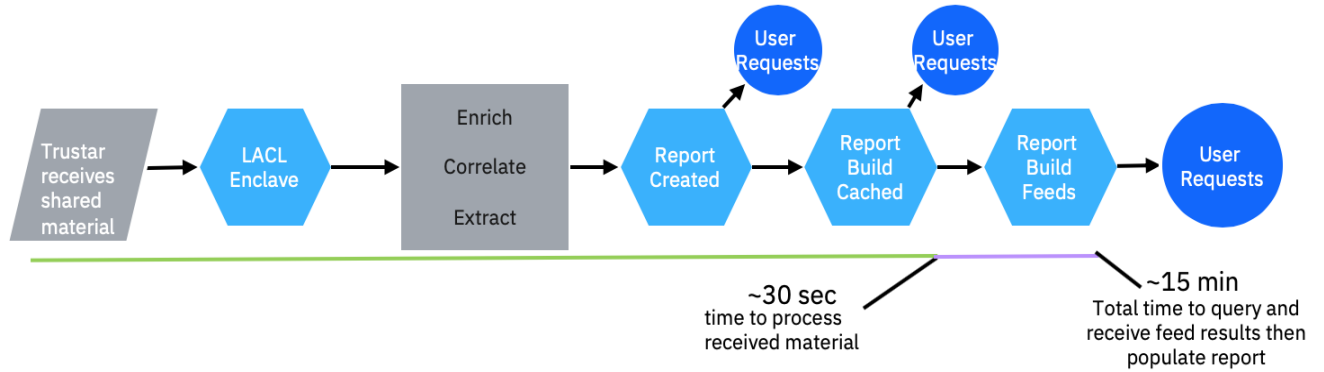


Figure 2: TruSTAR (Cyber TISP) performs extraction, enrichment, and correlation of the shared threat information. A TruSTAR Report is created to hold the processed results.

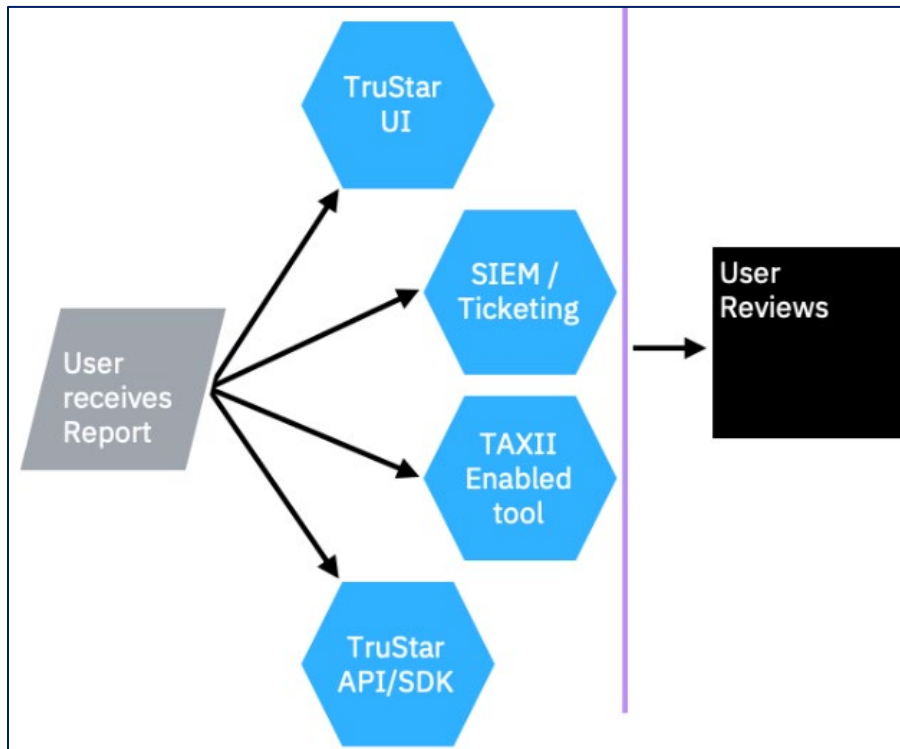


Figure 3: Partners may begin to review results when the Report is created. Partners access TruStar Reports with the TruStar User Interface (UI via Browser), SIEM/Ticketing tool, TAXII enabled tool, or the TruStar API/SDK

3. Enclave Email Inbox

Partner may submit incident and alert information directly to the Cyber TISP enclave using a variety of techniques, including email. This document provides a description of how to setup and use the enclave email submission feature.

Use Cases

Los Angeles Cyber Lab – TISP

1. A Partner belongs to an email listserv where IOCs are exchanged regularly and are receiving valuable context, but there is no easy way to extract and operationalize this intelligence.
2. You have automated alerts setup on your SIEM or case management system and want to automatically submit the details of an alert or case as a report to your enclave.

Configuration

- Destination Enclave: LACL TISP
- Send to Email Address: lacl_tisp_lro3bflhmcbcqo@enclave.trustar.co
- LACL TISP Enclave processes emails every minute.
- As with all other submissions, TruSTAR automatically extracts and correlates IOCs.
- An enclave email inbox may be configured in 1 to 2 hours

Email Submission Guidance

Partners need to send emails from the email account provided during configuration.

Partners need use the subject line prefix(s) provided during configuration.

Partners should verify the subject line prefix is in square brackets [].

If multiple subject line prefixes exist, then each one has to be in its own square [] bracket.

Submitted Emails become TruSTAR reports. TruSTAR uses the Subject line Prefix as the Report's Title.

Enclave Tags in Subject Line

Partners may include descriptive information about the email submission using tags.

1. Use the subject line. Insert tags as a comma separated list within { } brackets.
2. In the first line of the email body. Insert tags as a comma separated list within { } brackets.

Email Body

TruStar uses the email body as report content and automatically extracts IOCs found in the email body.

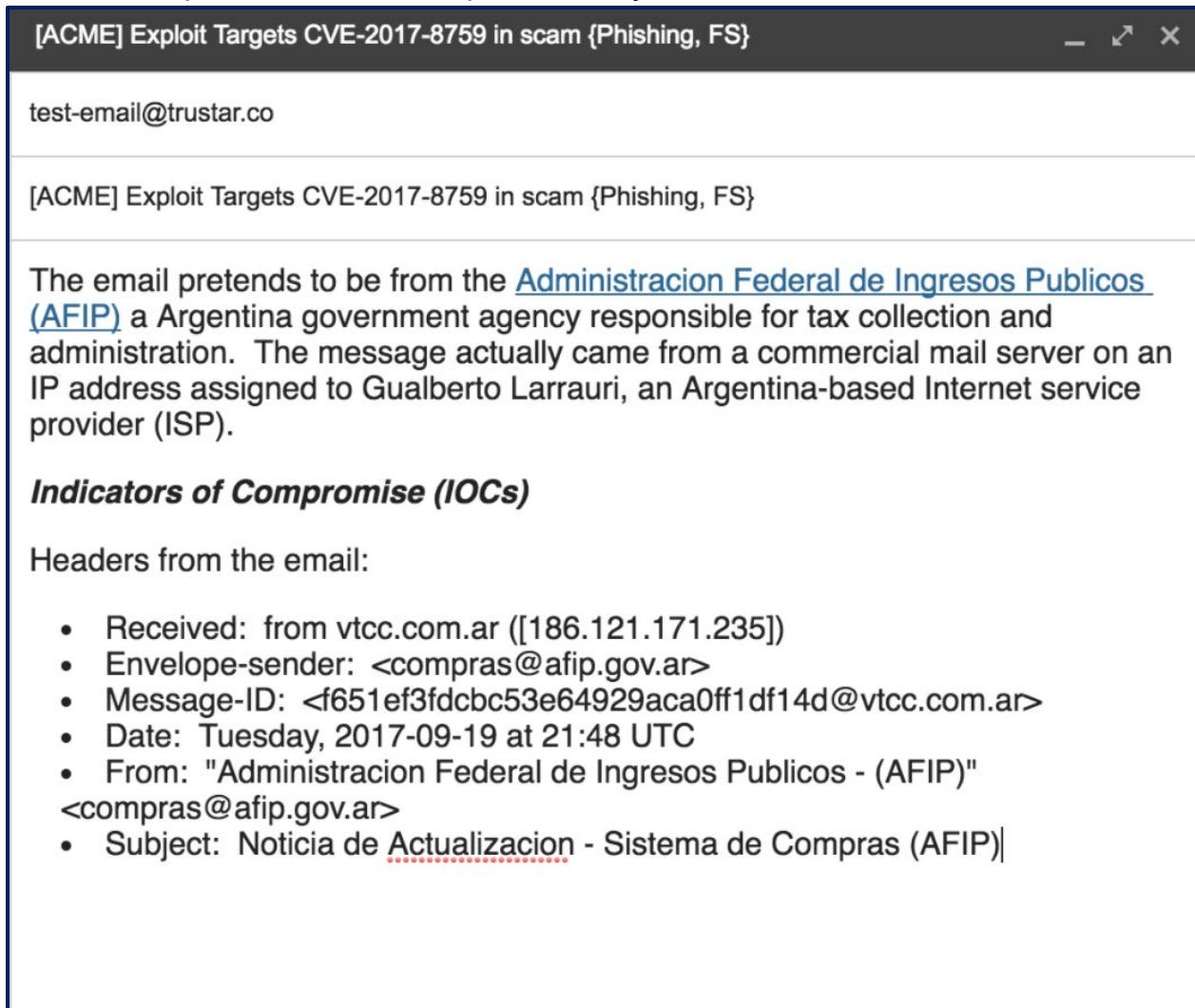
Attachments

TruSTAR automatically connects the email's attachment (PDF, Word, Text file, CSV, Excel or JSON) to the report body. If the attachments have any IOCs, then TruSTAR

automatically extracts the indicators. During the email ingestion process, the original format of the attachment may not remain.

Sample Email Submission

Here's a sample email that will be processed by TruSTAR.



The screenshot shows a window titled "[ACME] Exploit Targets CVE-2017-8759 in scam {Phishing, FS}" with a close button. The email address "test-email@trustar.co" is visible. The email body contains the following text:

[ACME] Exploit Targets CVE-2017-8759 in scam {Phishing, FS}

The email pretends to be from the [Administracion Federal de Ingresos Publicos \(AFIP\)](#) a Argentina government agency responsible for tax collection and administration. The message actually came from a commercial mail server on an IP address assigned to Gualberto Larrauri, an Argentina-based Internet service provider (ISP).

Indicators of Compromise (IOCs)

Headers from the email:

- Received: from vtcc.com.ar ([186.121.171.235])
- Envelope-sender: <compras@afip.gov.ar>
- Message-ID: <f651ef3fdcabc53e64929aca0ff1df14d@vtcc.com.ar>
- Date: Tuesday, 2017-09-19 at 21:48 UTC
- From: "Administracion Federal de Ingresos Publicos - (AFIP)" <compras@afip.gov.ar>
- Subject: Noticia de Actualizacion - Sistema de Compras (AFIP)

4. SIEM, Orchestration or Case Management Tool

Partners leverage multiple sources of threat intelligence and fuse it with historical event data to prioritize and enrich investigations. TruSTAR integrates with the list of threat intelligence sources. Connecting client's native integration to TruStar may require 2 to 4 hours of client's admin effort. Detailed support information about these sources can be found [here](#).

Los Angeles Cyber Lab – TISP

AWS GuardDuty	JIRA Cloud
Chrome Extension (New Version)	JIRA Server (Current Version)
Cisco AMP Threat Grid Feed	JIRA Server (On-prem)
Cisco AMP Threat Grid Indicator Query	Joe Sandbox
CrowdStrike Falcon Intelligence	LogRhythm
CrowdStrike Falcon Reports	MISP
CrowdStrike Falcon Stream	Okta App
Demisto	Phantom Cyber
Digital Shadows	Recorded Future
F-ISAC	RiskIQ PassiveTotal
Farsight Security	RiskIQ Blacklist Intelligence
FireEye iSight	Script Library
Flashpoint	ServiceNow [old]
IBM QRadar	ServiceNow [Current Version]
IBM Resilient	Splunk App 1.0.9 & Technology Add-On 1.0.9
Intel 471 Adversary Intelligence	TAXII Server
Intel 471 Alerts Watchlist	
Intel 471 Malware Intelligence	

5. STIX/TAXII enabled Tools

Partners may choose to use existing tools enabled with TAXII. A TAXII Server is software that offers automated exchange services by listening for connections from TAXII Clients looking to ingest data from the available services. Custom client STIX/TAXII configurations may require up to four weeks of configuration from the time credentials and STIX format provided to TruStar. Integration information for Partner Tools enabled with TAXII can be found [here](#).

Partners may use the TAXII Message Module Structure to submit threat information to TruSTAR. In the TAXII message modules (**libtaxii.messages_10** and **libtaxii.messages_11**), there is a class corresponding to each type of TAXII message.

For example, there is a **DiscoveryRequest** class for the Discovery Request message:

```
import libtaxii.messages_11 as tm11
discovery_request = tm11.DiscoveryRequest( ... )
```

For types that can be used across multiple messages (e.g., a Content Block can exist in both Poll Response and Inbox Message), the corresponding class (ContentBlock) is (and always has always been) defined at the module level.

```
content_block = tm11.ContentBlock( ... )
```


Other types that are used exclusively within a particular TAXII message type were previously defined as nested classes on the corresponding message class; however, they are now defined at the top level of the module. For example, a Service Instance is only used in a Discovery Response message, so the class representing a Service Instance, now just `ServiceInstance`, was previously `DiscoveryResponse.ServiceInstance`. The latter name still works for backward compatibility reasons, but is deprecated and may be removed in the future.

```
service_instance = tm11.ServiceInstance( ... )  
service_instance = tm11.DiscoveryRequest.ServiceInstance( ... )
```

See the [API Documentation](#) for proper constructor arguments for each type above.

6. TruSTAR API / SDK

The TruSTAR REST API allows you to easily synchronize the incident report information available in the TruSTAR platform to the monitoring tools and analysis workflows you use in your infrastructure.

API Submissions

API access is over HTTPS, and all data is transmitted securely in JSON format. More information [about our API](#).

Submit Report

1. Submit a new incident report, and receive the ID it has been assigned in TruSTAR's system.
2. The ID can be used to find the report through Station, or issue subsequent calls on the API.
3. Note that that a report cannot be tagged during submission. Tags can only be applied afterwards, through a separate call.
4. If a report contains more than 500 indicators, it will be rejected with a `413`(payload too large) error code. See [here](#) for details.

Parameters

The request JSON body should be a `Report` object. Specifically, the body must be well formed JSON with the following fields:

Parameter	Required	Default	Description
title	X		Title of the report

reportBody	X		Text content of report
externalTrackingId		null	External tracking ID provided by user. Must be unique across all reports for a given company.
externalUrl		null	URL for the external report that this originated from, if one exists. Limit 500 alphanumeric characters.
timeBegan		current time	ISO-8601 formatted incident time with timezone, e.g. 2016-09-22T11:38:35+00:00
distributionType	X		COMMUNITY (will disregard any enclavelds) or ENCLAVE (must include enclavelds)
enclavelds	Must be included if the distribution type is ENCLAVE		Non-empty array of TruSTAR-generated enclave ids (available on Station under settings or through the GET /enclaves endpoint). Use the enclave ID, NOT the enclave name.

Response (200)

The ID (a GUID) that the report has been assigned in TruSTAR’s system.

Example Usage

Request

```
curl -k -H "Content-Type: application/json" -X POST -d \
  '{"title":"curl api-report", "reportBody":"This is a test report body with some indicators: 1.2.3.4, evil.exe, api.evildomain.com, hash d2dd1bcdd6d6cfac59ba9638d2cd886c ", "externalTrackingId": "M-1234", "timeBegan":"2016-09-22T11:38:35+00:00", "distributionType": "ENCLAVE", "enclavelds":["e27b914b-b1ee-4d25-b4b2-d50db5208b4d", "ac6a0d17-7350-4410-bc57-9699521db992"]}' \
  -H "Authorization: Bearer {access_token}" "https://api.trustar.co/api/1.3/reports"
```

Response

```
81f89c56-265a-11e8-b467-0ed5f89f718b
```

Python SDK Submissions

Partners should use the TruSTAR [Python SDK](#) to develop specific integrations for workflow automation. The TruSTAR Python SDK is a Python package that can be used to easily interact with the TruSTAR Rest API from within any Python program. It is compatible with both Python 2 and Python 3, however some of the example scripts that use the package specifically target Python 2 only. More information and code samples [for our SDK](#).

Submit Report

- If **report.is_enclave** is **True**, then the report will be submitted to the enclaves identified by **report.enclaves**; if that field is **None**, then the enclave IDs registered with this [TruStar](#) object will be used.
- If **report.time_began** is **None**, then the current time will be used.

Parameters: report – The [Report](#) object that was submitted, with the **id** field updated based on values from the response.

Example:

```
>>> report = Report(title="Suspicious Activity",
>>>                 body="We have been receiving suspicious requests from 169.178.68.63.",
>>>                 enclave_ids=["602d4795-31cd-44f9-a85d-f33cb869145a"])
>>> report = ts.submit_report(report)
>>> print((report.id))
ac6a0d17-7350-4410-bc57-9699521db992
>>> print((report.title))
Suspicious Activity
```



Los Angeles Cyber Lab, Inc.

An Internet Security – Information
Sharing & Analysis Organization (IS-ISA0)

Supported by the U.S. Department of Homeland Security

Threat Intelligence Sharing Platform (TISP)

LACL X-Force Exchange Risk Score Documentation

July 3, 2019

Contents

Overview	2
Terms	3
X-Force Exchange Risk Score	4
1. Scope	4
2. XFE Threat Intelligence Sources	4
3. Risk Score Calculation	4
4. IBM Sourced Content Contributing To The Risk Score	5
5. Understanding The Risk Score	5

Overview

The LACL TISP utilizes IBM's X-Force Exchange (XFE) for analysis of data within the TISP (TruSTAR). XFE supplies a risk score, location, categorization information, historical content, WhoIs and passive DNS information for IPs. The risk score ranges from **1 to 10**, with 1 showing no risk and 10 as the highest risk score. XFE normalizes the risk score value as IBM receives threat information from several sources. XFE processes threat intelligence information, including internet scans and spam collection from across the globe and the risk score reflects the potential maliciousness.

For example, an IP source sending a high volume of spam has a higher risk score. Over time, the risk score may decrease if the IP becomes less active in its spam output, either by volume or by frequency. The following has more information about the risk score: <https://exchange.xforce.ibmcloud.com/faq>.

Terms

LACL – Los Angeles Cyber Lab, LA Cyber Lab

TISP – Threat Intelligence Sharing Platform

XFE – IBM X-Force Exchange

X-Force Exchange Risk Score

1. Scope

XFE threat intelligence analysis and risk scoring methodology for the LACL TISP and mobile application are outlined within this document.

2. XFE Threat Intelligence Sources

The following are the data sources utilized for the LACL TISP:

- Botnet Traps
- Web Crawling
- Email/Phishing Honeypots
- Open Relay Proxies
- X-Force Vulnerability Database
- Whois
- ASN
- Cert Stream
- Regional Internet Registries
- Tor Nodes
- DNS Analytics from PCH/Quad9
- IBM Customer Feedback about URLs, IPs, DGA matches, Squatting matches

Concerning the distribution proprietary threat intel versus external 3rd party feeds we have:

- 89% is XFE proprietary threat intel
- 11% is coming from external feeds

3. Risk Score Calculation

XFE's analytics engine manages the life-span of an indicator of compromise (IOC) dynamically per source and per category.

Risk Scoring Factors:

- How often have we seen an IOC (e.g. Phishing website observed in initial compromise)
- In how many sources have we seen an IOC (e.g. does a Malware Downloader occur in parallel on our Email Honeypots and on our OpenRelays)
- Is the IOC reoccurring from time to time
- When did we see the IOC the last time
- Is the IOC after a rescanning/recrawling clean now? (e.g. after the owner has fixed the vulnerability / removed an exploit)

XFE normalizes the risk scoring factors. XFE recommends taking steps to defend, block or filter when a risk score is ≥ 5.0 .

XFE uses dynamic risk scoring per IOC Category. For example, the lifespan of a phishing URL differs from a Botnet C2 Server.

XFE maintains an IP Reputation database. For example, a spearphishing email's originating source IP is recorded in the IP Reputation database with a risk score ≥ 5 . If XFE no longer sees spearphishing from this IP, the risk score lessens stepwise. Within a few days it will be below 5 (5 is the recommended threshold for which an action should be taken like a QRadar Offense being created).

For example, in other categories, an IP in our botnet traps or 3rd party list receives a risk score ≥ 5 . XFE lowers the risk score and within in few days it will be below 5 if the IP is not observed.

XFE uses customer feedback to permanently adjust and improve our algorithms to ensure coverage and a low false positive rate.

4. IBM Sourced Content Contributing To The Risk Score

Data processed per day

- 13M crawled and analyzed web pages and images
- 17M spams received via our spam honeypots

Data processed ever

- 40B analyzed web pages and images
- 3B known web hosts
- 9B unique email bodies
- 4.6M malware samples
- 18k identified Bad Actors
- 800 TB of Threat Intelligence Data in the X-Force Content Intelligence Data Center
- Updates for our consumers (such as XFE, QRadar, XGS, Lotus Protector for Mail Security, update frequency: 3-5 minutes)
- 230k new or updated URL categorizations per day
- 460k new or updated IP categorizations per day
- 1.2M new or updates spam hashes per day

5. Understanding The Risk Score

XFE aligned the risk score range with the Common Vulnerability Scoring System (CVSS), see <https://www.first.org/cvss/specification-document#5-Qualitative-Severity-Rating-Scale>.

XFE uses colors to express the rating:

Score	Rating	Color
1 - 3	Low	Green
4 - 6	Medium	Yellow
7 - 10	High*	Red

*Unlike CVSS, XFE does not distinguish between High and Critical

6. Revision History

Date of Change	Responsible Party	Summary of Change
July 3, 2019	IBM	Original Draft
Oct. 14, 2019	LACL	Final Formatting and Content Update

Feed overlap analysis matrix

	F1	F2	F5	F6	F7	F9
Feed #1 CIRCL OSINT Feed	-	1%	0%	0%	0%	0%
Feed #2 The Botvrij.eu Data	41%	-	0%	0%	1%	0%
Feed #5 blockrules of rules.emergin	0%	0%	-	0%	0%	0%
Feed #6 malwaredomainlist	2%	0%	0%	-	0%	0%
Feed #7 Tor exit nodes	1%	0%	0%	0%	-	0%
Feed #9 cybercrime-tracker.net - all	0%	0%	0%	0%	0%	-
Feed #11 listdynamic dns providers	0%	0%	0%	0%	0%	0%
Feed #15 diamondfox_panels	37%	0%	0%	0%	0%	0%
Feed #17 pop3gropers	0%	0%	0%	0%	0%	0%
Feed #18 Ransomware Tracker CSV	12%	0%	0%	0%	0%	0%
Feed #19 Feodo IP Blocklist	0%	0%	0%	0%	0%	0%
Feed #22 OpenPhish url list	0%	0%	0%	0%	0%	0%
Feed #23 firehol_level1	2%	0%	0%	0%	0%	0%
Feed #24 IPs from High-Confidence	3%	0%	0%	0%	0%	0%
Feed #25 Domains from High-Confic	2%	0%	0%	0%	0%	0%
Feed #26 ci-badguys.txt	0%	0%	1%	0%	0%	0%
Feed #27 alienvault reputation gene	0%	0%	1%	0%	0%	0%
Feed #28 blocklist.de/lists/all.txt	0%	0%	1%	0%	0%	0%
Feed #29 VNC RFB	0%	0%	0%	0%	0%	0%
Feed #30 sshpwauth.txt	0%	0%	3%	0%	0%	0%
Feed #31 sipregistration	0%	0%	0%	0%	0%	0%
Feed #32 sipquery	0%	0%	0%	0%	0%	0%
Feed #33 sipinvitation	0%	0%	0%	0%	0%	0%
Feed #34 All current domains belong	0%	0%	0%	0%	0%	0%
Feed #35 VXvault - URL List	0%	0%	0%	0%	0%	0%
Feed #38 http://cybercrime-tracker	0%	0%	0%	0%	0%	0%
Feed #39 http://cybercrime-tracker	0%	0%	0%	0%	0%	0%
Feed #41 blocklist.greensnow.co	0%	0%	0%	0%	1%	0%
Feed #42 conficker all domains gene	0%	0%	0%	0%	0%	0%
Feed #43 This list contains all domai	0%	0%	0%	0%	0%	0%
Feed #44 This list contains all optior	0%	0%	0%	0%	0%	0%
Feed #45 This list contains all brows	0%	0%	0%	0%	0%	0%
Feed #47 URLHaus Malware URLs	0%	0%	0%	0%	0%	0%
Feed #48 CyberCure - IP Feed	0%	0%	0%	0%	1%	0%
Feed #49 CyberCure - Blocked URL F	0%	0%	0%	0%	0%	0%
Feed #50 CyberCure - Hash Feed	0%	0%	0%	0%	0%	0%
Feed #51 ipsbamlist	0%	0%	0%	0%	0%	0%
Feed #52 mirai.security.gives	0%	0%	1%	0%	0%	0%
Feed #53 malsilo.url	0%	0%	0%	0%	0%	0%
Feed #54 malsilo.ipv4	0%	0%	0%	0%	0%	0%

Issues	Date Discovered	Verified By	Notes	Date Resolved
Account Creation:				
Create Account screen should check if the email is already registered and warn the user.	8/23/19	8/27/19	isEmailValid API	8/23/19
Unless the email is available, user shouldn't be able to move to the next screen.	8/23/19	8/27/19		8/23/19
The email field does not check for the email format. I was able to enter 123 in the email field and it accepted it as a valid email format.	8/23/19	8/27/19		8/23/19
I was able to move to the next screen with no email address.	8/23/19	8/27/19	Dim button unless email is validated, check via request when confirmEmail is typed	8/23/19
Password validation does not check for all categories of characters listed on the screen. I was able to continue with a password with no Upper case and no special characters.	8/23/19	8/27/19		8/23/19
The password screen is supposed to put check marks as each category of characters are satisfied.	8/23/19	8/27/19		8/23/19
I was able to move to the next screen without typing any passwords.	8/23/19	8/27/19		8/23/19
The personal or business selection screen is mission.	8/23/19	8/27/19		8/23/19
The industries screen should only be displayed if the user selects the business option.	8/23/19	8/27/19		8/23/19
I was able to go to the next screen without selecting anything in the industries screen. Users must	8/23/19	8/27/19		8/23/19
I was able to enter a zip code larger than 5 characters.	8/23/19	8/27/19	Note: Handling string length, but unable to find proper zip validator, more research	8/23/19
After trying to create the account with an email t	8/23/19	8/27/19	"Please try again" error	8/23/19
Verification link is not functional.	8/23/19	8/28/19	notification	8/27/19
After creating a new account, the app should not allow the user to see the rest of the application until the account has been verified. It should go to the screen which will indicate the following: 1. Your account hasn't been verified. Please click the verify link in the email sent to "email address". 2. It should also have a resend verify email button in case the user didn't get the email.	8/26/19	9/1		8/30/19
The verification email doesn't seem to be working? I clicked the link from the desktop and because the token was expired, I received this message (see notes). From the mobile app when I clicked the link, I received the same error and it didn't navigate to the mobile app so I can re-send the email with a new token.	8/27/19	8/28/19	{"success":false,"message":"Token is expired or not found.", "error":"Token is expired or not found.", "stack":"Error: Token is expired or not found.\n at PromisePreparedStatementInfo.execute (/app/node_modules/mysql2/promise.js:53:22)\n at /app/api/controllers/auth.js:305:43\n at process_tickCallback (internal/process/next_tick.js:68:7)", "errno":100}	8/27/19
Login:				
The error message for logging in with an invalid email address or password is not clear. "Invalid information. Please try again"	8/23/19	8/28/19	It should display the error message coming from the stored procedure.	8/27/19
The login screen doesn't check for a valid email format.	8/23/19	8/27/19	regex	8/23/19
The button Done should be replaced with login.	8/23/19	8/27/19		8/23/19
If a user logs into an account that hasn't been verified, it should go to the "Please Verify Account" screen.	8/26/19	9/1		8/30/19
Password Reset functionality is missing.	8/27/19	8/28/19		8/27/19
Password change is missing.	8/27/19	8/28/19		8/27/19
Password Change and Password Reset screens should include the password policy check boxes	8/29/19			8/30/19
Threat Trend:				
Number of days filter is missing.	8/23/19	8/27/19	Sectors separated into three graphs	8/26/19
Global: What is the yellow graph line?	8/23/19	8/27/19	Guarded report data	8/26/19
Industries:This screen does not display the graphs for the three industries. It only shows one graph.	8/23/19	8/27/19		8/26/19
The heat map doesn't appear to be working. It only plots two location. There should be more locations. The dots also need to be displayed in two colors indicating the guarded and critical threats.	8/27/19	9/1		8/28/19
On the home page, the "State of affairs in Greater LA" should be changed to "Security State of Affairs"	8/27/19	8/28/19		8/27/19
"Tip Of The Day" lable missing from the home page. The content text seem to be running into each other.	8/27/19	8/28/19		8/28/19
How It Works:				
The text on the top of the screen is cut off	8/23/19	8/27/19		8/25/19
The email address font is too big. It needs to fit on one line.	8/23/19	8/27/19		8/25/19
The red background of the "copy to clipboard" is shorter than the text.	8/23/19	9/1	Note: Tested on multiple phones, unable to duplicate	

Issues	Date Discovered	Verified By	Notes	Date Resolved	
My Account:					
Industry edit screen is not functional	8/23/19		8/27/19	Option to change Personal to Business - same request?	8/24/19
After clicking the save button the message "Profile updated!. Changes are reflected immediately" is not necessary.	8/23/19		8/27/19	Spinner on page instead	8/23/19
The profile update allowed me to change my profile password with no validation email.	8/23/19		8/27/19		8/30/19
email edit does not validate for email format	8/23/19		8/27/19		8/25/19
It allowed me to update the profile with "test" email.	8/23/19		8/27/19		8/25/19
We probably should not allow for profile email address change.	8/23/19		8/27/19	Hide "Edit Email" for now	8/23/19
Additional Email:					
Email format validation is missing	8/23/19		8/27/19		8/25/19
Verification link is not functional	8/23/19		9/1	Need to create a larger Resend Link button.	8/24/19
Verified and un-verified icons are missing next to the email.	8/23/19		8/27/19	Left of email	8/24/19
Allows multiples adds with empty emails	8/23/19		9/1	Clear empty fields with delete button as well	8/28/19
Unable to delete additional emails.	8/27/19		9/1		8/26/19
				Consider caching RSS alertLevel	
DATABASE Issues:					
CreateReport:					
when entering null, - getting an error becReportId cannot be null	8/26/19		8/27/19		8/26/19
changes made to Authenticate - added verified					08/30/19
General					
Test for error conditions: 1 - MySQL is down. 2 - API links are down	8/29/19				

Test Group	Test Tasks #	Task Instructions	Expected Results	Test Date
Name and Email Collection	1	Tap the Create Account button	email collection screen	8/29
	2	Enter First Name and Last Name	last name	8/29
	3	Enter a valid email format address	App Should Allow it	8/29
	4	Verify the email account re-enter the same address	field. The next button should become	8/29
	5	Verify the email address by re-entering a mismatched address	the verify email matches the first email	8/29
	6	Leave the names blank	The next button should remain disabled.	8/29
	7	Leave email address blank	The next button should remain disabled.	8/29
	8	Enter a non-standard email	The next button should remain disabled.	8/29
	9	Enter an email address that is already registered.	email is already registered.	8/29
	10	Tap the next button	App should advance to the next page	8/29
Password Collection	1	Enter a password with no letters	The next button should remain disabled.	8/29
	2	Enter a password with no caps	The next button should remain disabled.	8/29
	3	Enter a password with no numbers	The next button should remain disabled.	8/29
	4	Enter a password with no special characters	The next button should remain disabled.	8/29
	5	Enter a password with all the requirements included	required section should display checked.	8/29
	6	Confirm the password with a mis-matched password	The next button should remain disabled.	8/29
	7	Confirm the password with a matched password	The next button should remain disabled.	8/29
	8	Check the terms and agreements check box	The next button should become enabled.	8/29
	9	Tap the Submit button	App should advance to the	8/29
Account Type	1	Select the Personal account type	The next button should enable	8/29
	2	Tap the Next button	App should advance to the zip code screen.	8/29
	3	Select the Business account type	The next button should enable	8/29
	4	Tap the Next button	selection screen.	8/29
	5	Select one or more industry	the next button should enable	8/29
	6	Select more than three industry.	of 3 industries can be selected.	8/29
	7	De-select the industry options	the next button should disable	8/29
	8	Tap the Next button	App should advance to the zip code screen.	8/29
Zip Code	1	Tab the Done button with no zip code entered	is invalid.	8/29
	2	Enter a zip code less than 5 digits and tap the Done button.	is invalid.	8/29
	3	Tap the "Use your current location" link	current location zip code.	8/29
	4	Tap the Done button	screen.	8/29

Verification Screen				
Verification Screen	1	Before verifying the email link, tap the "Already Verified" button	not verified.	8/29
	2	Tap the "Resend Email" button	registered email address with the	8/29
	3	Tap the "Sign Out" link	App should go to the initial login screen.	8/29
	4	email and password.	screen.	8/29
	5	Verify the email link.		8/29
	6	After verifying the email link, tap the "Already Verified" button	and features.	8/29



Threat Intelligence Data Ecosystem Intelligence Sources

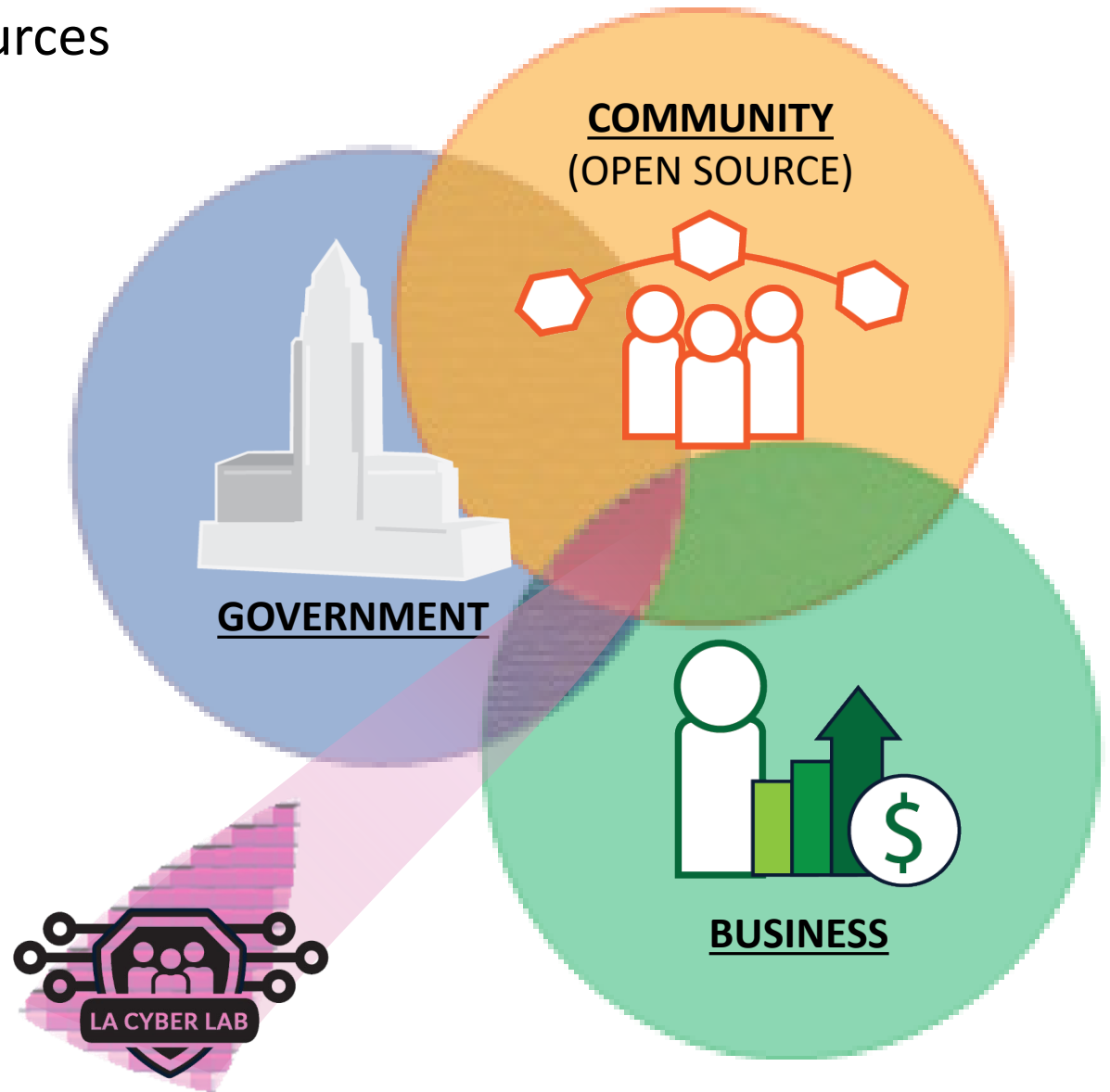
Three Categories Of Data

- Government (Public Sector)
Federal, State, Local Data (SLTT)
- Community (OSINT)
40 Unique data feeds
- Business (Private Sector)
12-15 Companies

Most organizations utilize various levels of these data feeds and ingests them for varied implementations

How the LACL Threat Data Delivers Value?

Correlation of OSINT, government and local business threats combined into one source benefits your existing cybersecurity defense strategy.





Threat Intelligence Data Ecosystem Business Sources

Private Sector Companies

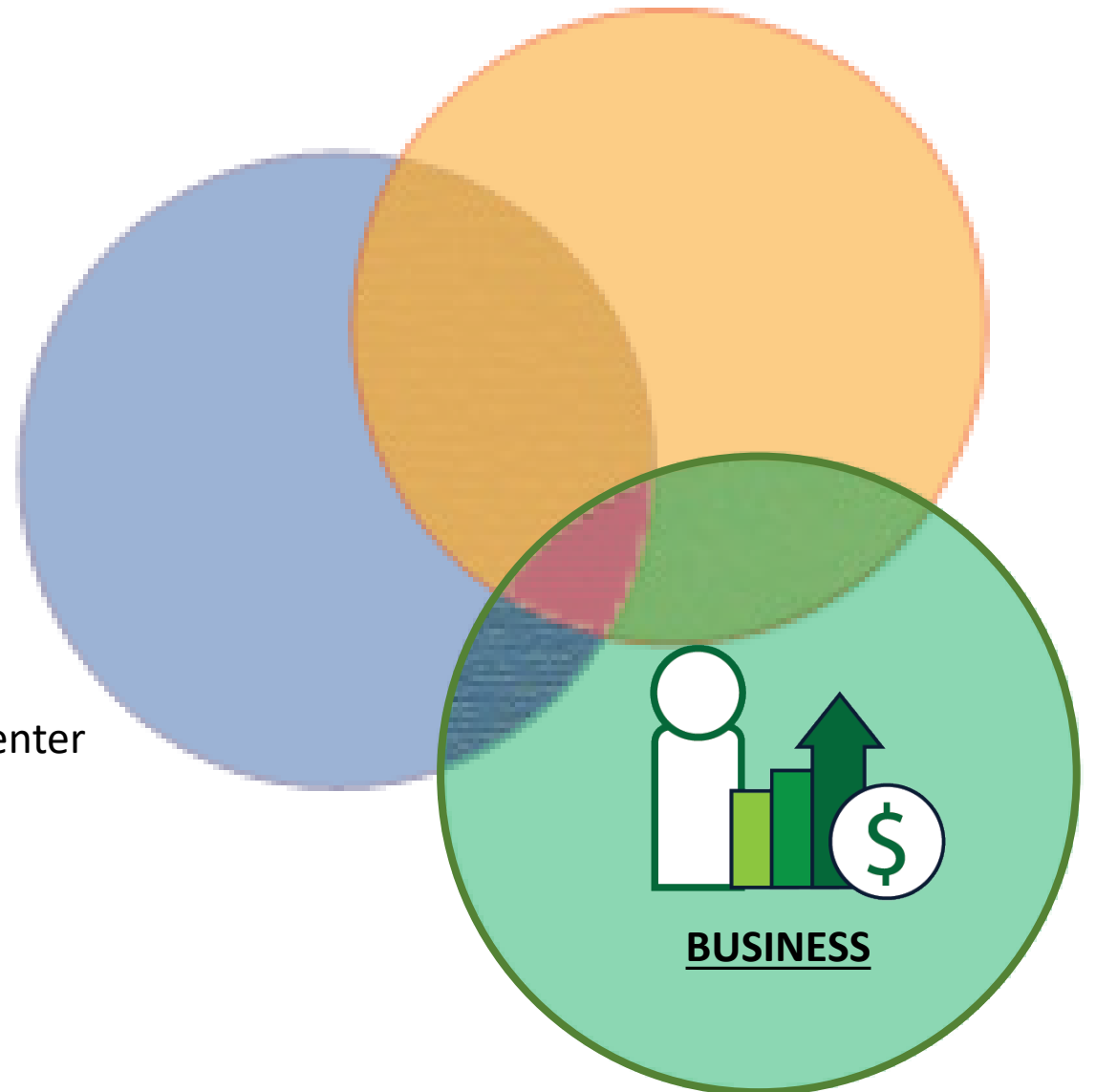
- 12-15 Partner Organizations providing threat data
 - IOCs
 - TTPs

Sectors Sharing To The LACL*

- Beauty
- Energy
- Entertainment
- Financial
- Healthcare
- Legal
- Media

BUSINESSES

City National Bank
Dollar Shave Club
Cedars-Sinai Medical Center
Hulu
Riot Games
SoCal Edison
Sheppard Mullin
21st Century Fox





Threat Intelligence Data Ecosystem Community Sources

Open Source Intelligence (OSINT) Data

- Darkweb
- Publicly Available Free Feeds

OSINT Data Sources

Feed #1 CIRCL OSINT Feed

Feed #2 The Botvrij.eu Data

Feed #5 blockrules of rules.emergingthreats.net

Feed #6 malwaredomainlist

Feed #7 Tor exit nodes

Feed #9 cybercrime-tracker.net - all

Feed #11 listdynamic dns providers

Feed #15 diamondfox_panels

Feed #17 pop3gropers

Feed #18 Ransomware Tracker CSV Feed

Feed #19 Feodo IP Blocklist

Feed #22 OpenPhish url list

Feed #23 firehol_level1

Feed #24 IPs from High-Confidence DGA-Based C&Cs Actively Resolving

Feed #25 Domains from High-Confidence DGA-based C&C Domains Actively Resolving

Feed #26 ci-badguys.txt

Feed #27 alienvault reputation generic

Feed #28 blocklist.de/lists/all.txt

Feed #29 VNC RFB

Feed #30 sshpwauth.txt

Feed #31 sipregistration

Feed #32 sipquery

Feed #33 sipinvitation

Feed #34 All current domains belonging to known malicious DGAs

Feed #35 VXvault - URL List

Feed #38 <http://cybercrime-tracker.net>

Feed #39 <http://cybercrime-tracker.net>

Feed #41 blocklist.greensnow.co

Feed #42 conficker all domains generated

Feed #43 This list contains all domains - A list for administrators to prevent mining in networks

Feed #44 This list contains all optional domains - An additional list for administrators

Feed #45 This list contains all browser mining domains - A list to prevent browser mining only

Feed #47 URLHaus Malware URLs

Feed #48 CyberCure - IP Feed

Feed #49 CyberCure - Blocked URL Feed

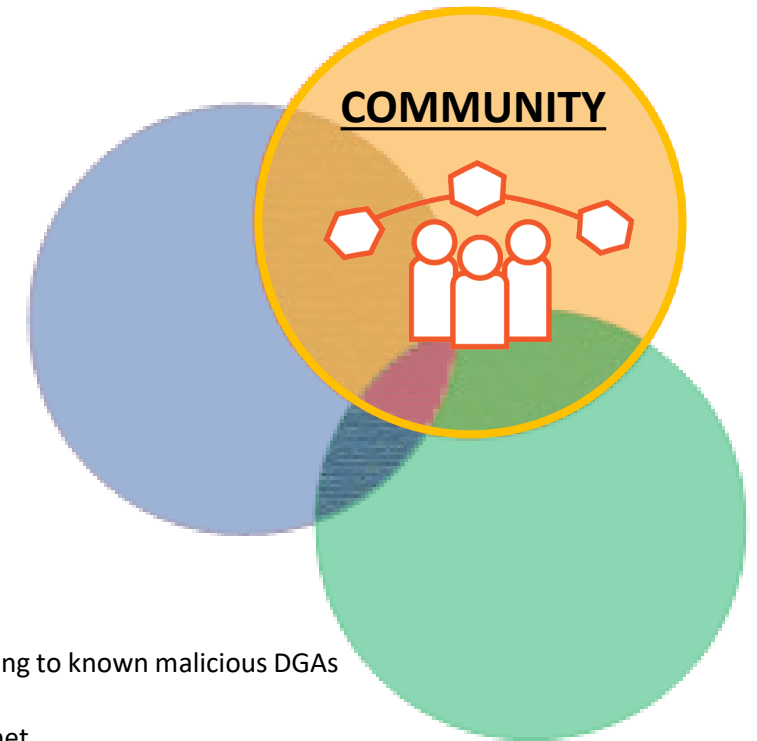
Feed #50 CyberCure - Hash Feed

Feed #51 ipspamlist

Feed #52 mirai.security.gives

Feed #53 malsilo.url

Feed #54 malsilo.ipv4





Threat Intelligence Data Ecosystem

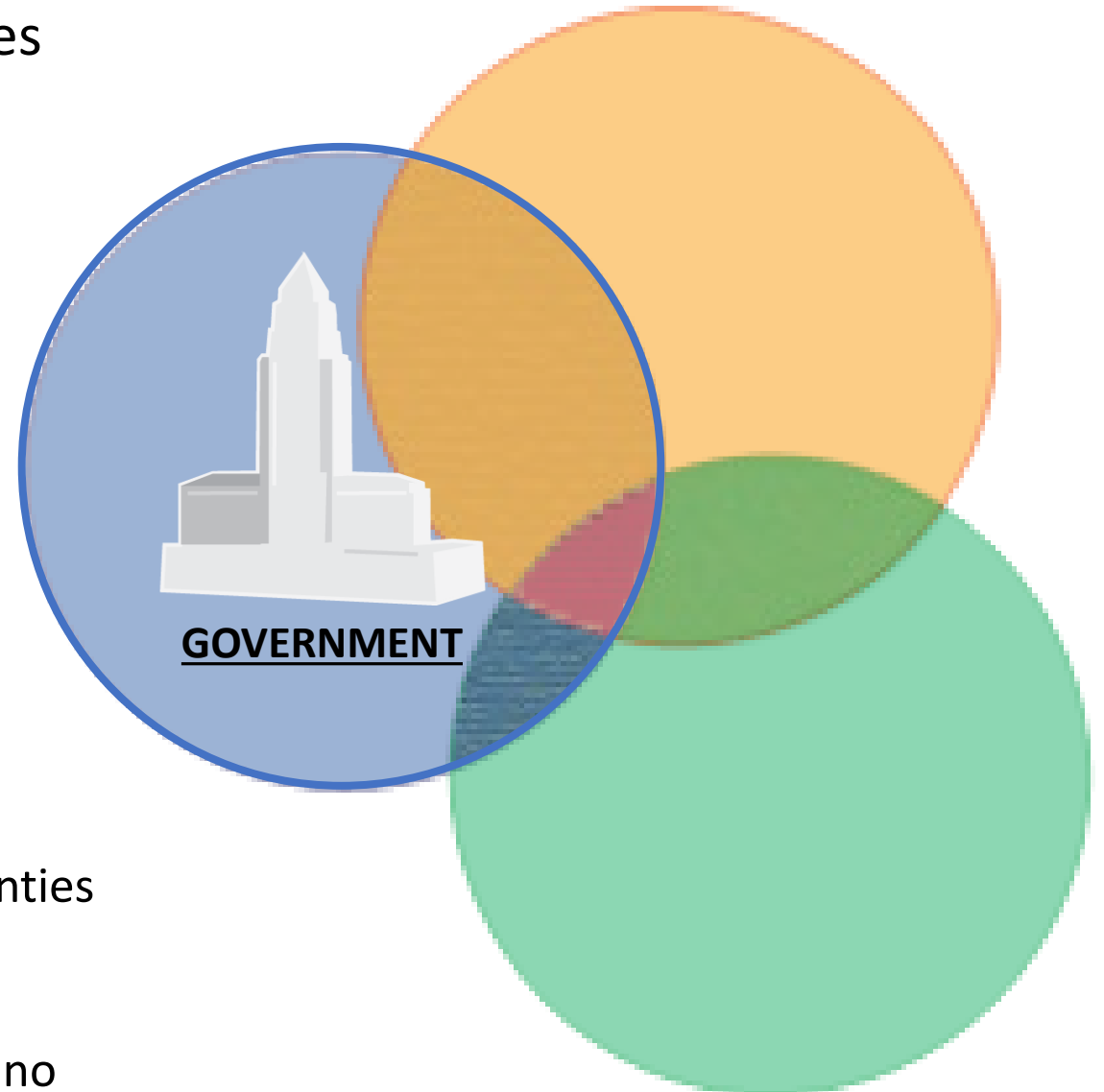
Government Sources

Public Sector Partners

- Federal
 - DHS – AIS Feed
- State
 - Cal OES*
- Local
 - City of Los Angeles
 - Port of Los Angeles

SLTT Future Expansion*

- Los Angeles County
 - LA County CISO
 - 88 Cities
 - 14 Los Angeles Tribes
- Surrounding Counties
 - Orange
 - Ventura
 - San Bernardino





Los Angeles Cyber Lab Ecosystem

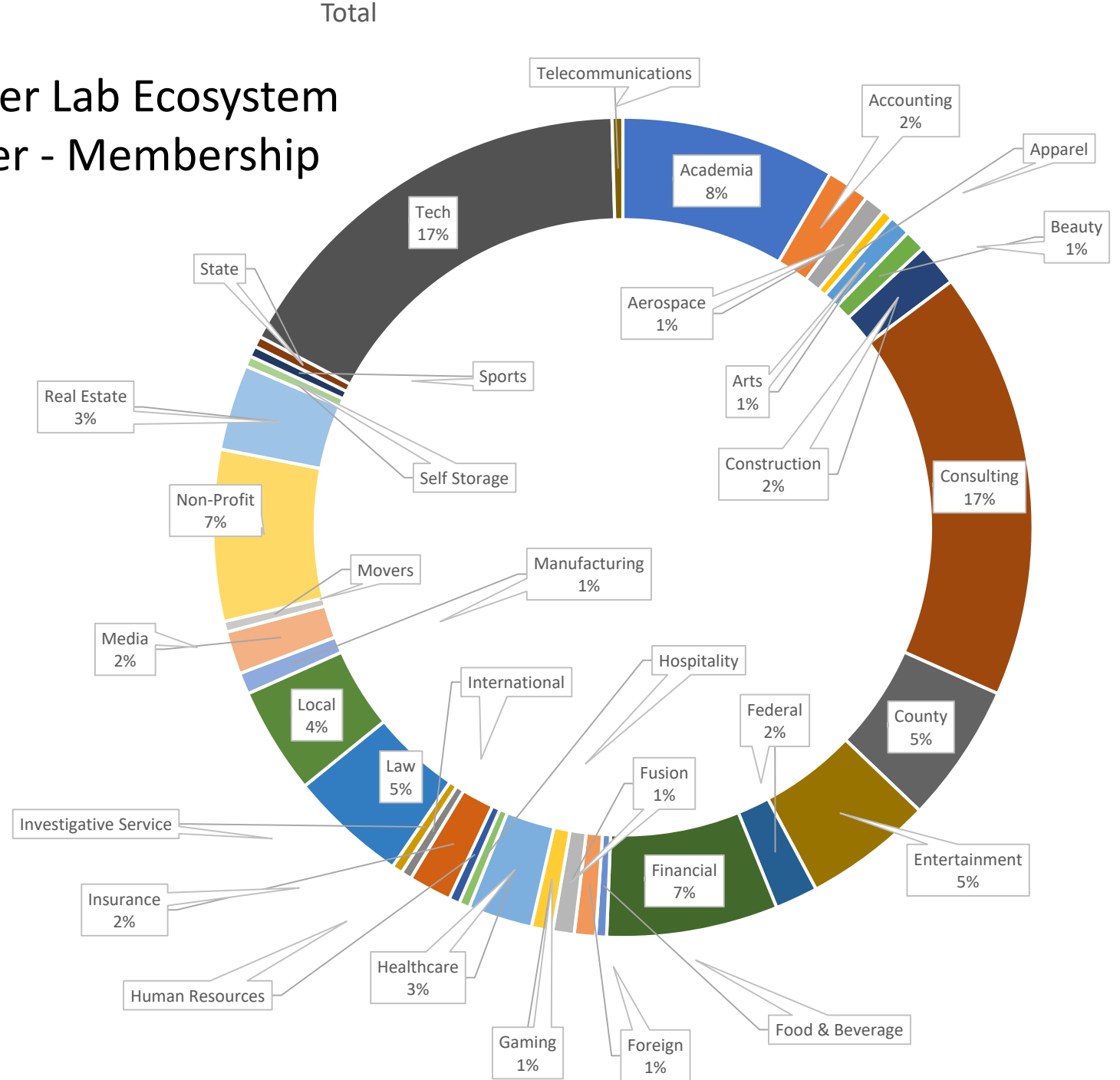
Who We Server - Membership

LACL Partners

City of Los Angeles
 City National Bank
 Dollar Shave Club
 Cedars-Sinai Medical Center
 Hulu
 Riot Games
 SoCal Edison
 Sheppard Mullin
 21st Century Fox

Major Sectors

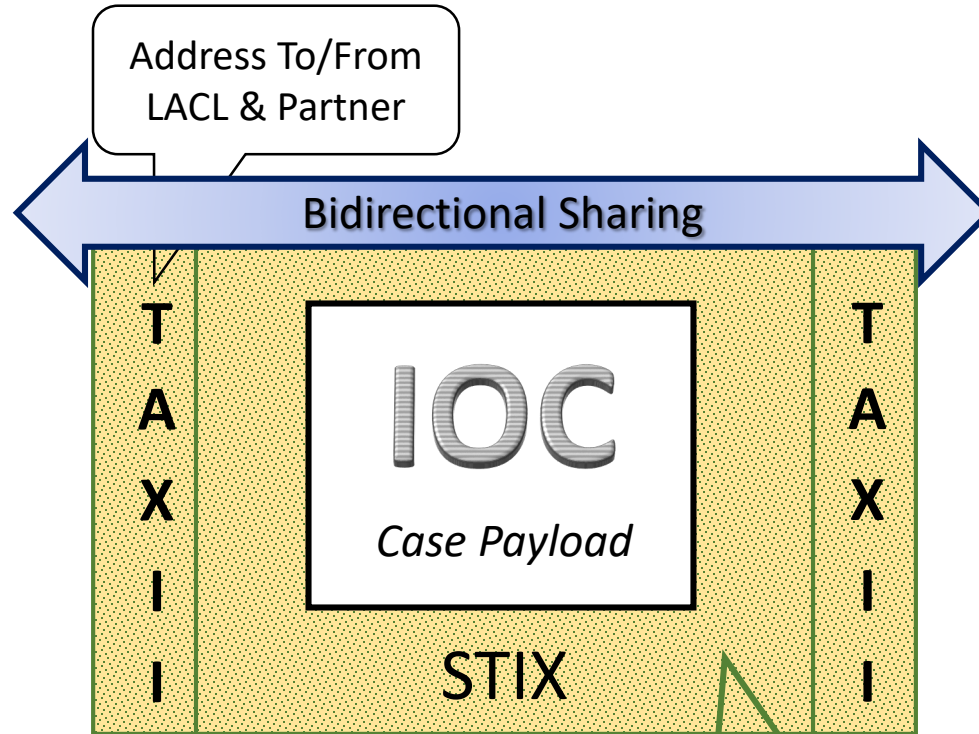
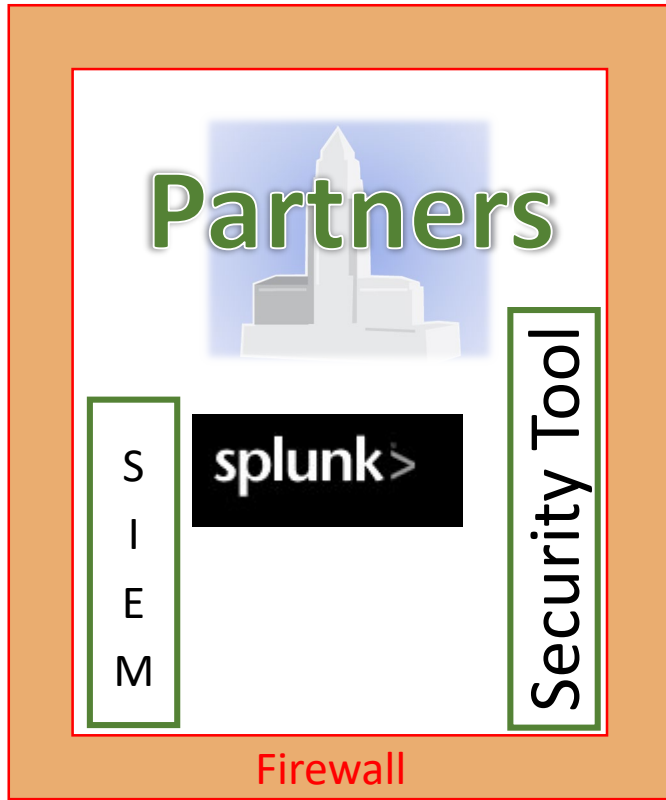
Tech
 Consulting
 Academia
 Financial
 Non-Profit



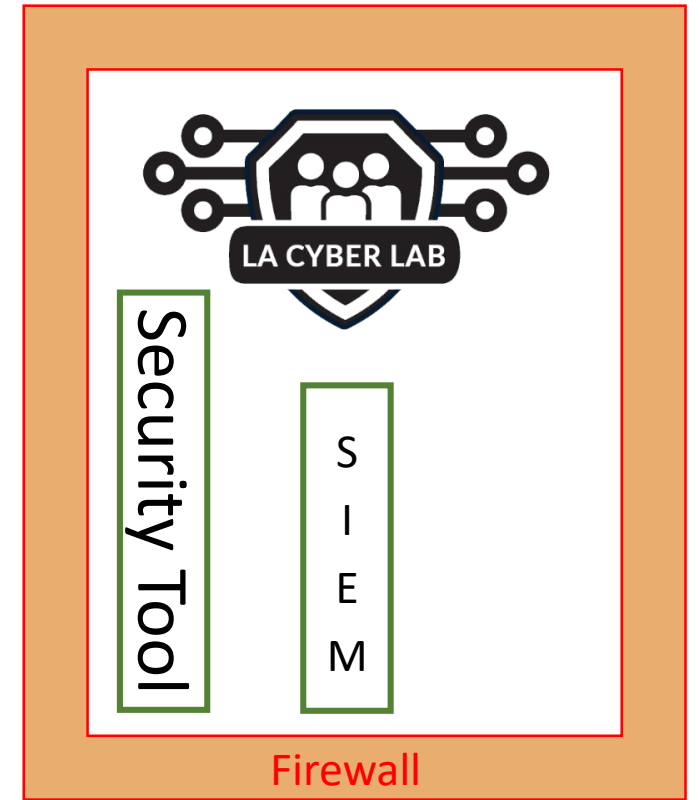


Los Angeles Cyber Lab Ecosystem Bidirectional Sharing 1.0

Current Sharing CONOP



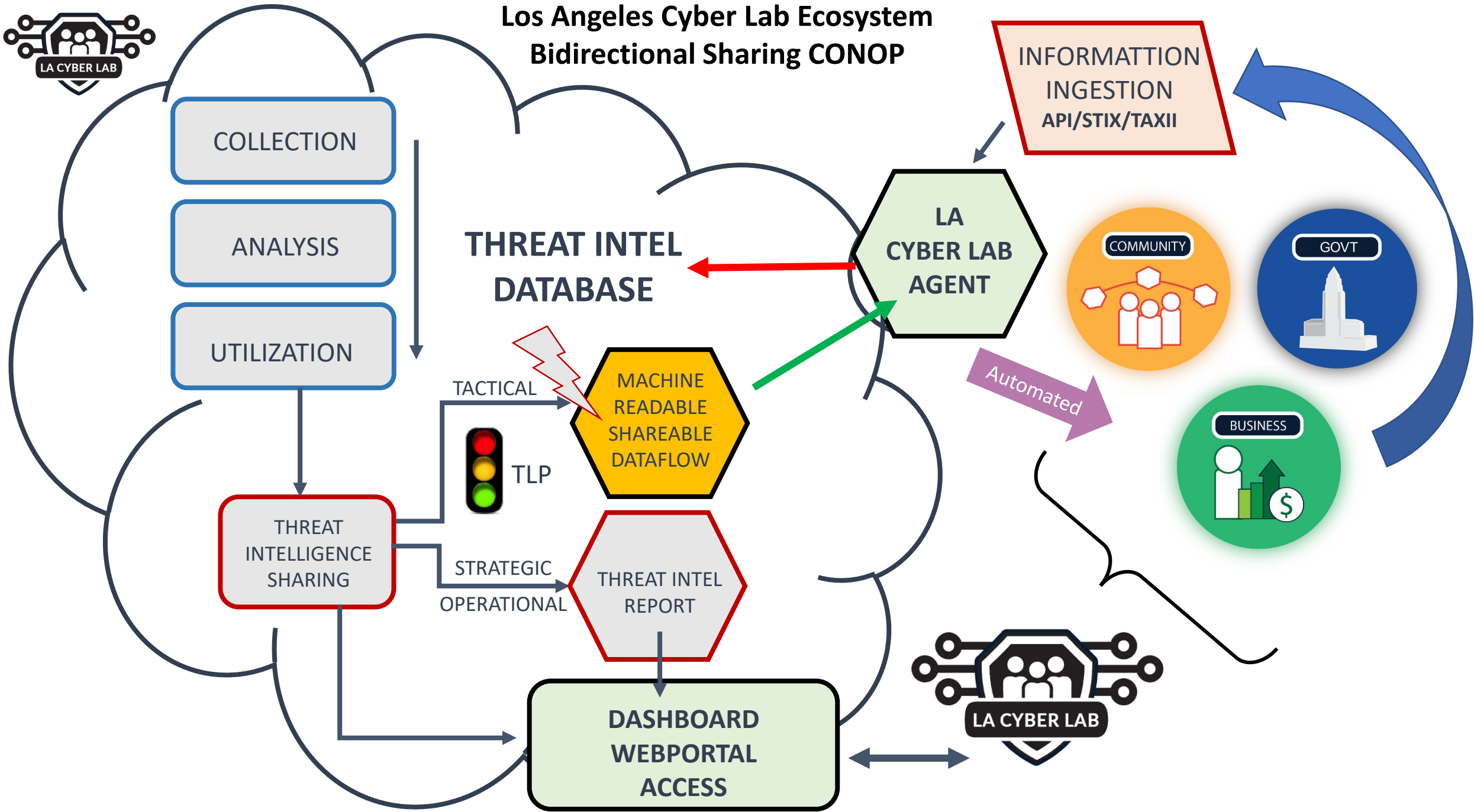
Type of information:
(e.g. IP, Domain, etc.)
of bad actor



Threats & Attacks
(Phishing/Malware)



Los Angeles Cyber Lab Ecosystem Bidirectional Sharing CONOP



THURSDAY, AUGUST 22

Show 50 entries

Search:

Time	Topic
7 a.m. - Noon	Registration
7:30 a.m. - 9 a.m.	Coffee Break Available
8 a.m. - 8:15 a.m.	Opening Remarks
8:15 a.m. - 8:30 a.m.	The Third Annual Information Sharing Hall of Fame Ceremony will recognize the newest Individual and Organizations inductees to the Information Sharing Hall of Fame and be presented by Dr. Greg White, executive director of the ISAO SO.
9 a.m. - 9:30 a.m.	KEYNOTE: InfraGard and Communities. This topic will be presented by Gary Gardner, chairman at InfraGard.
9:30 a.m. - 10 a.m.	Networking Break
10 a.m. - 10:30 a.m.	INTERNATIONAL KEYNOTE , presented by Anyck Turgeon, IBM.
10:30 a.m. - 11 a.m.	KEYNOTE: CyberUSA , presented by David Powell.
11 a.m. - Noon (TRACK #1)	The topic " Anatomy of an IOC " will be presented by Joshua Belk with LA Cyber Lab, Inc.





Threat Intelligence Sharing Platform

Connecting the Community

Two Vendors

- IBM with TruStar
- Mythos (Rosslyn Grp)

Three Unique Data Sources

- Government (Public Sector)
- Community (OSINT)
- Business (Private Sector)

Two Threat Focus Categories Of Data

- Business Email Compromise (BEC) aka Anti-phishing
- Indications of Compromise (IOCs)

Two Threat Sharing Vectors

- Standard B2B IOC sharing
- SMB/Individual M2M BEC threat sharing





Threat Intelligence Sharing Platform

Two Threat Sharing Vectors

- Standard B2B IOC sharing
- SMB/Individual M2M BEC threat sharing



Filter & Refine

- IOC Type
- Open Sources
- Closed Sources
- Tags
- Intel Researchers
- Date Last Seen
- My Enclaves (5)
- Acme Fraud
- Acme Investigations
- Acme Phishing
- Acme SOC
- Acme SOC - Vetted
- Community

IOC	ENCLAVES	CORRELATIONS	TOTAL SIGHTINGS	TAGS	FIRST SEEN	LAST SEEN
SHA1: 9a584dfefb1e0e8d431331790b026fb384f7eb8a	0	0	3	None	01-23-2019 21:50 PST	
IP: 185.7.215.175	0	0	5	None	10-29-2018 10:54 PDT	
URL: f195.imperion.com	0	0	5	None	10-29-2018 11:00 PDT	
IP: 185.19.85.172	0	0	6	None		
URL: rufex.ajfingenieros.cl	0	0	4			
IP: 209.85.223.195	0	0	6			
IP: 119.81.93.82	0	0	4			
MDS: ee5053cbf5cd63546464b085124faa8c					04-04-2019 10:43 PDT	04-04-2019 10:43 PDT

Mobile App Overlay:

- Activity Overview
- Threat Activities: 82 (Normal)
- Sectors: 125 (Breaching), 85 (Exploit)
- Threats: \$126.25 Global Trend
- Types of Threats: 12% (MIA), 27% (Phishing), 40% (Malware), 27% (Ransomware)
- Global Trends
- Sector Specific



Threat Intelligence Sharing Platform

Two Threat Focus Categories Of Data

- Business Email Compromise (BEC)
- Indications of Compromise (IOCs)

The screenshot displays the 'Enclave Insights for [BETA] - [BETA]' dashboard. It features several key sections:

- Internal Enrichment:** A list of reports such as '[AB-C120018605] Issue 5686411: phishing attac...' and '[AB-C12002174L] Issue 5690752: phishing attac...'.
- Community Enrichment:** A list of reports including '[AB-C11994381P] Terra Abuse Report' and '[AB-C12002325Q] Strategic & Tactics for \$killful ...'.
- Relevant IOCs:** A list of IP addresses and domains, such as '54.36.157.33', 'jgw11-smtp.fstcdn.com', and 'web2.premiumdln.com'.
- Intel Source Scoring (BETA):** A section for source scoring with a 'SCORE BREAKDOWN' chart showing IP, URL, and HASH categories with corresponding scores and 'Subscribe' buttons.
- Community Trends:** A sidebar on the right showing 'Trending IOCs' (Top 10), 'Trending Malware' (Top 6), and 'Trending Vulnerabilities' (Top 2).

This screenshot shows a detailed incident report for 'ExecutiveSpearPhish-test'. The report includes:

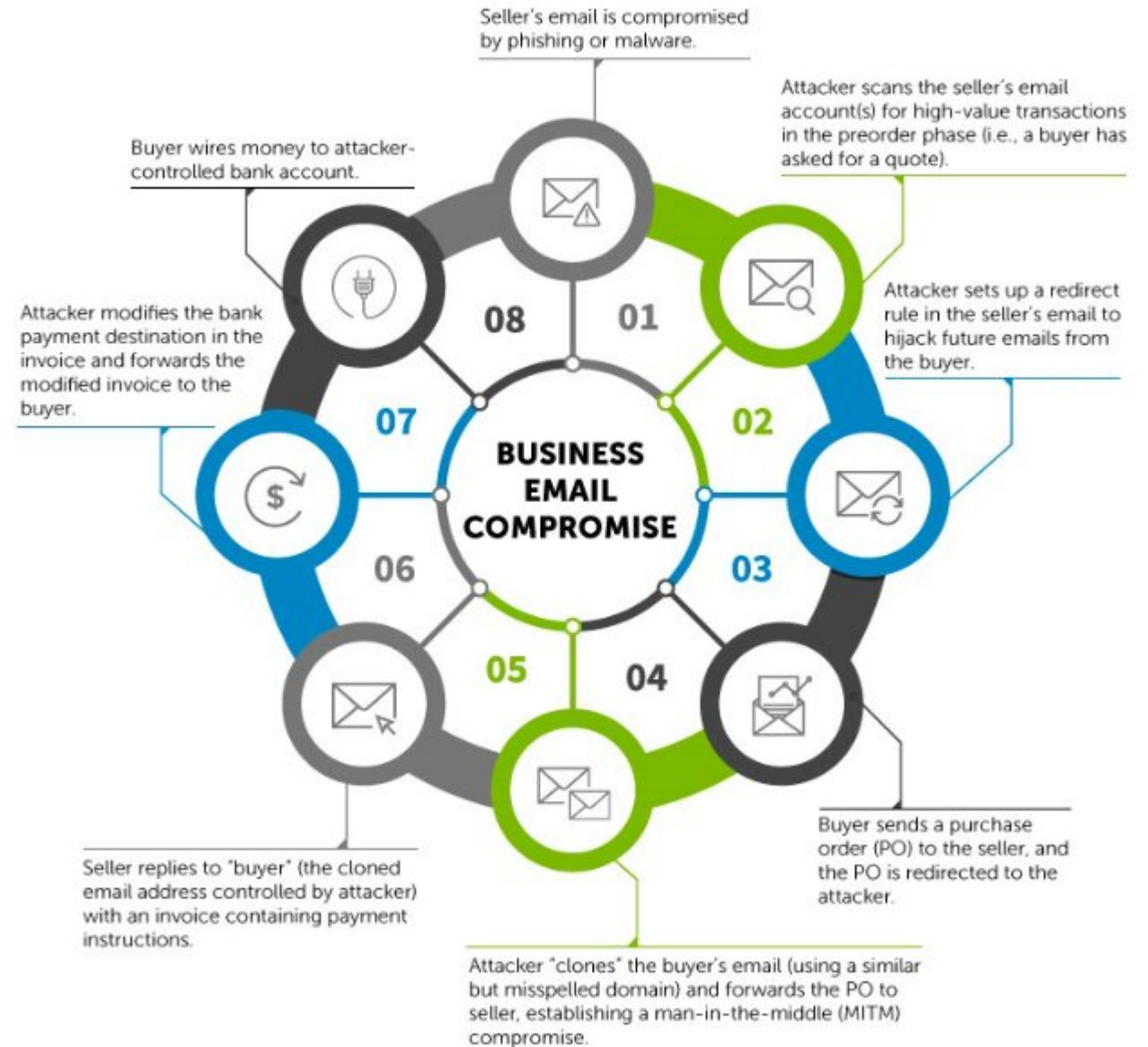
- Metadata:** 'SUBMITTED 04-03-2019 14:01 PDT', 'UPDATED 04-04-2019 14:01 PDT', 'ENCLAVES', 'CORRELATIONS 28', and 'TAGS'.
- Content:** 'Incident Report: 2015-0512', 'Reporting Date (UTC): 15 Aug 2015', and '**** Incident Overview Information'.
- Categories:** 'Categories (CAT): Employee phishing attack'. A note states: 'Provide any additional information to explain how the categories were determined: Employee reported suspect email. Impact from this incident: Critical. Incident Description: We had multiple reports of suspicious email overnight and the IT team reported notifications from email security appliance of a possible...'
- Network Diagram:** A central hub-and-spoke network diagram with nodes representing email accounts and connections indicating relationships or data flow.



Threat Intelligence Sharing Platform

Two Threat Focus Categories Of Data

- **Business Email Compromise (BEC)**
- Indications of Compromise (IOCs)





Threat Intelligence Sharing Platform

Go LOUD 9.17.19

Outreach & Strategic Communications

- Summer Speaker Series
- Networking Events
- Darkweb Training
- **Summit (est. 9.17.19)**

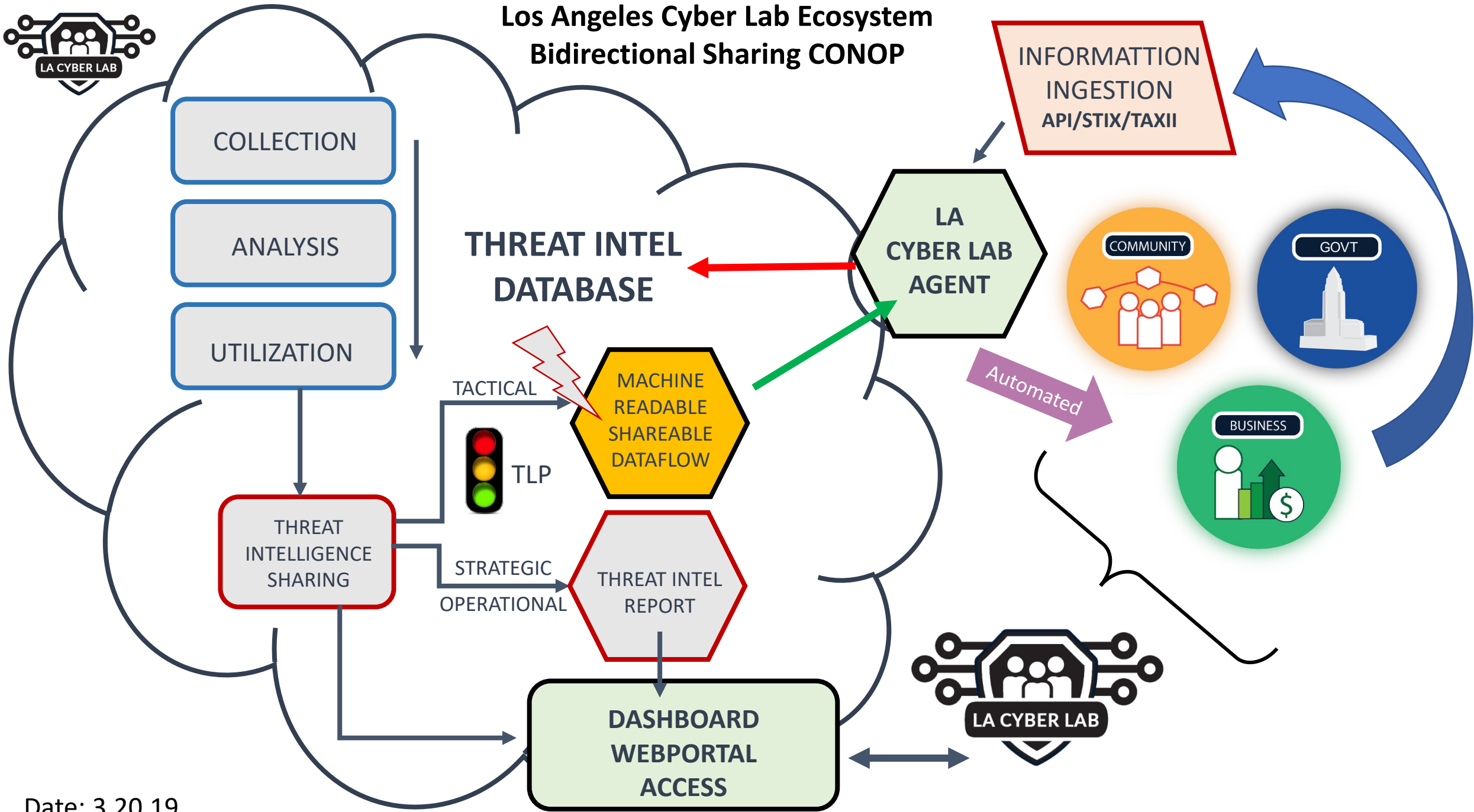
Target Audiences

- Largest 10-15 Cities
- Surrounding Counties
- State
- Large Companies (Mature Security Programs)
- CMAP



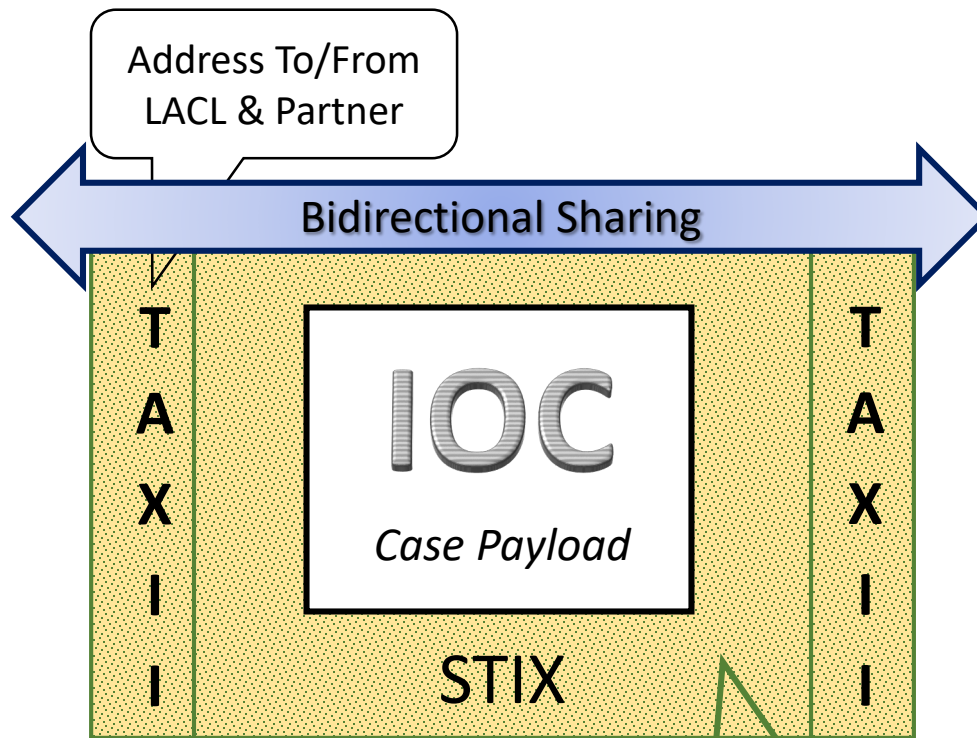
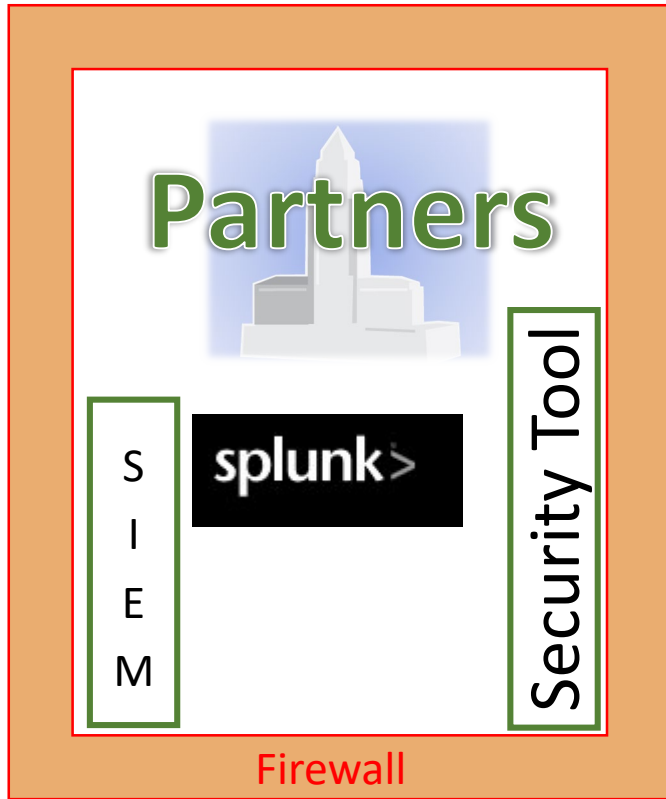


Los Angeles Cyber Lab Ecosystem Bidirectional Sharing CONOP

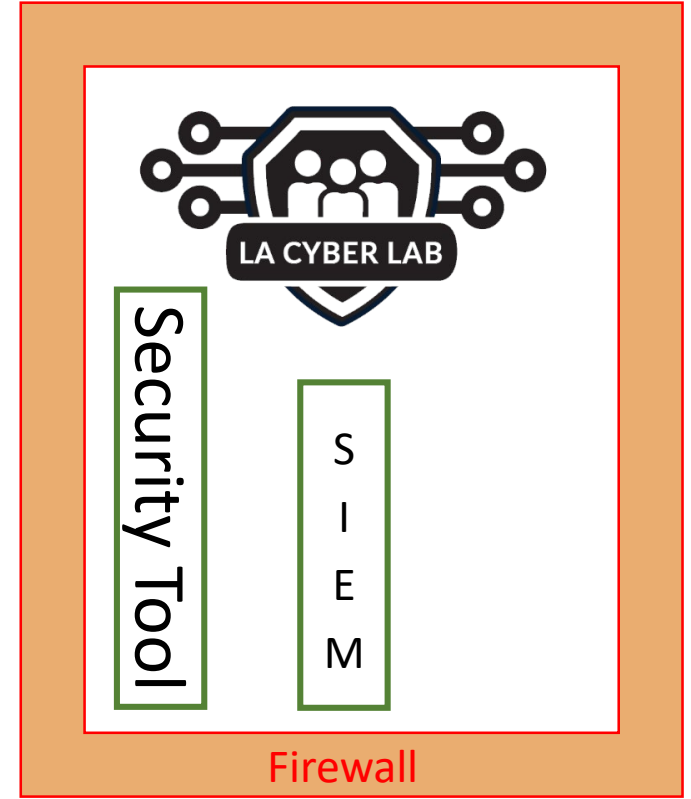




Los Angeles Cyber Lab Ecosystem Bidirectional Sharing 1.0 Sharing CONOP 5.15.19



Type of information:
(e.g. IP, Domain, etc.)
of bad actor



Threats & Attacks
(Phishing/Malware)

