



3RD ANNUAL NATIONAL
**CYBERSECURITY
SUMMIT**



Leveraging MITRE ATT&CK® for Cyber Operations and Risk Management

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. More information available at <https://attack.mitre.org/>.



3RD ANNUAL NATIONAL
**CYBERSECURITY
SUMMIT**

Introductions

- Casey Kahsen
 - Section chief of network forensics for CISA hunt and incident response team
 - Previously served as incident response engagement lead and technical lead for host forensics
 - Extensive work in operationalizing ATT&CK for hunt and incident response operations
- Adam Isles
 - Principal, Chertoff Group, Cyber Defense, Risk Management
 - Led build-out of cyber defense model utilizing ATT&CK for organizations in financial services, retail and manufacturing sectors
 - Prior roles at DHS, DOJ



What is the Security Objective(s)?

- Considerations:
 - Business model
 - Adversary interest
 - How could an adversary compromise me?
 - Security approach and security investments
- Measuring effectiveness:
 - Do our countermeasures actually work?
 - In the event of compromise, are we prepared to respond?



Enter...ATT&CK

1

“Periodic Table” of Tactics & Techniques (prerequisite for mapping to defensive countermeasures)

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (7) Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (5) Shared Modules Software Deployment Tools System Services (2) User Execution (2) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (11) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (15) External Remote Services Hijack Execution Flow (11) Hijack Execution Flow (11) Implant Container Image Office Application Startup (6) Pre-OS Boot (3) Scheduled Task/Job (5) Server Software Component (3) Traffic Signaling (1) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Boot or Logon Autostart Execution (11) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Event Triggered Execution (15) Exploitation for Privilege Escalation Group Policy Modification Hijack Execution Flow (11) Process Injection (11) Scheduled Task/Job (5) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Boot or Logon Autostart Execution (11) Boot or Logon Initialization Scripts (5) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Group Policy Modification Hide Artifacts (6) Hijack Execution Flow (11) Impair Defenses (6) Indicator Removal on Host (6) Indirect Command Execution Masquerading (6) Modify Authentication Process (3) Modify Cloud Compute Infrastructure (4) Modify Registry Obfuscated Files or Information (6) Pre-OS Boot (3) Process Injection (11) Rogue Domain Controller Rootkit Signed Binary Proxy Execution (10) Signed Script Proxy Execution (1) Subvert Trust Controls (4) Template Injection Traffic Signaling (1) Trusted Developer Utilities Proxy Execution (1) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (4) Valid Accounts (4) Virtualization/Sandbox Evasion (3) XSL Script Processing	Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Input Capture (4) Man-in-the-Middle (1) Modify Authentication Process (3) Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Kerberos Tickets (3) Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials (6)	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion (3)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Archive Collected Data (3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Man in the Browser Man-in-the-Middle (1) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

2

Library of Threat Actor Groups (enables mapping to business)

Home > Groups > APT19

APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms.^[1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.^{[2] [3] [4]}

Source: MITRE Corporation

3

Additional Data Elements (enables mapping to defensive countermeasures)

- Data sources
- Mitigations
- Filters (Windows, Linux, cloud, ICS, etc.)



Pyramid of Pain

- ATT&CK Reflects tactics and techniques observed in the real world
- Why is this important?
 - Industry historically focused on methodology that is low on the pyramid
 - Forces adversary to change tools and behavior to avoid detection
 - Lowers their ROI
 - For the Defender:
 - Behavior focused detection > artifact focused detection
 - ATT&CK based hunting

What to search? David Bianco's pyramid of pain



10



Evolution of ATT&CK at CISA

- 2017
 - Large scale campaign tracked via behavioral markers
- 2018
 - Early adoptions of the *Operations Management System* (OMS)
- 2019
 - Began working with MITRE to:
 - Research playbooks
 - Common techniques hunted for across IR industry
 - Data sources required to perform ATT&CK based hunting (tooling to accommodate)
- 2020
 - Evolution of the OMS to leverage ATT&CK
 - ATT&CK integration into custom Splunk App
 - ATT&CK integration into engagement report (customer deliverable)



Operations Management System (OMS)

- Centralized command center location for our deployment teams:
 - Team management and tasking (Planner)
 - Collaboration and document sharing (Teams)
 - Engagement notes and documentation (OneNote)
 - Engagement document management (SharePoint)
- Goals:
 - Significant reduction of **time to effective analysis** (automation & templates)
 - Compounded effect results in reduction of
 - Time to effective detection
 - Time to effective defense
 - Time to effective reporting



OMS cont.

- Pre-built templates
 - Standardized tasks (e.g. service)
 - All teams function
- Allows our leads (end)
 - Designate tasks
 - Track progress of

The screenshot displays the OMS interface with three main tabs: Initial Access, Execution, and Persistence. The Initial Access tab is active, showing a list of task templates. The 'External Remote Services' template is highlighted with a blue box. A modal window is open for this template, showing configuration options.

Initial Access Tab:

- + Add task
- Drive-By Compromise (0/19)
- Exploit Public-Facing Applications (0/16)
- External Remote Services (0/6)**
- Hardware Additions (0/13)
- Replication through Removable Media (0/4)
- Spearphishing Attachment (0/20)
- Spearphishing Link (0/20)

Execution Tab:

- + Add task
- AppleScript

Persistence Tab:

- + Add task
- .bash_profile and .bashrc

External Remote Services Task Configuration:

- Assign
- Bucket: Initial Access
- Progress: Not started
- Priority: Medium
- Start date: Start anytime
- Due date: Due anytime
- Notes: 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.
<https://attack.mitre.org/techniques/T1133/>
<https://capec.mitre.org/data/definitions/555.html>
- Data sources: Authentication logs
NFS: vpn logs
HFS: user directory review
- Checklist 0 / 6
 - NFS - VPN logs
 - HFS - VPN server authentication review
 - HFS - Windows Event Logs
 - HFS - ShimCache, AmCache, Prefetch (Evidence of execution artifacts)
 - HFS - File Item Listing
 - HFS - Registry Hives
 - Add an item

OMS cont.

- Analytical tasks organized and use ATT&CK methodology
 - Characterizes phases of threat actor activity
 - Industry standard lexicon/terminology
- Baseline data for understanding the analytical task
 - Junior analysts
- Adversary tactics based hunting
 - Drives our teams to look for relevant data that is **high on the pyramid**
- OMS 2.0
 - Leverage decision trees based on identified techniques (if X is detected, then search for Y)



ATT&CK in CIS

Identified Techniques				filters						
Threat actor techniques identified during the engagement and analysis				stages: act platforms: Windows, Azure, Azure AD, Office 365						
Initial Access	Execution	Persistence	Privilege	Defense	Credential	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration

legend	
■	New TTPs Detected by HIRT
■	TTPs Known and Detected by HIRT

(1) Institute Multi-Factor Authentication for Access to M365

ACME currently utilizes username and password for authentication to M365, syncing cloud credentials to Active Directory. As seen in this incident, simple username and password authentication is easily compromised by an adversary, with the adversary gaining complete access to the compromised account's email, which contain vital information.

CISA recommends that ACME leverage the security of multi-factor authentication (MFA) supplied within M365. MFA utilizes two or more factors to authenticate to systems. This can be a combination of username and password and a token, either soft or physical. With this extra step, an adversary would be prevented from gaining access to ACME's M365 environment if they were able to compromise username and password credentials again.

Summary: MFA ([M1032]) helps mitigate the following threat actor techniques that were observed in use in this incident: |

Table 3: Observed ATT&CK techniques that align with this mitigation

Initial Access	Persistence	Collection
Valid Accounts [T1078]	Account Manipulation [T1098]	Email Collection [T1114]

Initial Access	Execution	Persistence	Privilege	Defense	Credential	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Account Manipulation	Exploitation of Remote Services	Data from Information Repositories	Commonly Used Port	Data	Compressed					
User Enumeration	Remote Desktop Protocol	Data from Local System	Connection Proxy	Data	Encrypted					
Command and Control	Remote File Copy	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Alternative Protocol						
Exfiltration		Data Staged	Remote Access Tools	Exfiltration Over Command and Control Channel						
Item Work Configuration		Email Collection	Remote File Copy							
Item User/User			Uncommonly Used Port							

adversary techniques

ATT&CK: Tying Mission/Business Model to Threat and Tying Threat Actors to TTPs

1

ID key business attributes



- Core manufacturing processes
- Sensitive IP
- Personal data
- Volume of financial transactions

2

Research to identify threat actors targeting those business attributes



- Research and analysis of Open-Source, Commercial Threat Intelligence
 - MITRE ATT&CK, etc.
- Alerts from CISA, other public sector sources
- Engage w/ defenders to confirm relevance

3

Map threat actors to TTPs

Initial	T1059	T1037	T1053	T1143	T1110	T1046	T1037	T1115	T1132	T1002	Impact
T1073	T1086	T1053	T1050	T1064	T1141	T1201	T1077	T1113	T1105	T1022	T1487
T1189	T1086	T1053	T1050	T1064	T1141	T1201	T1077	T1113	T1105	T1022	T1487
T1193	T1086	T1053	T1050	T1064	T1141	T1201	T1077	T1113	T1105	T1022	T1487
T1192	T1086	T1053	T1050	T1064	T1141	T1201	T1077	T1113	T1105	T1022	T1487
T1194	T1086	T1053	T1050	T1064	T1141	T1201	T1077	T1113	T1105	T1022	T1487
	T1035	T1023	T1088	T1112	T1503	T1217	T1021	T1185	T1043		T1485
	T1047	T1158	T1068	T1117	T1056	T1482	T1534	T1125	T1090		T1486
	T1117	T1060	T1055	T1107	T1081	T1083	T1210	T1119	T1094		T1529
	T1223	T1078	T1138	T1150	T1040	T1135	T1075	T1005	T1103		T1494
	T1203	T1098		T1099	T1040			T1074	T1020		T1490
	T1085	T1108		T1078		T1120			T1071		T1493
	T1218	T1067		T1134		T1069			T1055		
	T1220	T1138		T1088		T1057			T1102		
	T1170			T1012		T1012			T1024		
	T1191			T1089		T1018			T1008		
	T1173			T1055		T1063					
	T1106			T1085		T1018					
	T1204			T1218		T1082					
				T1220		T1016					
				T1140		T1045					
				T1170		T1033					
				T1095		T1007					
				T1116		T1124					
				T1090		T1497					
				T1106							
				T1102							
				T1146							
				T1191							
				T1073							

- TTPs are risk-rated and sorted based on priority
- Supplement with ubiquitous TTPs
 - TTPs used by all groups regardless of sightings



ATT&CK: Sample Threat Model

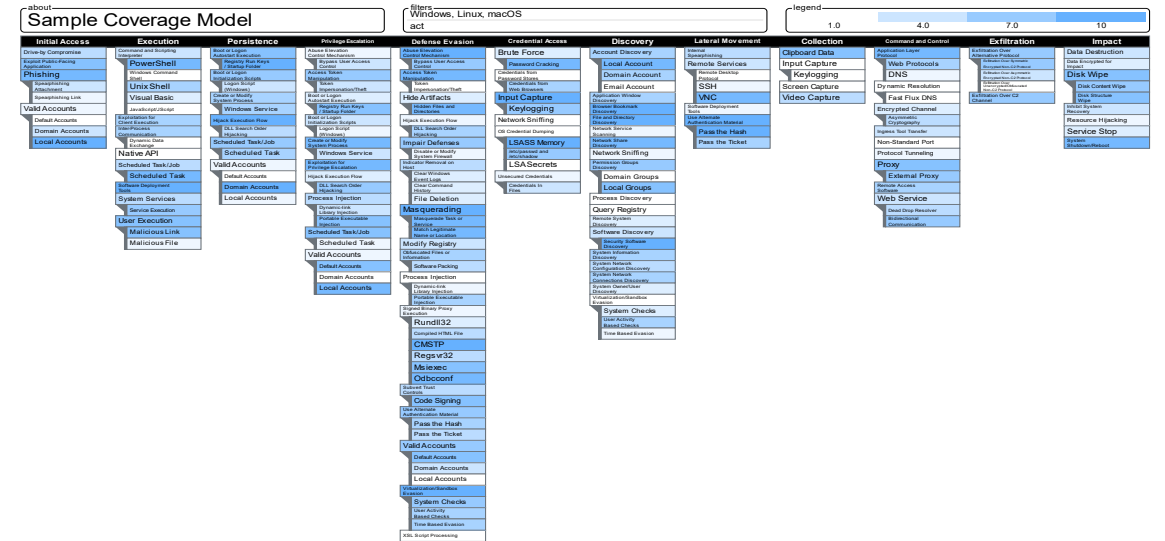
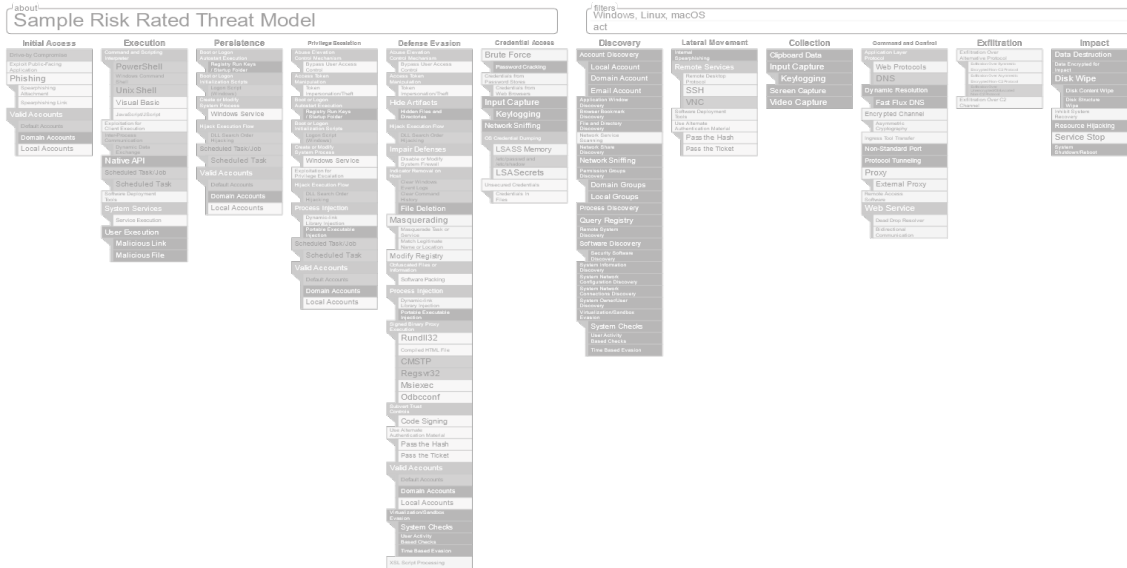
about
Sample Threat Model

filters
Windows, Linux, macOS
act

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Internal Spearphishing	Clipboard Data	Application Layer Protocol	Exfiltration Over Alternative Protocol	Data Destruction
Exploit Public-Facing Application	PowerShell	Registry Run Keys / Startup Folder	Bypass User Access Control	Bypass User Access Control	Password Cracking	Local Account	Remote Services	Input Capture	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Data Encrypted for Impact
Phishing	Windows Command Shell	Boot or Logon Initialization Scripts	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Domain Account	Remote Desktop Protocol	Keylogging	DNS	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Disk Wipe
Spearphishing Attachment	Unix Shell	Logon Script (Windows)	Token Impersonation/Theft	Token Impersonation/Theft	Credentials from Web Browsers	Email Account	SSH	Screen Capture	Dynamic Resolution	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Disk Content Wipe
Spearphishing Link	Visual Basic	Create or Modify System Process	Boot or Logon Autostart Execution	Hide Artifacts	Input Capture	Application Window Discovery	VNC	Video Capture	Fast Flux DNS	Exfiltration Over C2 Channel	Disk Structure Wipe
Valid Accounts	JavaScript/JScript	Windows Service	Registry Run Keys / Startup Folder	Hidden Files and Directories	Input Capture	Browser Bookmark Discovery	Software Deployment Tools		Encrypted Channel		Inhibit System Recovery
Default Accounts	Exploitation for Client Execution	Hijack Execution Flow	Boot or Logon Initialization Scripts	Hijack Execution Flow	Keylogging	File and Directory Discovery	Use Alternate Authentication Material		Asymmetric Cryptography		Resource Hijacking
Domain Accounts	Inter-Process Communication	DLL Search Order Hijacking	Logon Script (Windows)	DLL Search Order Hijacking	Network Sniffing	Network Service Discovery	Pass the Hash		Ingress Tool Transfer		Service Stop
Local Accounts	Dynamic Data Exchange	Scheduled Task/Job	Create or Modify System Process	Impair Defenses	OS Credential Dumping	Network Share Discovery	Pass the Ticket		Non-Standard Port		System Shutdown/Reboot
	Native API	Valid Accounts	Windows Service	Indicator Removal on Host	LSASS Memory	Permission Groups Discovery			Protocol Tunneling		
	Scheduled Task/Job	Default Accounts	Exploitation for Privilege Escalation	Disable or Modify System File/shadow	etc/passwd and etc/shadow	Domain Groups			Proxy		
	Scheduled Task	Domain Accounts	Hijack Execution Flow	File Deletion	LSASecrets	Local Groups			External Proxy		
	Software Deployment Tools	Local Accounts	DLL Search Order Hijacking	Masquerading	Unsecured Credentials	Query Registry			Remote Access Software		
	System Services		Process Injection	Dynamic-link Library Injection	Credentials in Files	Software Discovery			Web Service		
	Service Execution		Dynamic-link Library Injection	Masquerade Task or Service		Security Software Discovery			Dead Drop Resolver		
	User Execution		Portable Executable Injection	Match Legitimate Name or Location		System Information Discovery			Bidirectional Communication		
	Malicious Link		Scheduled Task/Job	Modify Registry		System Network Configuration Discovery					
	Malicious File		Scheduled Task	Obfuscated Files or Information		System Network Connections Discovery					
			Valid Accounts	Software Packing		System Owner/User Discovery					
			Default Accounts	Process Injection		Virtualization/Sandbox Evasion					
			Domain Accounts	Dynamic-link Library Injection		System Checks					
			Local Accounts	Portable Executable Injection		User Activity Based Checks					
				Signed Binary Proxy Execution		Time Based Evasion					
				Rundll32							
				Compiled HTML File							
				CMSTP							
				Regsvr32							
				Msiexec							
				Odbcconf							
				Subvert Trust Controls							
				Code Signing							
				Use Alternate Authentication Material							
				Pass the Hash							
				Pass the Ticket							
				Valid Accounts							
				Default Accounts							
				Domain Accounts							
				Local Accounts							
				Virtualization/Sandbox Evasion							
				System Checks							
				User Activity Based Checks							
				Time Based Evasion							
				XSL Script Processing							



ATT&CK: Prioritizing Investments

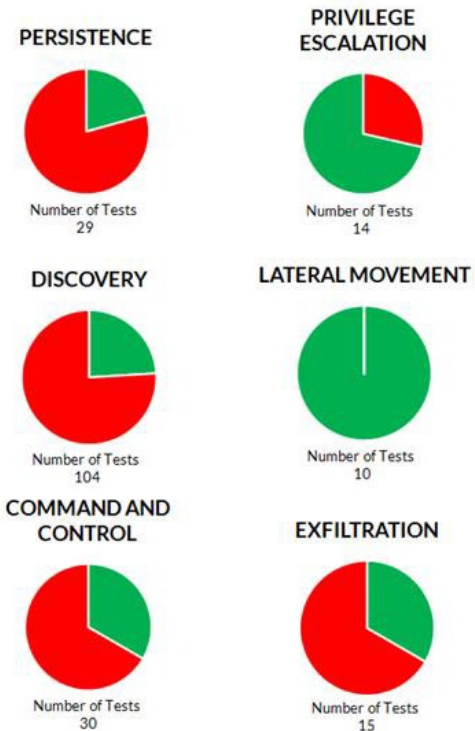


3RD ANNUAL NATIONAL
CYBERSECURITY
SUMMIT

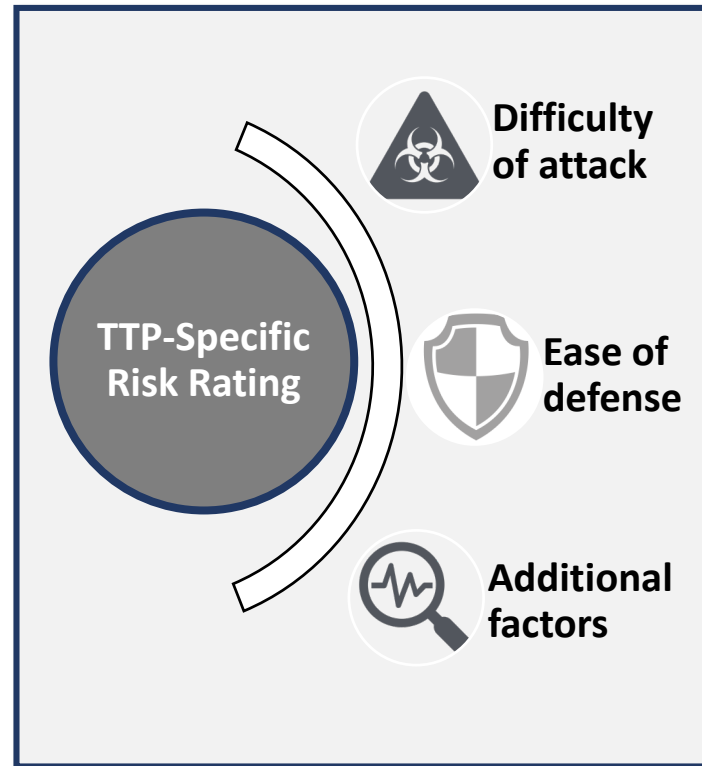


ATT&CK: Measuring Performance

**Run Testing;
Obtain Pass/Fail test results**



Apply TTP-specific Risk Rating



**Generate
Performance Rating**



**Trending/
benchmarking context**



**Risk
Diagnostic
Example**



3RD ANNUAL NATIONAL
**CYBERSECURITY
SUMMIT**



ATT&CK & Risk: Summary



ATT&CK TTP ID numbering in CISA alerts helps identify repeat TTPs (and thereby prioritize countermeasures)



When CISA alerts identify targeted asset types, this helps identify sample sets for testing



INHERENT RISK

THREAT MODEL

THREAT RATING

MAPPING

SAMPLE SET

MEASURE

BUSINESS CASE

Isolate a core set of risk-informing factors and generate inherent risk profiles across business units

Identify likely threat actors based on client's industry sector; generate set of TTPs likely to be applied against organization

Risk-rate TTPs based on factors such as ease of attack, difficulty of defense, impact, frequency

Map organization's defensive countermeasures to likely TTPs

Identify sample set of assets for initial diagnostic

Measure overall effectiveness in defending against sample TTP set

Develop business case justification for investments based on risk reduction potential



CISA alerts help map threat actors and TTPs to industry sectors



ATT&CK Mitigation ID numbering in CISA alerts help map TTPs to mitigations



3RD ANNUAL NATIONAL
CYBERSECURITY
SUMMIT





How'd I do?

- Survey Monkey Link
- Mobile Link
 - Text Survey to XXX-XXX

