CISA Cybersecurity Resources for State, Local, Tribal, and Territorial

Overview

CISA offers the following cybersecurity services to support the security and resilience of state, local, tribal, and territorial (SLTT) partners:

Action CISA's Top Three Resources for SLTT

- Connect with your **regional Cybersecurity Advisor.**
- Sign up for **Cyber Hygiene Services.**
- Work with your regional Cybersecurity Advisor to perform a **Cyber Performance Goals Assessment**.

Regional Cybersecurity Advisors

https://www.cisa.gov/about/regions

- Provide cybersecurity preparedness assessments and technical assistance.
- Gateway to CISA cybersecurity services, products, and programs.
- Support preparation, response, and recovery efforts for hazards impacting critical infrastructure.
- Conduct and integrate infrastructure assessments and analysis—including dependencies and cascading effects—on critical infrastructure to influence decision-making at all phases of emergency management.
- Facilitate information sharing between public and private sector critical infrastructure partners.
- Improve situational awareness of cybersecurity risks and incidents.
- Connect SLTT partners to the **SLTT Security Operations Center (SOC) Call**, a bimonthly call that shares timely cyber defense information tailored for SLTTs.

Cyber Hygiene Services

https://www.cisa.gov/cyber-hygiene-services

- Cyber Hygiene services can assist SLTT partners in:
  - Reducing risk to internet-facing configurations and known vulnerabilities.
  - Avoiding surprises.
  - Sharpening their responses.
  - Broadening their security horizon.
- CISA also consistently reviews Cyber Hygiene data to message entities on emerging vulnerabilities.

Cybersecurity Performance Goals Assessment

https://www.cisa.gov/cpg

- CISA's Cybersecurity Performance Goals (CPGs):
  - Are a set of practices organizations should implement to kickstart their cybersecurity efforts.
  - Can help SLTT partners determine the areas they need to invest additional time in and develop to improve cyber defense.
- SLTT partners can work with their regional Cybersecurity Advisor to perform a CPG Assessment.

As of September 2025

Additional Services:

Secure Cloud Business Applications (SCuBA)

https://www.cisa.gov/scuba

SCuBA provides tailored cloud solutions guidance and secure configuration baselines (SCBs) for Microsoft 365 (M365) and Google Workspace (GWS) applications.

ScubaGear and ScubaGoggles tools:

- Compare tenant configurations to CISA's security recommendations.
- Lower the amount of effort required for organizations to assess themselves, providing a detailed report.
- Have code updates released on a regular basis to address Google's and Microsoft's configuration updates.
- Do not collect data or share with CISA, they only create output reports.

Logging Made Easy (LME)

https://www.cisa.gov/lme

CISA's LME provides a free, easy-to-deploy log management solution. It includes real-time threat alerts, customizable dashboards, and community collaboration on GitHub, helping small to medium-sized organizations improve their cybersecurity.

LME offers:

- Centralized logging.
- Proactive threat detection.
- Enhanced security by allowing organizations to monitor their networks, identify users, and actively analyze Sysmon data.

Protective Domain Name System Resolver

https://www.cisa.gov/pdns

Protective DNS Resolver is a device-centric service that blocks and secures organizations' web traffic from reaching malicious destinations by using state-of-the-art DNS technologies.

Through advanced analysis of DNS logs data, the Protective DNS service provides customers:

- An increased visibility into DNS traffic across their networks through flexible analysis tools, dynamic dashboards, and customizable alerts.
- It also filters DNS queries to prevent resolution for known malicious domains and/or IP addresses.
- This service is only available to limited number of entities at this time.

Malcolm

https://www.cisa.gov/malcolm

Malcolm is a network traffic analysis tool suite which enables the user to capture full network packet artifacts (PCAP files) and logs in OT/ICS environments, allowing customers to collect and index IT & OT logs, enrich log data with threat intelligence and network context, and support customer cyber hygiene goals (asset inventory, continuous monitoring, etc.)

Use Malcolm for:

- Network Visibility.
- Threat Detection & Hunting.
- User-Friendly Visualization
- Scalability & Flexibility.
- Compliance & Forensics.

Cybersecurity Publications and Products

https://www.cisa.gov/news-events/cybersecurity-advisories

- CISA continually releases cybersecurity alerts, advisories, and tools to help entities enhance their cyber defense. Recent Examples:
  - **Eviction Strategies Tool**
    https://www.cisa.gov/resources-tools/resources/eviction-strategies-tool
  - **CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt**
    https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a
  - **Primary Mitigations to Reduce Cyber Threats to Operational Technology**
    https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

Professional Services

CISA provides a limited number of vulnerability assessments and vulnerability services to critical infrastructure entities. Engage with your Regional Cybersecurity Advisor to learn more.