CIS Services

For State, Local, Tribal, and Territorial Government Organizations

As the complexity of cyber-attacks continue to evolve and the frequency of those cyber-attacks increase, organizations must apply a defense-in-depth approach to ensure their ability to protect, prevent, detect, respond to, and recover from external and internal attacks. Since there is no single technology or set of controls that will provide a complete solution, this layered, risk-based approach to security is essential, regardless of the size, complexity, or vertical industry of the organization.

The Center for Internet Security® (CIS®) has architected security solutions with the critical nature of defense-in-depth in mind. U.S. State, Local, Tribal and Territorial (SLTT) government organizations can deploy a defense-in-depth strategy to significantly improve their cybersecurity posture with these services offered by CIS, the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®).

CIS SecureSuite®

CIS SecureSuite Membership includes tools and resources to help implement cybersecurity best practices:

- CIS Benchmarks secure configuration guides (Word, Excel, OVAL/XML)
- Unlimited scans/assessments with CIS-CAT® Pro Assessor (a CIS Benchmark configuration assessment tool) which includes CIS-CAT Pro Dashboard reporting
- CIS Controls® cybersecurity best practices and related resources

CIS SecureSuite Membership is offered to all SLTTs at no cost by CIS.

CIS Endpoint Security Services (ESS)

CIS ESS offers device-level protection and response to strengthen an organization's cybersecurity program, and provides active defense against both known (signature-based) and unknown (behavioral-based) malicious activity, as well as effective defense against encrypted malicious traffic. The service includes various measures to protect endpoint devices and is fully monitored and managed 24×7×365 by our Security Operations Center (SOC). CIS ESS can stop an attack in its tracks upon identifying a threat on an endpoint, regardless of the network it is connected to, taking an active role in mitigating and remediating malware affecting an organization's devices by killing or quarantining files.

Albert Network Monitoring and Management

Albert is a cost-effective Intrusion Detection System (IDS) available to SLTT entities, including election organizations, critical infrastructure, and public education.

- Turnkey solution incorporating 24×7×365 monitoring and management

Utilizes commercial, open-source, and custom signatures developed from leveraging our federal partners for access to recently de-classified signatures, indicators CIS derives from incident response cases, as well as member submitted and third-party threat data.

Managed Security Services

The 24×7×365 SOC provides SLTT entities cost-effective log and security event monitoring of existing devices including, but not limited to, IDS/IPS, firewalls, switches & routers, servers, endpoints and web proxies. Actionable items are escalated to organizations as an alert and our SOC is always on hand to answer questions regarding alerts or notifications received.

Digital Forensics and Incident Response (DFIR)

CIS offers DFIR services to both MS-ISAC and EI-ISAC members at no cost, providing host and network forensics, understanding the root cause of a compromise, investigating insider threat activity, analyzing malware, and providing recommendations for remediating a cyber-attack.

Vulnerability and Risk Management

CIS provides cost-effective vulnerability management solutions for networks and web applications as well as penetration testing and phishing engagements. Some services include:

- Network discovery and mapping
- Vulnerability assessment reporting
- Testing vulnerabilities for false-positives
- Identification of high-value assets
- Prioritizing vulnerabilities based on risk
- Custom phishing campaigns

Our network and web application penetration testing services simulate a real-world cyber-attack. Taking the vantage point of an attacker, our experts attempt to exploit vulnerabilities in an organization's IT infrastructure in order to determine the likelihood and potential scope of a cyberattack. At the conclusion of testing, the findings are delivered in a detailed report, with prioritized remediation recommendations.

Malicious Domain Blocking and Reporting (MDBR)

MDBR is a highly effective, no-cost solution available to both MS-ISAC and EI-ISAC members that proactively blocks network requests from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats such as malware, phishing, and ransomware. Organizations are provided with weekly reports summarizing the potentially malicious requests that were detected.

MDBR can be implemented in minutes, on existing systems, without additional hardware or software.

For more information contact the Center for Internet Security at services@cisecurity.org.