CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MS-ISAC Services Guide

MS-ISAC Services Guide

Contents

MS-ISAC Overview

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®), has been designated by the Cybersecurity & Infrastructure Security Agency (CISA) as the key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments.

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication.

The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit cisecurity.org/ms-isac/ or info@msisac.org for more information.

JOINING THE MS-ISAC

There is no cost to join the MS-ISAC, and membership is open to all SLTT government entities. The only requirement is agreement to the Terms and Conditions, which outlines a member's responsibilities to protect information that is shared.

What We Offer

- The MS-ISAC provides **real-time** network monitoring and management, threat analysis, and early warning notifications through CIS's 24×7×365 Security Operations Center (SOC).
- Focal point for cyber threat prevention, protection, response and recovery for U.S. SLTT governments.
- We perform **incident response and remediation** through our team of security experts.
- The MS-ISAC conducts **training sessions and webinars** across a broad array of cybersecurity related topics.
- We continually develop and distribute **strategic, tactical, and operational intelligence** to provide timely, actionable information to our members.
- We provide **cybersecurity resources** for the public, including daily tips, monthly newsletters, guides, and more.

Who We Serve

CISOs, CIOs, and other security professionals from:

- U.S. State, Local, Tribal, and Territorial governments
- U.S. State/Territory Homeland Security Advisors
- DHS-recognized Fusion Centers and local law enforcement entities

How We Do Business

- We cultivate a **collaborative environment** for information sharing.
- We focus on **readiness and response,** especially where the cyber and physical domains meet.
- We facilitate **partnerships** between the public and private sectors.
- We focus on **excellence** to develop industry-leading, cost-effective cyber-security resources.
- **Collectively** we achieve much more than we can individually.

"All services performed by the MS-ISAC were not only prompt, but professional and efficient. Communication was handled very well and the report was fantastic."

MS-ISAC Member

Member Responsibilities

In order to maintain the MS-ISAC's trusted, collaborative environment, each member understands that the following principles of conduct will guide their actions.

Each member agrees to:

- Share appropriate information between and among the members to the greatest extent possible
- Recognize the sensitivity and confidentiality of the information shared and received
- Take all necessary steps to protect confidential information
- Transmit sensitive data to other members only through the use of agreed-upon secure methods
- Take all appropriate steps to help protect our critical infrastructure

Members are also asked to share their **public-facing IP ranges and domain space** with the MS-ISAC to facilitate efficient and effective discovery and notification of system compromises and potential vulnerabilities.

"I will continue to leverage this expert and valuable service as long as it exists. The MS-ISAC CIRT was once again very efficient and provided a robust root cause analysis in a timely fashion."

MS-ISAC Member

Reporting an Incident and Requesting Assistance

Members are encouraged to report incidents, even if they are not requesting assistance, to improve situational awareness for the benefit of all members.

Types of incidents to report include the following:

- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Compromised password(s)
- Execution of malware, such as viruses, trojans, worms, ransomware, or botnet activity
- Defacement of a government web page
- Disruption or attempted denial of service (DoS)
- Unauthorized access to information
- Unauthorized use of a system for transmitting, processing, or storing data
- Unauthorized use or elevation of system privileges

If the cybersecurity incident you are reporting requires direct assistance, the CIRT, a unit comprised of highly trained and experienced staff, is able to assist you at no cost. Our incident response experts can assist with the following:

- Emergency conference calls
- Log analysis
- Mitigation and response recommendations
- Reverse engineering
- Threat Intelligence

REPORTING CYBERSECURITY INCIDENTS

To report an incident, please contact the MS-ISAC SOC for 24×7×365 assistance:

PHONE
1-866-787-4722

EMAIL
soc@cisecurity.org

Security Operations of the MS-ISAC

No-cost Services

Security Operations Center

The MS-ISAC operates within CIS's SOC, which is a 24x7x365 joint security operations and analytical unit that monitors, analyzes and responds to cyber incidents targeting SLTT government entities.

The SOC provides real-time network monitoring and notification, early cyber threat warnings and advisories, and vulnerability identification and mitigation.

Cyber Vulnerability and Threat Research

Analysts monitor federal government, third party, and open sources to identify, analyze, and then distribute pertinent intelligence.

Compromised System Notifications

Provided to members in the event of a potential compromise identified based on the MS-ISAC's unique awareness of the threat landscape.

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. Learn more on page 4.

Cyber Incident Response Team (CIRT)

CIRT provides SLTT governments with malware analysis, computer and network forensics, malicious code analysis/mitigation, and incident response. External vulnerability assessments are also available post a cyber incident. This service helps victims of cyber incidents to check if their remediation efforts have been effective.

National Liaison Team

The National Liaison Team is assigned to CISA Central to represent MS-ISAC and SLTT interests. CISA Central is a 24×7×365 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

Cyber Threat Intelligence (CTI)

The CTI team collects, analyzes, and delivers actionable intelligence to operators and decision-makers responsible for defending SLTT governments. CTI maintains a curated, real-time, bi-directional indicator sharing platform which makes indicators available in the industry standard STIX/TAXII format at no cost to SLTTs and which can be integrated into local security operations. This platform is unique among the industry as it is tailored specifically for SLTTs.

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.

"They scheduled a phone call within hours of my initial email—it was great! We're all understaffed, so it's invaluable to have help available during a crisis. A free service is even better, since purchase approval can take a while. I am so thankful to have MS-ISAC in my corner."

MS-ISAC Member

Malicious Domain Blocking and Reporting (MDBR)

The Malicious Domain Blocking and Reporting (MDBR) service is available for U.S. State, Local, Tribal, and Territorial (SLTT) government members of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) and Akamai. This service provides an additional layer of cybersecurity protection that is proven, effective, and easy to deploy.

About MDBR

MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

REGISTER FOR MDBR

To register for MDBR, please visit https://mdbr.cisecurity.org/

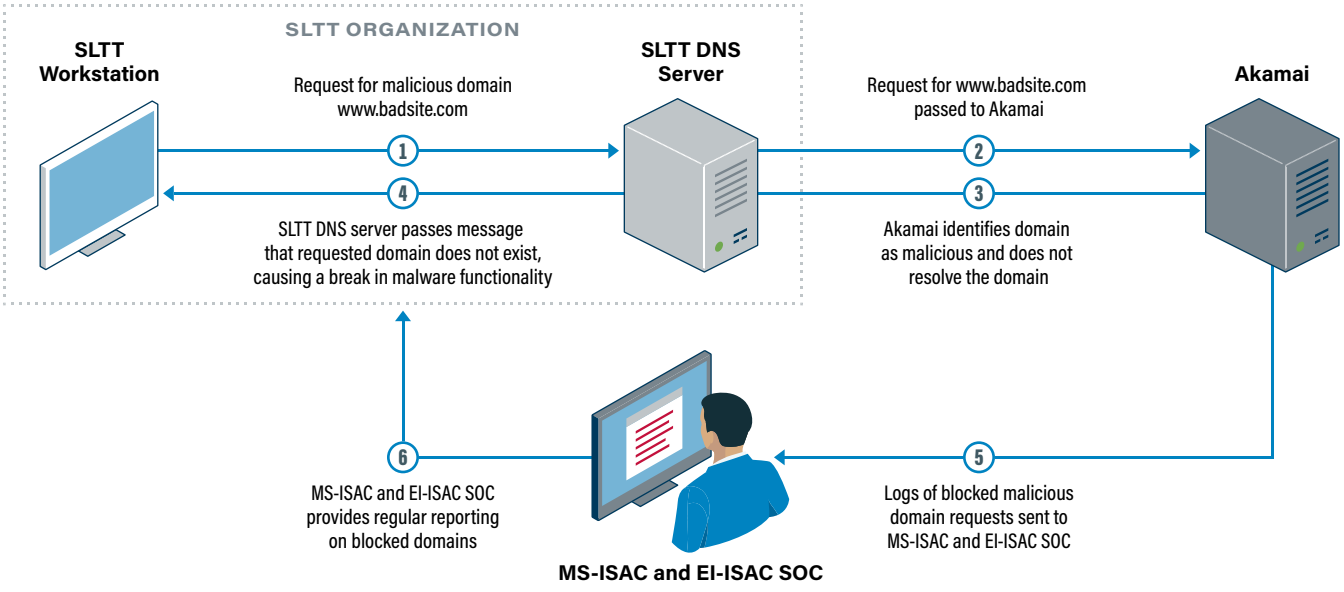
How MDBR Works

MDBR proactively blocks network traffic from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats. Once an organization points its domain name system (DNS) requests to the Akamai's DNS server IP addresses, every DNS lookup will be compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, will be blocked and logged. CIS will then provide reporting that includes log information for all blocked requests and assist in remediation if needed.

The service is easy to implement and requires virtually no maintenance as CIS and Akamai fully maintain the systems required to provide the service.

Akamai provides all logged data to the CIS SOC, including both successful and blocked DNS requests. This data will be utilized to perform detailed analysis and reporting for the betterment of the SLTT community and for organization-specific reporting for each SLTT organization that implements the service. CIS will provide regular reporting and intelligence services for SLTT members.

↓ Malicious Domain Blocking and Reporting Data Flow



Malicious Code Analysis Platform

The Malicious Code Analysis Platform (MCAP) is a web-based service that enables members to submit suspicious files, including executables, DLLs, documents, quarantine files, and archives for analysis in a controlled and non-public fashion. Additionally, the platform enables users to perform threat analysis based on domain, IP address, URL, hashes, and various Indicators Of Compromise (IOCs).

This platform allows users to obtain the results from analysis, behavioral characteristics, and additional detailed information that enables them to remediate the incident in a timely manner. This communication with our members provides the MS-ISAC with the situational awareness needed to assess the malware threat characteristics facing our SLTT government entities on a national level.

MCAP REGISTRATION

The Malicious Code Analysis Platform is available to all members free of charge. To register for an account, send an email to mcap@cisecurity.org using the following format:

SUBJECT LINE:
"MCAP Account Request"

BODY OF THE EMAIL:
First and last name, name of government entity, email address.

"We so appreciate all that you have done to help! I can't tell you how much it helped to know that you were with us through this (incident)."

MS-ISAC Member

Cyber Threat Intelligence and Analytical Products

Cybersecurity Advisories

Short and timely emails containing technical information regarding vulnerabilities in software and hardware.

Cyber Alert

Short and timely emails containing information on a specific cyber incident or threat.

White Paper

Detailed technical papers providing key information about a topic of interest.

Situational Awareness Report (SAR)

Highlights of the MS-ISAC's previous month's activities and statistics related to incident response, network monitoring, and general information gathering.

Short-form Analytic Report (SFAR)

Concise, easily digestible 1-2 page threat intelligence assessments with substantiation and analytic confidence clearly articulated.

Long-form Analytic Report (LFAR)

Lengthier, more in-depth threat intelligence reports with multiple assessments and confidence clearly articulated throughout.

Weekly and Monthly IOCs

Reports highlighting malicious IPs and domains the MS-ISAC has identified through monitoring during the past week or month.

Study

Strategic or operational view of a specific actor, group, campaign, malware family, nation state, or other collective target set of data. Studies take a longer view than other products, and while they may contain technical information, they are used primarily to support strategic conclusions, driving decision-making at higher levels, such as policy changes at the State and Federal level.

CIS SecureSuite Membership

CIS SecureSuite Membership provides integrated cybersecurity tools and resources to organizations of every size.

CIS SecureSuite Membership is FREE for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

For more information or to register, please contact freesecuresuite@cisecurity.org.

Maintaining secure configurations are a complicated and time-consuming activity. Even if system configurations were secure to start with, the once-hardened IT environments will drift over time. You can effectively monitor your configurations, quickly identify vulnerabilities, and prevent configuration drift with CIS-CAT Pro. Your team can automate configuration assessments, conduct remote scans, implement security best practices, and more. CIS SecureSuite Membership is available at no cost to U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

CIS-CAT® Pro

CIS-CAT Pro combines the powerful security guidance of the CIS Controls and CIS Benchmarks into an assessment tool. Leveraging the CIS-CAT Pro Assessor and Dashboard components, users can view conformance to best practices and improve compliance scores over time.

- Select CIS Benchmarks annotated with CIS Controls mappings
- Semi-automated assessment of CIS Controls V7.1 Implementation Group 1 on Windows 10 and Windows Server with CIS Controls Assessment Module
- Multiple reporting formats (Microsoft Excel, HTML, etc.) with easy-to-view remediation steps for noncompliant settings
- Evidence-based reports which can be exported in various formats (HTML, XML, CSV, TXT)
- Remote assessment capability
- Vulnerability scanning functionality

CIS-CAT Pro Assessor works on-prem or in the cloud to scan target system configuration settings and reports compliance with corresponding CIS Benchmarks. Scans are typically completed in just a few minutes, saving users hours of tedious manual configuration review.

CIS-CAT Pro Dashboard consumes assessment reports and shows system compliance over time.

- CIS Controls view for annotated CIS Benchmark content
- View assessment results per-Benchmark or per-device
- Custom device tagging (PCI, admin, etc.) to view compliance for a group of systems
- Create exceptions to CIS Benchmark content and dynamically recalculate assessment scoring
- Alert notifications and difference reports for configuration drift between scans

CIS CSAT Pro

CIS CSAT Pro is an on-premises CIS Controls self-assessment tool that allows organizations to conduct, track, and assess their implementation of the CIS Controls.

- Collaborate across teams and assign user roles
- Choose which specific Sub-Controls to include
- Upload documentation as supporting evidence
- Track assessment over time
- Monitor alignment to other security frameworks
- Anonymously compare results to an industry average or other peer groups

CIS WorkBench

CIS WorkBench is a community platform where Members can collaborate and access resources.

https://workbench.cisecurity.org/

- Easily tailor CIS Benchmarks recommendations to fit organizational or compliance policies
- Export CIS Benchmarks in various formats (Microsoft Word, Microsoft Excel, XCCDF, OVAL, XML)
- CIS Build Kits (GPOs, Linux scripts, and more) for rapidly implementing CIS Benchmark recommendations

MS-ISAC Member Initiatives and Collaborative Resources

MS-ISAC membership enables entities to participate with their peers across the country, sharing knowledge, building relationships, and improving cybersecurity readiness and response.

Emergency Conference Calls

Members have access to conference calls to brief all members on major incidents or emerging events.

Monthly Member Threat Briefing

One-hour webcast briefings that provide members with updates on the threat landscape, status of national initiatives impacting them, and relevant news from members. DHS has a standing agenda item on each call.

Cyber Threat Briefings

The MS-ISAC provides cyber threat briefings to our members based on our expertise of the cyber threat landscape and incidents targeting SLTT governments.

Workgroups

Focused working committees to share ideas, generate recommendations, and produce deliverables to support the MS-ISAC and member-related programs (see page 8).

Members-Only Access to HSIN

The MS-ISAC has a Community of Interest (COI) on the Homeland Security Information Network (HSIN) which allows our membership a secure and confidential platform for sharing information. The COI includes the MS-ISAC cyber alert level map—a visual representation of the current cyber status of each state, updated on a monthly basis; and a library of policies, reports, guides, recorded webcasts, sector specific discussion groups, and many additional member resources.

REQUEST A SUBJECT MATTER EXPERT

MS-ISAC can provide subject matter experts for presentations and conferences.

Please reach out to info@cisecurity.org with your requests.

"It was very helpful to have the MS-ISAC to turn to at this difficult time. The MS-ISAC team was extremely helpful during every step of the project."

MS-ISAC Member

MS-ISAC Workgroups

Workgroups are voluntary committees focused on specific initiatives and deliverables in support of the MS-ISAC mission.

Who can participate in a Workgroup?

Any member from any state, local, tribal, or territorial government.

What do the Workgroups do?

They serve a significant role in the creation and implementation of MS-ISAC initiatives. These Workgroups are also a tremendous opportunity to collaborate with your peers across the country. They identify current issues facing SLTT governments and help determine the future course of addressing cybersecurity challenges. They have been responsible for:

- Authoring the Nationwide Cybersecurity Review (NCSR) question set and analyzing the results
- Participating in the development and execution of cybersecurity tabletop exercises
- Increasing participation in National Cybersecurity Awareness Month activities
- Authoring the monthly newsletter and other publications

How much time will I need to commit?

- Level of commitment varies by group
- Extent of involvement is completely your choice

Current Workgroups

Business Resiliency

Focuses on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations, and communications.

Cybersecurity Metrics

Focuses on recommending and implementing methodologies to help SLTT entities with cybersecurity metrics and compliance inventory, assessment, and audit of their cybersecurity assets. This workgroup works jointly with DHS, National Association of State Chief Information Officers (NASCIO) and the National Association of Counties (NACo) to support the DHS Nationwide Cybersecurity Review.

K-12

Brings together a diverse group of educational agencies, in hopes of better understanding the issues, challenges and concerns of school districts throughout the country. The Workgroup strives to meet those needs and improve the overall cybersecurity posture of the community to support the overall mission of the MS-ISAC.

Education and Awareness

Focuses on implementing innovative strategies, improving existing programs, and promoting successful localized initiatives for national cybersecurity education, awareness, and training content to support the overall mission of the MS-ISAC.

HOW DO I JOIN A WORKGROUP?

Send an email to info@cisecurity.org with "Workgroup Request" in the subject line, and include the following:

- **Name**
- **Workgroup of interest**
- **Entity/Agency name**
- **Email and telephone number**

Share your expertise by joining a Workgroup today!

"I can honestly say that your organization has made an immediate impact in our overall security readiness. Thank you."

MS-ISAC Member

Nationwide Cybersecurity Review

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment designed to evaluate cybersecurity maturity. The Senate Appropriations Committee has requested an ongoing effort to chart nationwide progress in cybersecurity and identify emerging areas of concern. In response, DHS has partnered with the MS-ISAC, NASCIO, and NACo to develop and conduct the NCSR.

Who can participate?

All states (and agencies), local governments (and departments), and tribal and territorial governments.

How does the NCSR work?

- Hosted on a secure portal
- Based on the NIST Cybersecurity Framework
- Based on key milestone activities for information risk management
- Closely aligned with security governance processes and maturity indexes embodied in accepted standards and best practices
- Covers the core components of cybersecurity and privacy programs

When does the survey take place?

The survey will be available from October to December each year. For more information and to register, visit cisecurity.org/ms-isac/services/ncsr/.

Advantages of participation

- Access to NIST, COBIT, ISO and CIS Controls informative references
- Free and voluntary self-assessment to evaluate your cybersecurity posture
- Customized reports to help you understand your cybersecurity maturity, including:
  - A detailed report of your responses along with recommendations to improve your organization's cybersecurity posture
  - Additional summary reports that gauge your cybersecurity measures against peers (using anonymized data)
  - Insight to help prioritize your effort to develop security controls
- Benchmarks to gauge your own year-to-year progress
- Metrics to assist in cybersecurity investment justifications
- Contribute to the nation's cyber risk assessment process

The Survey

The NCSR provides survey participants with instructions and guidance. Additional support is available, including supplemental documentation at the link listed below and the ability to contact the NCSR help desk.

Once the NSCR is complete, participants will have immediate access to an individualized report measuring the level of adoption of security controls within their organization. This report includes recommendations on how to raise your organization's risk awareness.

The MS-ISAC and DHS will review all aggregate data and share a high-level summary with all participants. The names of participants and their organizations will not be identified in this report. This report is provided to Congress in alternate years to highlight cybersecurity gaps and capabilities among our state, local, territorial and tribal governments.

DID YOU KNOW?

State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grant recipients are now required to complete the NCSR. These grants include funds that can be used to enhance the cybersecurity maturity of organizations. Learn more at www.fema.gov/grants/preparedness/homeland-security.

Cybersecurity Education

The MS-ISAC produces numerous communications to engage our members and help national efforts for better cybersecurity.

Education and Awareness Materials

Monthly Newsletters: These newsletters use non-technical language, and they can be rebranded to suit individual member needs. Newsletter topics include details on the most current threats and suggested best cybersecurity practices.

Monthly Webinars: These feature timely topics and experts from the public and private sector sharing insight on addressing cyber challenges and are open to the public.

Cybersecurity Awareness Toolkit

The Cybersecurity Awareness Toolkit features educational materials designed to raise cybersecurity awareness. Digital materials are aggregated for your use.

FedVTE

The Federal Virtual Training Environment (FedVTE) is DHS' online, on-demand training center. FedVTE provides SLTT IT professionals with hands-on labs and training courses. https://fedvte.usalearning.gov/

Best of the Web Contest

The MS-ISAC conducts an annual Best of the Web contest to recognize SLTTs to be inclusive of tribes, education, etc., who use their websites to promote cybersecurity. We review the cybersecurity websites for all 50 state governments and the many local governments that decide to participate. The judging is based upon several criteria including cybersecurity content, usability, accessibility, and appearance.

The contest recognizes outstanding websites and highlights them as examples for others to consider when they are developing or redesigning their own sites.

The Best of the Web contest kicks off in the beginning of October, which is National Cybersecurity Awareness Month. The winners are announced on the November ISAC Monthly Membership Call.

Poster Contest

The MS-ISAC conducts an annual Kids Safe Online poster contest to encourage young people to use the internet safely. The contest encourages young people to create cybersecurity messages other kids will appreciate and apply to their own lives.

The contest is open to all public, private, or home-schooled students in kindergarten through twelfth grade. Winning entries of the MS-ISAC Kids Safe Online poster contest are what make up the next year's MS-ISAC Cybersecurity Awareness Toolkit, which is shared digitally with MS-ISAC members.

The MS-ISAC Kids Safe Online poster contest is launched at the beginning of National Cybersecurity Awareness Month, and submissions are due the following January.

FOR MORE INFORMATION

For questions regarding education and awareness materials or participation in any of these programs, please contact info@cisecurity.org.

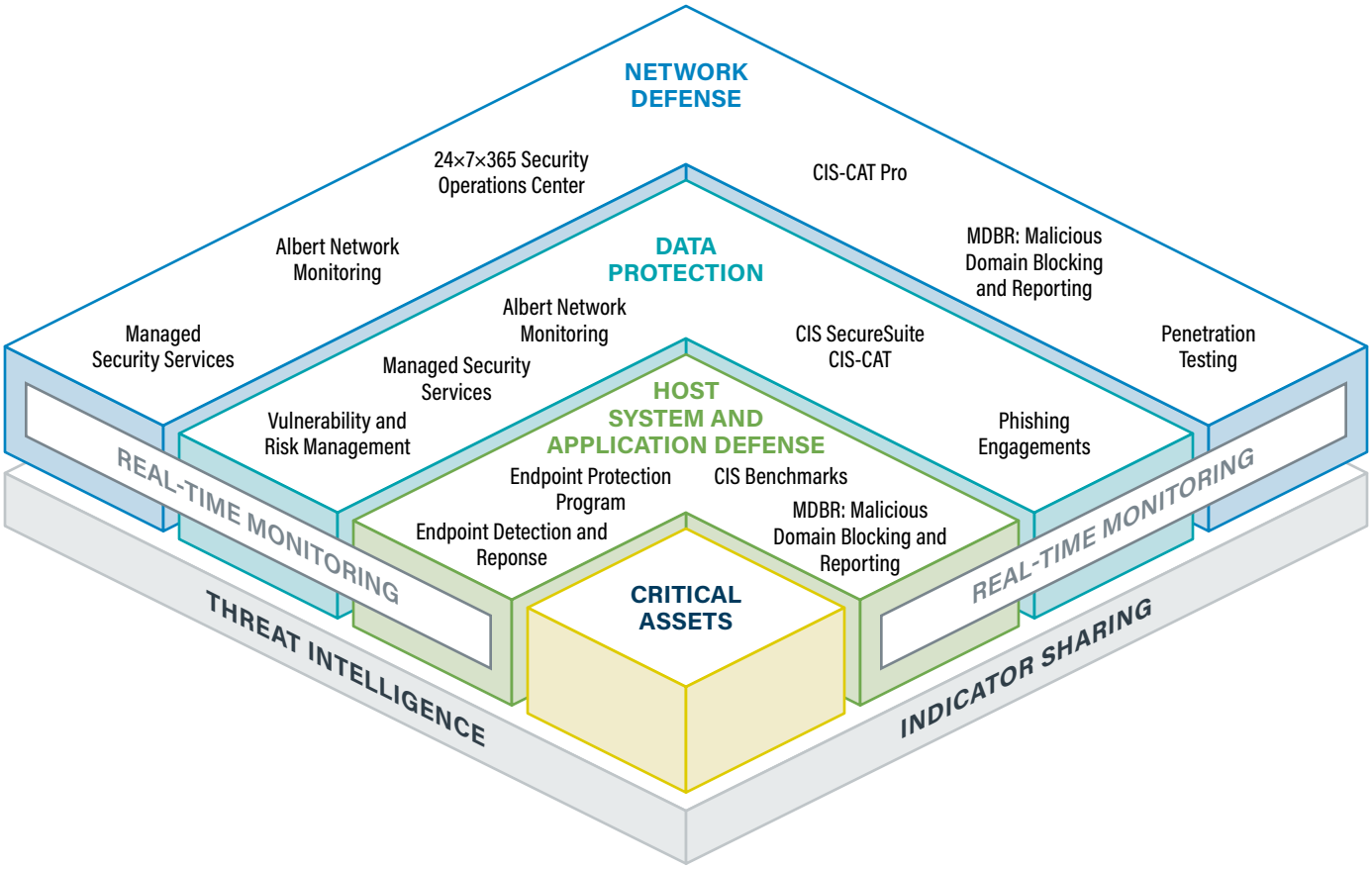
For more information on DHS services, visit www.cisa.gov.

Fee-based Services

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.

CIS has architected security solutions with the critical nature of defense-in-depth in mind. U.S. SLTT government organizations can deploy a defense-in-depth strategy to significantly improve their cybersecurity posture with these services offered by CIS, the MS-ISAC, and the EI-ISAC.

The CIS Defense-in-depth Model ↓



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 cyber-attack. At the conclusion of testing, the findings are delivered in a detailed report, with prioritized remediation recommendations.

Managed Security Services

The CIS 24x7x365 SOC provides SLTT entities cost-effective log and security event monitoring of existing devices including, but not limited to, IDS/IPS, firewalls, switches and routers, servers, endpoints, and web proxies. Actionable items are escalated to organizations as an alert and our 24×7×365 SOC is always on hand to answer questions regarding alerts or notifications received.

CIS CyberMarket®

The CIS CyberMarket assists SLTT governments and nonprofit entities in achieving a greater cybersecurity posture through trusted expert guidance and cost-effective procurement. The CIS CyberMarket builds public and private partnerships and works to enhance collaboration that improves the nation's cybersecurity posture. The CIS CyberMarket makes cybersecurity purchasing effective, easy, and economical. Discounts include:

- Training
- Software
- Consulting Services

FOR MORE INFORMATION

If you would like more information about these services or a quote, please contact CIS at services@cisecurity.org.

"The assistance from the MS-ISAC during a very stressful time has been much appreciated. It's comforting to know that we have your skills, knowledge, and expertise ready to assist."

MS-ISAC Member

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. This service is committed to building and maintaining the most comprehensive set of detection rules and signatures in order to quickly and accurately identify threats impacting SLTT entities.

Turnkey solution incorporating 24x7x365 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.

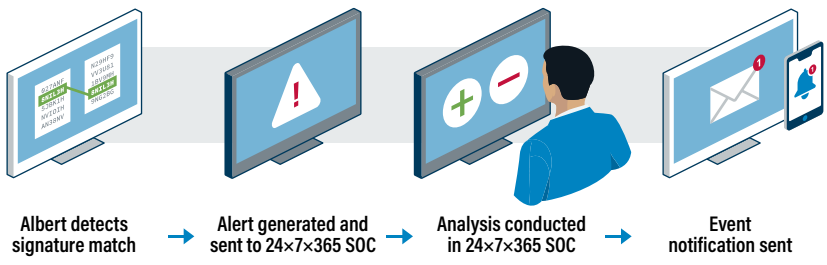
"Within 2 seconds of the script being launched, the computer was automatically isolated from the network. I had set a rule so any critical items like this would cause the PC to be isolated. We received the initial MS-ISAC email at 11:29, 1 minute after script launch. I would say our protection systems worked as well as we could hope."

City Member

Why is the Albert Service Unique?

- Government-specific focus and tailored to SLTT governments' cybersecurity needs.
- Experienced cybersecurity analysts review each cybersecurity event, which results in minimizing the number of false-positive notifications. This system allows first responders to focus on actionable events.
- Correlation of data from multiple public and private partners:
  - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
  - When a major new threat is identified, the MS-ISAC will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT governments cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTT governments, including nation-state attacks.
- MS-ISAC staff are deployed at the CISA Central in Arlington, VA. This liaison relationship facilitates valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Availability of a CIRT for forensic and malware analysis which is part of the no-cost MS-ISAC membership.
- Cost-effective solution that is significantly less expensive than the purchase and maintenance of a typical commercial IDS solution.

↓ **Albert notification cycle**



Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity