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

Services Guide

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

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's State, Local, Tribal, and Territorial governments.

Table of Contents

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

Overview

What We Offer

- The MS-ISAC provides **real-time** network monitoring, threat analysis, and early warning notifications through our 24x7 Security Operations Center (SOC).
- The U.S. Department of Homeland Security (DHS) has designated the MS-ISAC as its **key cybersecurity resource** for State, Local, Tribal, and Territorial governments, including Chief Information Security Officers (CISOs), Homeland Security Advisors and Fusion Centers.
- 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 cybersecurity 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

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

Membership Overview

The Multi-State Information Sharing and Analysis Center (MS-ISAC), is part of the nonprofit Center for Internet Security (CIS). The MS-ISAC is a voluntary community focused on improving cybersecurity for State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC started in 2004. Since then we have built and nurtured an environment of collaboration and information sharing. The U.S. Department of Homeland Security (DHS) has designated the MS-ISAC as its key cybersecurity resource for State, Local Tribal and Territorial governments, including Chief Information Security Officers, Homeland Security Advisors and Fusion Centers.

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

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; and
- 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.

> ***"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*

> ***"I can honestly say that your organization has made an immediate impact in our overall security readiness. Thank you."***
>
> *— MS-ISAC Member*

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

The MS-ISAC Security Operations Center

What is the MS-ISAC SOC?

The MS-ISAC operates a Security Operations Center (SOC), which is a 24x7 joint security operations and analytical unit that monitors, analyzes and responds to cyber incidents targeting U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

Core Services of the MS-ISAC SOC:

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

The MS-ISAC Core Services:

- **Cyber Vulnerability & 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.
- **Cybersecurity Exercises:** The MS-ISAC participates in federally sponsored cybersecurity exercises and acts as a voice for SLTT governments in planning meetings.
- **Monitoring Services:** The MS-ISAC provides network monitoring services for SLTT government entities. (See pages 7 & 15)
- **Anomali:** Anomali is the MS-ISAC's STIX/TAXII offering that includes two tools for analyzing and sharing indicators, STAXX and Threatstream. STAXX is a free tool that can subscribe to and publish STIX/TAXII feeds. MS-ISAC members also receive access to Anomali Threatstream, which is an advanced platform for threat information sharing, research and analysis.
- **CIS SecureSuite® Membership:** CIS SecureSuite leverages the CIS Benchmarks™ and the CIS Controls with a host of cybersecurity tools and services to automate configuration assessment and provide enhanced insight for organizations of all sizes to improve their cybersecurity posture. CIS SecureSuite Membership is available at no cost to SLTTs.

CIS SecureSuite® Membership

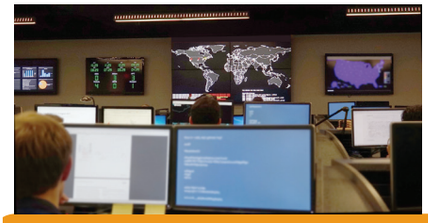
- **Fee Based Services**: The MS-ISAC offers a variety of fee based services for SLTT government entities to take advantage of. (See pages 15-16)

Additional Services Include:

The **Computer Emergency Response Team (CERT)** provides SLTT governments with malware analysis, computer and network forensics, malicious code analysis/mitigation, and incident response.

The **Intelligence Analysis Team (Intel)** makes informed assessments about cyber trends, actors, tactics, techniques, and procedures (TTPs).

The **National Liaison Team** is assigned to the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, VA. The NCCIC is a 24x7 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.



"We appreciated the time the MS-ISAC CERT provided to us to validate our findings and provide valuable insight on opportunities for future improvement. The states are very blessed to have access to the talents of the MS-ISAC CERT in times of crisis."

— 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 incident you are reporting requires direct assistance, the Computer Emergency Response Team (CERT), a unit comprised of highly trained and experienced staff, is able to assist you with a cybersecurity incident at no cost.

Our incident response experts can assist with the following:

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

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

— MS-ISAC Member

"Thank you for providing this invaluable service!"

— MS-ISAC Member

To report an incident, please contact the MS-ISAC SOC for 24x7 assistance:

Phone: **1.866.787.4722**

Email: **soc@msisac.org**

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

Network Security Monitoring and Analysis Services (Albert)

The MS-ISAC offers a fully managed network monitoring service known as Albert. The Albert service consists of an Intrusion Detection System (IDS) sensor placed on an organization's network—typically inside the perimeter firewall, monitoring an organization's Internet connection—that collects network data and sends it to the MS-ISAC for analysis. Based on the MS-ISAC's vast repository of indicators of compromise, we are able to identify malicious activity and alert the affected organization.

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.

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 NCCIC in Arlington, VA. This liaison relationship facilitates valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Availability of a CERT 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.

Vulnerability Management Program

The Vulnerability Management Program (VMP) alerts our membership on a monthly basis regarding out-of-date and vulnerable software. A scripted request is sent to each of the thousands of SLTT domains we are aware of to pull data on versioning information related to each domain. The VMP staff will then notify domain owners when out-of-date software is identified.

What Data Are We Collecting?

- Server type and version (IIS, Apache, nginx, etc.)
- Web programming language and version (PHP, Python, Perl)
- Content Management System and version (WordPress, Drupal, etc.)
- Other web server software and version (OpenSSL)

VMP

Following the analysis and review of the information returned, a notification is sent to the affected entity with a spreadsheet attached. The spreadsheet contains two tabs: "Domains" and "Software." All the domains that have been profiled are included in the "Domains" tab. If one or more software versions were identified, the "Software" tab will contain the related software, version, status, and CVE number as a link and CVSS score as a color-coded severity.

In addition to domain profiling, the MS-ISAC also performs IP address port profiling. The MS-ISAC Port Profiling Tool connects to SLTT public IP addresses provided by our MS-ISAC members. Each IP address profiled receives a small number of packets on a selection of commonly used ports. The data obtained during this process is the same information that could be collected by anyone on the public Internet and is often used by attackers for reconnaissance purposes prior to an attack. Our intent is for members to utilize this information as a reminder to keep Internet facing systems up-to-date and securely configured. These notifications are sent on a monthly basis and contain the following information:

- Profiled IP Address
- Profiled Port Number
- Service Running on the Port
- Reverse DNS record
- Banner of the host

If possible, we also collect information related to:
Software type and version (OpenSSH, Cisco, IIS, etc.) Publically available hardware (ICS and SCADA devices, printers, cameras, routers, switches, etc.)

We also highlight certain open ports within the report that we feel should be more closely reviewed, as they may pose a significant threat to the organization.

Members should use these monthly notifications to conduct further analysis in order to ensure that Internet facing systems are fully patched, running the most up-to-date software and are securely configured in order to limit the possibility of a successful attack.

? For questions regarding the domains or IP addresses that the MS-ISAC has on file for your organization, please contact info@msisac.org.

Domain and IP listings can be edited at any point in time during your membership.

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

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 (IOC's).

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

This platform is available to all members free of charge. To register for an account, send an email to mcap@msisac.org using he following format:

- Subject Line:
  "MCAP - Account Request"
- Body for the Email:
  First and last name,
  name of government entity,
  email address.

Cyber Threat Intelligence & Analytical Products

- **Cybersecurity Advisories:** Cybersecurity Advisories are short and timely emails containing technical information regarding newly discovered vulnerabilities in software and hardware.
- **Cyber Alerts:** Cyber Alerts are short and timely emails containing information on a specific cyber incident or threat.
- **Cyber Intel Advisories:** Cyber Intel Advisories provide detailed information and warning notices with limited analysis. Recipients are invited to attach their own branding (seal, logo, or shield) and republish the document as a jointly branded paper.
- **Desk References:** Desk references provide in-depth information and intelligence analysis on specific topics, such as active hacktivist groups and the most common malware, frauds and scams.
- **Intel Bytes:** Intel Bytes are brief analytical summaries on timely local or world events or significant threats.
- **Intel Papers:** Intel Papers provide in-depth analysis and detailed information regarding the background, history, tools, techniques, and/or procedures on a particular topic.
- **Joint Papers:** The MS-ISAC coordinates with federal and SLTT governments, fusion centers and other agencies to produce joint analytical papers on a variety of topics.
- **HSA Cyber Monthly Update:** A newsletter produced for the National Governors Association Governors' Homeland Security Advisory Council that summarizes and provides analysis on recent news articles. Members may attach their own branding and redistribute the newsletter as a jointly branded paper.
- **Security Primers:** Security Primers are a one-page summary that recommend the best response to a specific scenario. The Primers increase security awareness and encourage secure behavior.
- **Situational Awareness Report (SAR):** This highlights the MS-ISAC's previous month's activities and statistics related to incident response, network monitoring and general information gathering.
- **White Papers:** White Papers are detailed technical papers providing key information about a topic of interest.
- **Weekly Attacking IPs and Domains:** Weekly reports are provided highlighting malicious IPs and domains the MS-ISAC has identified through monitoring during the past seven days.

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

MS-ISAC Member Initiatives & 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.

CIS SecureSuite® Membership

- **CIS SecureSuite Membership:** CIS SecureSuite leverages the CIS Benchmarks and the CIS Controls with a host of cybersecurity tools and services to automate configuration assessment and provide enhanced insight for organizations of all sizes to improve their cybersecurity posture. CIS SecureSuite Membership is available at no cost to SLTTs.
- **Annual In-Person Meeting:** Each year, the MS-ISAC hosts an annual multi-day event bringing all members together, along with the federal government and other partners. We focus on action-oriented deliverables that are most important to the members. The meeting is open to all MS-ISAC members interested in attending. There is no registration fee for this event.
- **Emergency Conference Calls:** Members have access to conference calls to brief all members on major incidents or emerging events.
- **ESP Tool:** The CIS Enumeration and Scanning Program (CIS-ESP) is an application built to be deployed in an enterprise Windows environment to assist in the collection of data to determine if a compromise has occurred. The information collected enhances understanding the scope of an incident and identifies active host-based threats on a computer network. The application works by enumerating and polling systems within an Active Directory environment by way of Windows Management Instruction (WMI) queries. This process is used entirely for data collection and no modifications are made to the systems being scanned.
- **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 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.
- **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 pages 11-12)
- **Membership Discounts**
  - **CIS CyberMarket:** The CIS CyberMarket works with organizations in the public and private sectors to provide cost-effective, high-quality cybersecurity solutions for our nation's SLTT governments and non-profit entities at a discount.

CIS CyberMarket

"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

These 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 (SLTT) 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 Cyber Security Review (NCSR) question set and analyzing the results;
- participating in the development and execution of cybersecurity exercises;
- increasing participation in National Cyber Security Awareness Month activities; and
- creating important membership materials such as the MS-ISAC Cybersecurity Awareness Toolkit.

National Cyber Security Awareness Month

How much time will I need to commit?

- Level of commitment varies by group.
- Groups generally meet by phone monthly and in person annually.
- Extent of involvement is completely your choice.

How do I join a workgroup?
Send an email to info@msisac.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!

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

MS-ISAC Workgroups

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 Cyber Security Review.

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.

Intel and Analysis
Focuses on promoting the development, understanding, and awareness of actionable intelligence and analysis.

Mentoring Program
Focuses on pairing new security leaders in management positions (such as Chief Information Security Officers and Chief Security Officers) with more experienced security leaders to enhance their skill sets and foster personal and professional growth.

Application Security
Focuses on connecting individuals with an interest in application security to create guides and resources to assist the greater MS-ISAC membership tackle this challenging topic.

Nationwide Cyber Security Review

The Nationwide Cyber Security Review (NCSR) is a voluntary self-assessment survey to evaluate cybersecurity management. 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.

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); and
  - 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; and
- Contribute to the nation's cyber risk assessment process.

How does the Nationwide Cyber Security Review 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.

Survey
The NCSR provides survey participants with instructions and guidance. Additional support is available, including supplemental documentation and the ability to contact the NCSR help desk directly from the survey. 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.

When does the survey take place?
The survey will be available from October to December each year.
For more information and to register, visit:
http://msisac.cisecurity.org/resources/ncsr

"The NCSR provides a unique perspective on your security maturity as a snapshot of your program against the NIST Cybersecurity Framework. It provides valuable insights in measuring your security program while giving you annual comparatives of growth and peer-to-peer analysis! Well worth over $60K to any organization in helping to roadmap your security operation!"

— Gary Coverdale, CISO-Mono County

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

Cybersecurity Education

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

Education and Awareness Materials

- **Daily Cyber Tips:** Available to our members via RSS feeds.
- **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.
- **Bi-Monthly National Webcasts:** 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 and hard copy materials are available to our members to order. Members are encouraged to brand these materials for their own organizations.

Best of the Web Contest

The MS-ISAC conducts an annual Best of the Web contest to recognize state and local governments 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.

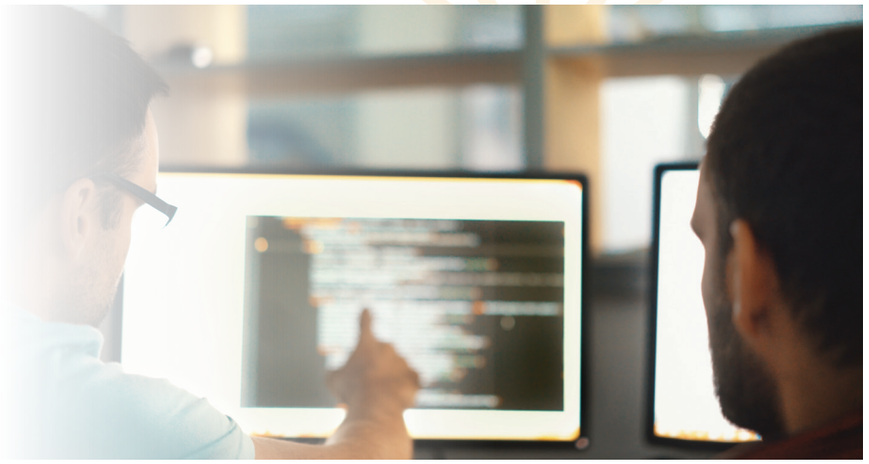
The Best of the Web Contest kicks off in the beginning of October, which is National Cyber Security Awareness Month. The winners are announced at the end of the month.

Poster Contest
The MS-ISAC conducts an annual National K-12 Computer Safety 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 National Poster Contest are what make up the next year's MS-ISAC Calendar, which is distributed to MS-ISAC members as part of the cybersecurity toolkit.

The MS-ISAC Poster Contest is launched at the beginning of National Cyber Security Awareness Month, and submissions are due the following January.

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.



For questions regarding education and awareness materials or participation in any of the items listed above, please contact info@msisac.org.

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

Fee Based Services for SLTT Entities

Network Security Monitoring and Analysis Service (Albert)
is a near real-time, fully managed, 24x7 network monitoring and analysis service that identifies and alerts on traditional and advanced threats within an enterprise network. Pricing is based on Average Internet Utilization.

In addition to the Albert monitoring service, we also have the ability to monitor traditional network security devices such as firewalls, IDS/IPS, web proxies, and host based intrusion detection devices. This monitoring is accomplished with our Managed Security Services (MSS) offering in partnership with a third party provider. All events generated by the MSS are evaluated by our SOC analysts and escalated to the affected entity.

Managed Security Services (MSS) are comprised of monitoring and/or management of security devices:

- Security Event Analysis & Notifications 24x7
- Monitoring and Management services are available for the following security devices:
  - Firewall monitoring
  - Host-based Intrusion Detection System monitoring
  - IDS/IPS monitoring and management
  - Proxy monitoring

Vulnerability Assessment Services: The MS-ISAC network and web application assessments can identify, prioritize and report critical vulnerabilities within your network and web application assessments.

- Network Vulnerability Assessment
- Web Application Assessment, including manual analysis of reported vulnerabilities to eliminate false positives.
- Prioritization of vulnerability remediation
- Customized reporting & vulnerability remediation support included
- Payment Card Industry (PCI) compliance scanning available
- Pricing for one time, monthly, or quarterly service is available

Consulting Services (Statement of Work Required):

Phishing Assessments

To help organizations assess their vulnerability to phishing attacks, MS-ISAC offers phishing assessments that are highly customizable to the organization. In a MS-ISAC phishing assessment, employees in the target organization will be delivered a specially-crafted email masquerading as an agreed-upon email sender.

Organizations can customize:

1. Email content
2. Phishing link or attachment
3. Landing page
4. Forms following the landing page to capture user credentials
5. Personalized email for each target user

Ex: "The password for <email> has expired. Please click here"

MS-ISAC phishing assessments demonstrate two primary areas of vulnerability:

1. The ability of an attacker to lure a target to a website that may host exploits, which could be used to compromise the target's workstation.
2. The ability for an attacker to rapidly collect sensitive user credentials that could be used to gain access to an organization's network.

Assessment Deliverables

After the phishing assessment, the MS-ISAC consultant will provide a detailed report containing the assessment results. The report will determine if the target organization is susceptible to phishing attacks and if it is likely that an attack would elicit the necessary end user interactions required for successful intrusion. The final report will also include the assessment's goals, theory, attack method, concluded results, statistics, campaign effectiveness and conclusions, and recommendations.

Network and Web Application Penetration Testing

The MS-ISAC offers both network and web application penetration testing services. These services simulate a real-world cyber attack, allowing organizations to safely review the security posture of their networking devices and web applications. Taking the vantage point of an attacker, our testing experts attempt to exploit external resources and gain access to internal resources that compromise the organization's infrastructure.

Methodology

Our penetration tests use an iterative, four-phased approach employing techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 100-115 Information

Security Testing and Assessment standard. This testing method includes activities to pinpoint vulnerabilities at each operational layer of the target network, aimed to identify critical weaknesses inherent to web applications, many of which are outlined in the OWASP Top 10 Web Application Vulnerabilities Project. Using a combination of automated tools and manual techniques, we thoroughly assess your organization's systems to identify exploitable vulnerabilities which could be used by cyber threat actors.

Deliverables

For each network and web application engagement, we deliver a written report detailing each vulnerability type discovered along with a risk rating of low, medium, or high. Reports include specific details for each vulnerability found including:

- how the vulnerability was discovered;
- the potential impact of its exploitation;
- recommendations for remediation;
- vulnerability references.

Fee Based Services for SLTT Entities

Consulting Services (Statement of Work Required):
continued —

Security Assessment
Organizations are under constant attack, targeted by well-funded criminals and nation-state actors. These groups use sophisticated attacks that often go undetected by many standard signature-based defense mechanisms. Because of this, organizations are often compromised for long periods of time, in some cases weeks, months, or even years, before being made aware that there is an issue. The goal of the compromise assessment phase is to identify any pre-existing compromises that may exist within the organization.

CIS-ESP
The CIS Enumeration and Scanning Program (CIS-ESP) is an application built to be deployed in an enterprise Windows environment to assist in the collection of data to determine if a compromise has occurred. The information collected enhances understanding the scope of an incident and identifies active host-based threats on a computer network. The application works by enumerating and polling systems within an Active Directory environment by way of Windows Management Instruction (WMI) queries. This process is used entirely for data collection and no modifications are made to the systems being scanned but is extremely valuable when conducting a security assessment.

Internal Systems Assessment
CIS-CAT: The CIS Configuration Assessment Tool (CIS-CAT) is a Java-based application that compares the configuration of target IT systems to CIS Benchmarks and reports back the level of compliance. Any indications of lack of compliance are potential areas to improve an organizations cyber security posture and will be included in the final report.

Network Perimeter Assessment / Infrastructure Architecture Review
The goal of the network perimeter assessment is to ensure the effectiveness of the layers of security in place to protect the organization's data, assets, and information residing on the network. This portion of the assessment will include a review of the following areas:

- **Firewall Configuration** – Will perform a review of the firewall rules in place as well as a review of the level of logging being performed by the firewall.
- **Remote Access Methods** – Will identify all systems that allow inbound remote access from outside the enterprise environment. Systems identified will be reviewed for the existence of appropriate security controls.
- **OS levels** – Review of perimeter systems to ensure that they are up-to-date with the latest patches and OS levels.
- **Wireless network configurations** – Review of wireless networking configuration to ensure adequate security measures are in place preventing unauthorized access to the network.
- **Review of administrative and other accounts** – This is a review of system accounts to limit the possibility of an account being used to facilitate a system compromise. Examples include ensuring administrative accounts have been renamed, default passwords have been changed, and guest accounts have been disabled.

CIS CyberMarket

Membership Discounts

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 questions regarding the CIS CyberMarket or any of the items listed above, please contact info@msisac.org.

31 Tech Valley Drive
East Greenbush, NY 12061
info@msisac.org
soc@msisac.org
518.266.3460