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

Welcome to the MS-ISAC!

To get started:

- Learn how to report an incident at any time to the MS-ISAC SOC
- Add additional staff members to your account
- Submit your public IP ranges and domain space for monitoring
- Create an account on the Malicious Code Analysis Platform (MCAP)
- Complete your registration for access to the secure portal

This guide provides details about each of the items listed above as well as additional MS-ISAC services.

24x7 Security Operations Center (SOC)

The MS-ISAC Security Operations Center provides real-time network monitoring, early cyber threat warnings and advisories, and vulnerability identification and mitigation.

24x7 Support

Reporting

Analysis & Monitoring

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

☎ Phone: **1.866.787.4722**

Email: **soc@msisac.org**

MS-ISAC Computer Emergency Response Team (CERT)

Members are encouraged to report incidents, even if they are not requesting direct assistance, to improve the situational awareness of the MS-ISAC membership.

The Computer Emergency Response Team is able to assist with cybersecurity incidents.

Our incident response experts can provide:

- Emergency Conference Calls
- Network & Web Application Vulnerability Assessments
- Free Access to Tools to Assess your Configuration
- Forensic Analysis , Malware Analysis & Log Analysis
- Reverse Engineering
- Mitigation Recommendations
- Cyber Threat Intelligence
- Verbal and written reports are provided following the reported incident

MS-ISAC Distribution List

Each organization may have an unlimited number of contacts added to the MS-ISAC distribution lists to receive communications directly.

The primary contact will receive full access (Level 4) and we encourage our members to add additional staff to their account. The primary contact should indicate what level of access each additional staff member should receive as outlined below.

4

Level 4
Level 1, Level 2 & Level 3 + Account on the MS-ISAC's section of a secure federal portal

3

Level 3
Level 1 & Level 2 + Organization specific notifications (Incident Notifications, Threat Information)

2

Level 2
Level 1 + MS-ISAC member publications (Weekly Malware IP and Domain Reports, Monthly Situational Awareness Report, Cyber Alerts, and Intel Papers)

1

Level 1
Public information only (Special Discount Buys, Cyber Advisories, Monthly Newsletters, and National Webcasts)

+

To add additional staff, simply send an email to your account manager or info@msisac.org with the information below.

Name:

Level of Access:

Email:

Phone Number:

Work Cell Phone Number (if applicable):

Title:

Physical Mailing Address (Non P.O. Box):

IP Range & Domain Space

The MS-ISAC SOC can monitor your public IP range and domain space as part of your membership. The MS-ISAC 24x7 SOC will notify your organization via phone or email regarding evidence of:

- **Web defacements**
- **System compromises**
- **Compromised user credentials**
- **IPs connected to a malicious command and control server**
- **Indicators of compromise from MS-ISAC network monitoring (Albert)**
- **IPs connected to sinkholes or honey nets**

Please submit your IP range and domain space to: soc@msisac.org. IPs are accepted in CIDR notation; wildcard domains are not allowed.

Vulnerability Management Program (VMP)

The Vulnerability Management Program is an MS-ISAC initiative that works off of the domains provided by your organization. The objective of this program is to alert MS-ISAC members on potential threats and vulnerabilities to and serve as a reminder to keep Internet facing systems patched and up to date.

What Data Are We Collecting?

- Server type & version (IIS, Apache, Nginx, etc.)
- Web Programming Language & version (PHP, ASP, etc.)
- Content Management System & version (WordPress, Joomla, Drupal, etc.)

VMP

Malicious Code Analysis Platform (MCAP)

The Malicious Code Analysis Platform (MCAP) is a web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion including:

- Executables
- Dll's
- Documents
- Quarantine Files
- Archives
- URLs

MCAP

This platform is available to all members at no cost. Access can be obtained by sending and email to mcap@cisecurity.org using the following format:

Subject Line: MCAP – Account Request

First Name:

Last Name:

Name of Organization:

Email Address:

Is your organization a recipient of suspicious emails?

MS-ISAC members can receive analysis of suspicious emails by forwarding or sending the emails as an attachment to suspiciousemail@cisecurity.org.