Multi-State Information Sharing & Analysis Center®

Join the MS-ISAC Today!

20 YEARS AS YOUR TRUSTED CYBER DEFENSE COMMUNITY

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

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

HOME FIELD ADVANTAGE:

How the MS-ISAC Can Help Strengthen K12 Cybersecurity

Michelle Nolan

Regional Engagement Manager

Michelle.Nolan@cisecurity.org

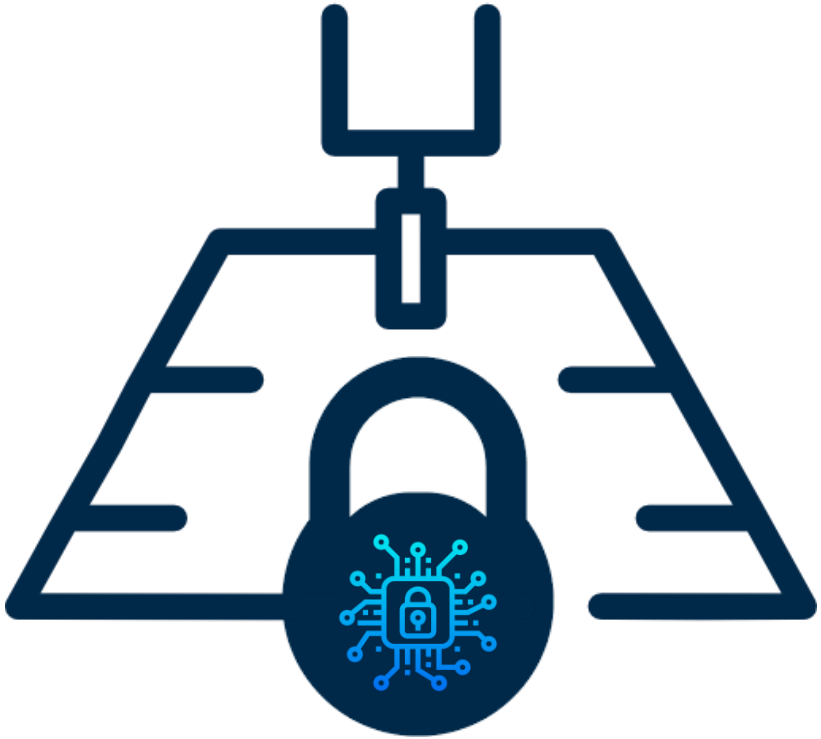
518-516-3030

Confidential & Proprietary

Homefield Advantage

How the MS-ISAC Can Help Strengthen K12 Cybersecurity

- ✓ Have the **RIGHT PLAYERS**
- ✓ A **SCOUTING REPORTS** is helpful
- ✓ Leverage a **PLAYBOOK**
- ✓ Tap into the **SPECIAL TEAMS**



Confidential & Proprietary

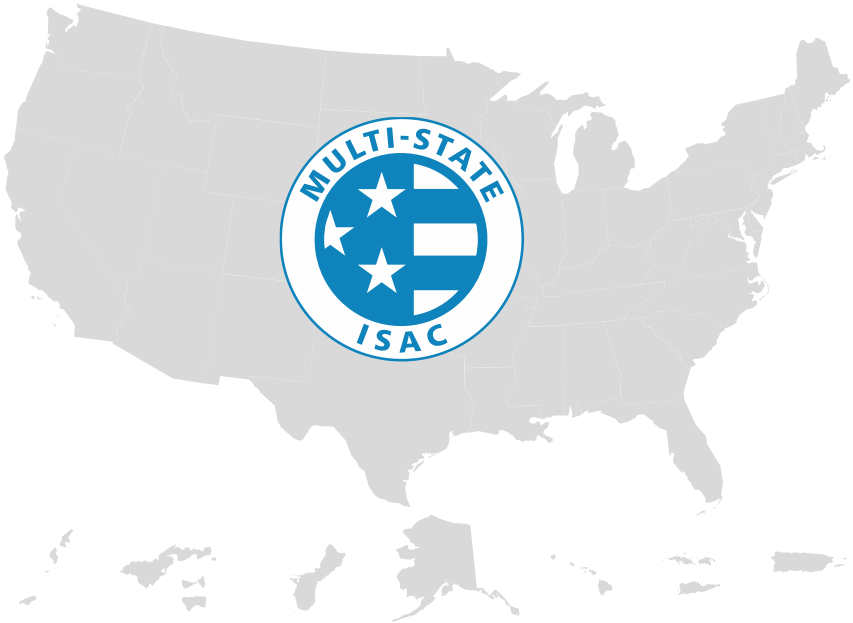
Multi-State Information Sharing & Analysis Center®

The MS-ISAC®

- Designated by the Cybersecurity & Infrastructure Security Agency (CISA) as a key resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.

- A division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit.

https://learn.cisecurity.org/ms-isac-registration



Confidential & Proprietary

Who We Serve…

State, Local, Tribal, and Territorial Governments

- 50 State Governments
- 14,000+ Local Governments
- 6 Territorial Governments
- 190 Tribal Governments
- 80 DHS-recognized Fusion Centers

MS-ISAC Members include

- 136 Total Montana Members
- 47 Montana K-12 School Districts
- 5 Montana Public Higher Education
- 4,200+ K12 Members Nationally

MS-ISAC: Focused Visibility on K12 Sector

Joint #StopRansomware Advisory and K12 Report

https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

https://www.cisecurity.org/ms-isac/k-12

K12 Landscape - A Look Back

K12 Cyber Attacks in the News

K-12 EDUCATION

[redacted] School District to Spend $10M on Ransomware Response

Following a ransomware attack March 12 that shut down systems and forced the cancellation of classes, [redacted] Public Schools is spending nearly $10 million on network security, fraud monitoring and other services.

October 18, 2021 • Stephen T. Watson, The Buffalo News, N.Y.

Content fr
1 Educ
2 Highe

Ransomware gang wanted $40 million in [redacted] schools cyberattack

By Lawrence Abrams

April 2, 2021 07:03 AM

K-12 EDUCATION

[redacted] Need 'Months' to Deal with Ransomware Attack

[redacted] School District in [redacted] will take months to investigate a ransomware incident last month that may have exposed private information from students and staff at the school before 2011.

November 02, 2021 • Valerie Myers, Erie Times-News, Erie, Penn.

Content fr
1 Educa
2 Highe
3 Highe

MISSOURI

Ransomware attack: Network outage forces [redacted] School District to virtual learning Thursday

Ransomware Impacts

Disruptions to K12 Learning Processes and Systems

Malware typically encrypts data and attacker holds the key for ransom

- Restricted access to networks and data
- Theft of sensitive student and staff information
- Disruption of critical systems
- Potentially significant monetary losses
- Canceled school days and delayed exams
- Assume that it’s not a matter of *if* you will be attacked, but *when* you will be attacked.

Preparation is key!

Trends for 2023

Threats Facing K12 Schools

Threats Facing K12 Schools:

- “K12s are likely to continue being a primary target for financially motivated threat actors.”
- “Ransomware groups are highly likely to remain the dominant threat with continued use of double and triple extortion tactics.”
- “Cyber insurance will become increasingly restrictive and inaccessible to resource-poor organizations like K12 schools.”

Cyber Threat Advisory

Alert Level

Guarded

Indicates a general risk of increased hacking, virus or other malicious activity

- Severe
- High
- Elevated
- Guarded
- Low

TJ Sayers, cyber threat intelligence manager at the Center for Internet Security (CIS)

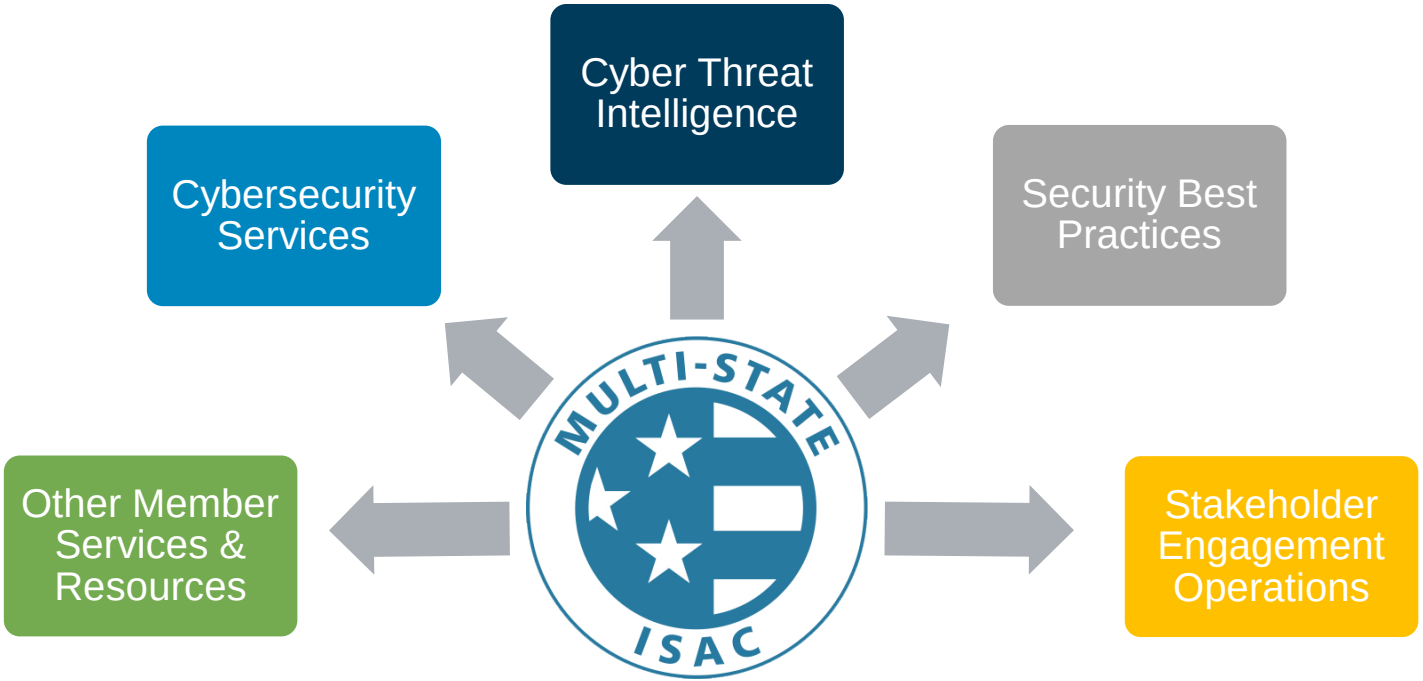
K-12 Community Assessment

Top Five Security Concerns

Lack of sufficient funding	**Budget** • The average K-12 school allocated 8% or less of their IT budget for cybersecurity • 18% of schools dedicated less than 1% of IT budget to cybersecurity
Increasing sophistication of threats	**Frequent Target of Cyber Threats** • 29% of K-12 member organizations* reported that they were victims of a cyber incident
Lack of documented processes	**Processes** • 37% of K-12 members* did not have an incident response plan
Lack of a cybersecurity strategy	**Cybersecurity Strategy** • 83%* had cyber insurance to mitigate their cyber risk • 81%* had not fully implemented multi-factor authentication (MFA) • 29%* had not implemented MFA on any systems
Inadequate availability of cybersecurity professionals	**Staffing** • 49% of K-12 schools had between one and five cyber/IT employees

Taking Burden off of K12s

Benefits of MS-ISAC Membership



Malicious Domain Blocking and Reporting (MDBR)

https://mdbr.cisecurity.org/

Security Focused DNS service:

Blocks malicious domain requests before a connection is even established!

Simple Implementation:

No new hardware or software required

Helps limit infections related to:

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

Confidential & Proprietary

Security Operations Center

24x7x365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Confidential & Proprietary

Recommended Action Plan

To Help Prevent and Defeat Cyber Attacks

K-12s face a persistent cybersecurity threat that demands an active defense. Take the following five actions to build an **Effective Cybersecurity Program**.

- **Build Your Cyber Community**
- **Conduct Cyber Assessments**
- **Grow Your Cyber Intelligence**
- **Leverage Network and Endpoint Defense Services**
- **Implement Best Practices**

Build Your Cyber Community

No-Cost MS-ISAC Benefits to K12s

Cyber Threat Intelligence

- Cyber Alerts & Advisories
- Quarterly Threat Report
- Regular IOCs
- White Papers
- Cyber Threat Briefings
- Real-Time Intelligence Feeds

Cybersecurity Services

- 24x7x365 Security Operations Center (SOC)
- ISAC Threat Notification Service (IP & Domain Monitoring)
- Malicious Domain Blocking & Reporting (MDBR)

Security Best Practices

- CIS SecureSuite Membership
  - *Tools to implement the CIS Critical Security Controls and CIS Benchmarks*

Other Member Resources

- MS-ISAC Webinars
- MS-ISAC Working Groups
- Nationwide Cybersecurity Review (NCSR)
- Homeland Security Information Network (HSIN)
- CIS CyberMarket

Nationwide Cybersecurity Review (NCSR)

https://www.cisecurity.org/ms-isac/services/ncsr

A no-cost, anonymous, annual self-assessment based on NIST CSF

(open October – February)

Requirement for the Homeland Security Grant Program (HSGP) and the State and Local Cybersecurity Grant Program (SLCGP)

NATIONWIDE CYBERSECURITY REVIEW

Organization specific metrics; Reporting templates and resources to help with prioritization

NCSR information & registration:

Confidential & Proprietary

Foundational Assessment

foundationalassessment@cisecurity.org

- **Get started with a Foundation Assessment:**
  - Brief 32 question assessment to evaluate essential activities in a cybersecurity program
  - Aligns to NIST CSF and the CIS Critical Security Controls
  - For SLTTs that have never completed the NCSR
- **Next step:**
  - Complete the NCSR for a wholistic review of your cybersecurity program
  - Open October - February

Confidential & Proprietary

Implement Best Practices

Start with Implementation Group (IG) 1

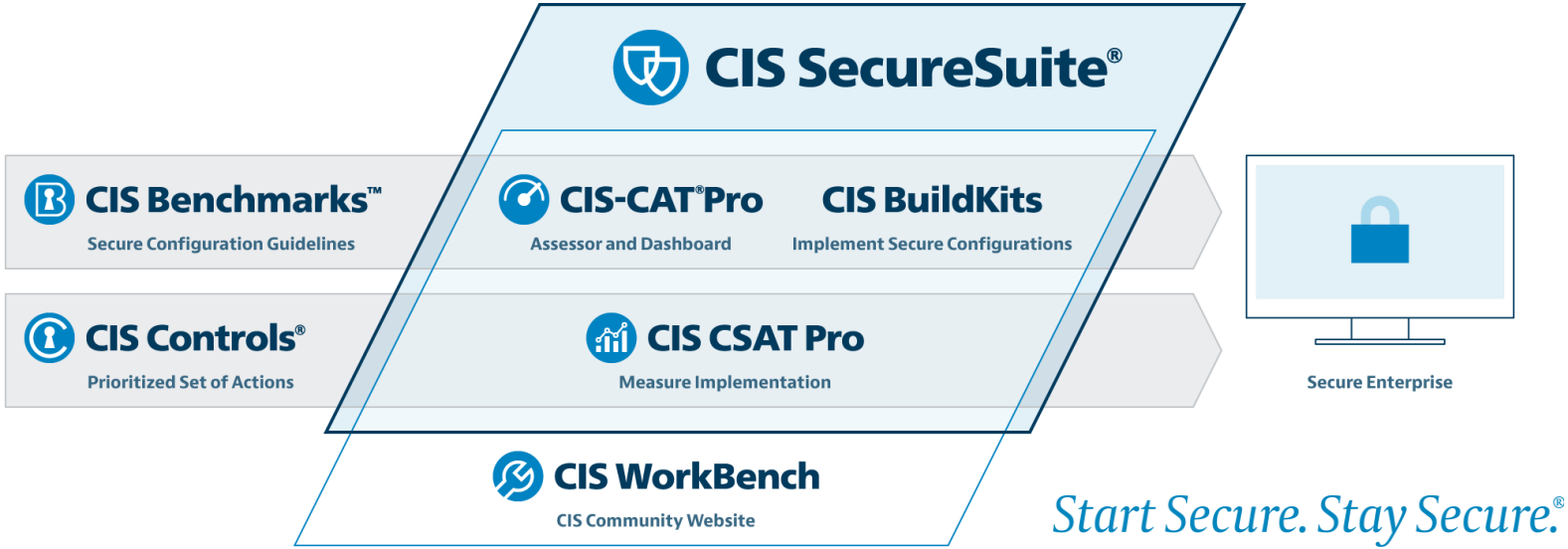
- **CIS Critical Security Controls**
  - A prioritized set of actions to protect your organization and data from known cyber-attack vectors.
- **Implementation Group 1**
  - Defined as “essential cyber hygiene”
  - Represents the essential Safeguards that mitigate the most common attacks
  - 56 Safeguards out of the 153 total

CIS Controls

https://www.cisecurity.org/controls/

CIS SecureSuite®

FreeSecureSuite@cisecurity.org

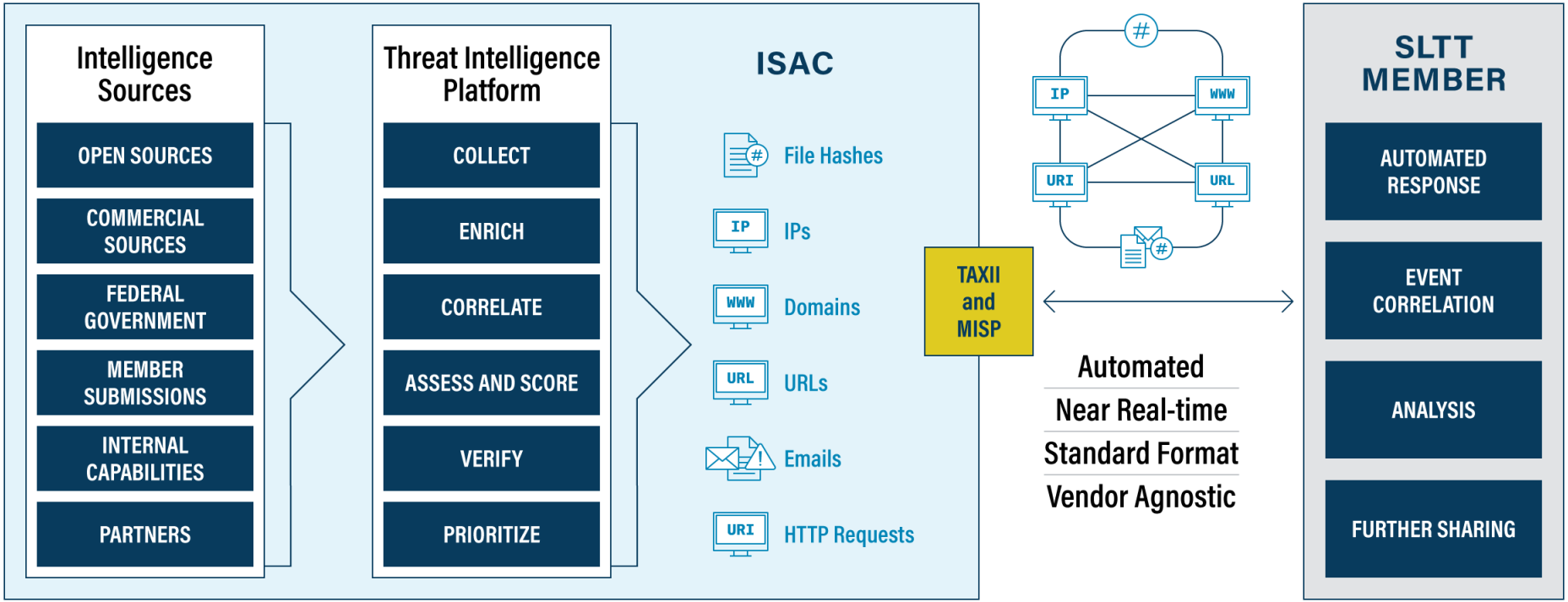


https://www.cisecurity.org/cis-securesuite/member-webinars

Confidential & Proprietary

Grow Your Cyber Intelligence

Indicator Sharing Program



Confidential & Proprietary

Network and Endpoint Defense

Services@cisecurity.org

NO COST MS-ISAC SERVICES:

- Malicious Domain Blocking and Reporting (MDBR)
- ISAC Threat Notification (IP & Domain Monitoring)

LOW COST CIS SERVICES:

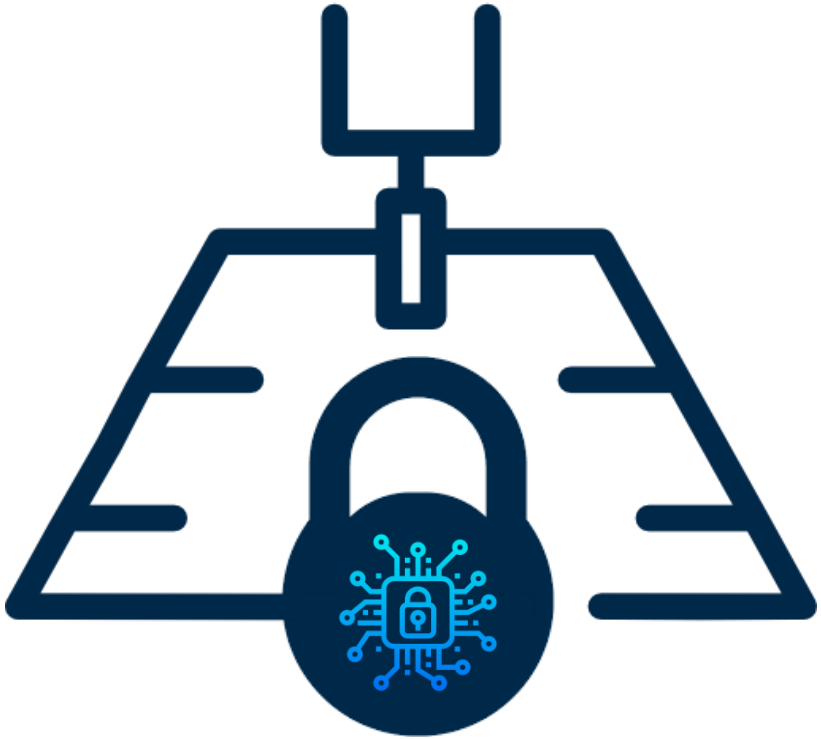
- Network Monitoring (Albert)
- Endpoint Security Service (ESS)

Confidential & Proprietary

Homefield Advantage

How the MS-ISAC Can Help Strengthen K12 Cybersecurity

1. Having the **RIGHT PLAYERS** on your Team – The MS-ISAC is here and ready to play!
2. Using our **SCOUTING REPORTS** – Our K12 Report and Joint Cybersecurity Advisory are designed to keep you one step ahead.
3. Leveraging our **PLAYBOOK** of five recommended actions - To help build Effective Cybersecurity Programs.
4. Tapping into our **SPECIAL TEAMS** of no cost and low-cost services.



Confidential & Proprietary

Snapshot of a K12 Cyber Incident

soc@cisecurity.org

What Happened?

July 2022, a K12 member district serving less than 5,000 students was impacted by ransomware.
They notified the MS-ISAC of the incident

MS-ISAC Response: SOC

MS-ISAC SOC triaged the initial incident, collecting details, offering recommendations, and connecting the member to the CIRT.

MS-ISAC Response: CIRT

CIRT analyzed 100GB of data to understand threat actor actions and IOCs. CTI provided additional intelligence on the threat actor. CIRT provided scripts to K12 to determine if identified IOCs were present; also provided guidance to assist with ongoing recovery efforts.

The Impact

K12 member said MS-ISAC response was instrumental in understanding the incident timeline, developing IOCs, and obtaining necessary guidance to help restore the network.

Confidential & Proprietary

Cyber Incident Response Team (CIRT)

- Incident Response
- Malware Analysis
- Log Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Confidential & Proprietary

Recommendations

What to do Today, Tomorrow and Beyond

- **Today**: Join the MS-ISAC
  - *https://learn.cisecurity.org/ms-isac-registration*
- **Tomorrow**: Enroll in MDBR
  - *https://www.cisecurity.org/ms-isac/services/mdbr*
- **Next Week**: Enable MFA and obtain vulnerability scans
  - *https://www.cisa.gov/cyber-hygiene-services*
- **Next Two Weeks**: Enable logging on all systems
- **Future Steps**: Establish an Incident Response (IR) and Data Backup plan
  - *Control #17: https://learn.cisecurity.org/cis-controls-download*

Confidential & Proprietary

Resource Links

CISA/MS-ISAC Joint Ransomware Guide

- Best practices and incident response guidance
- https://www.cisa.gov/stopransomware/ransomware-guide
- https://www.cisa.gov/stopransomware

ANY QUESTIONS?

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

Thank You!

Michelle Nolan

Regional Engagement Manager

Michelle.Nolan@cisecurity.org | 518-516-3030

Confidential & Proprietary