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

MS-ISAC Services Overview

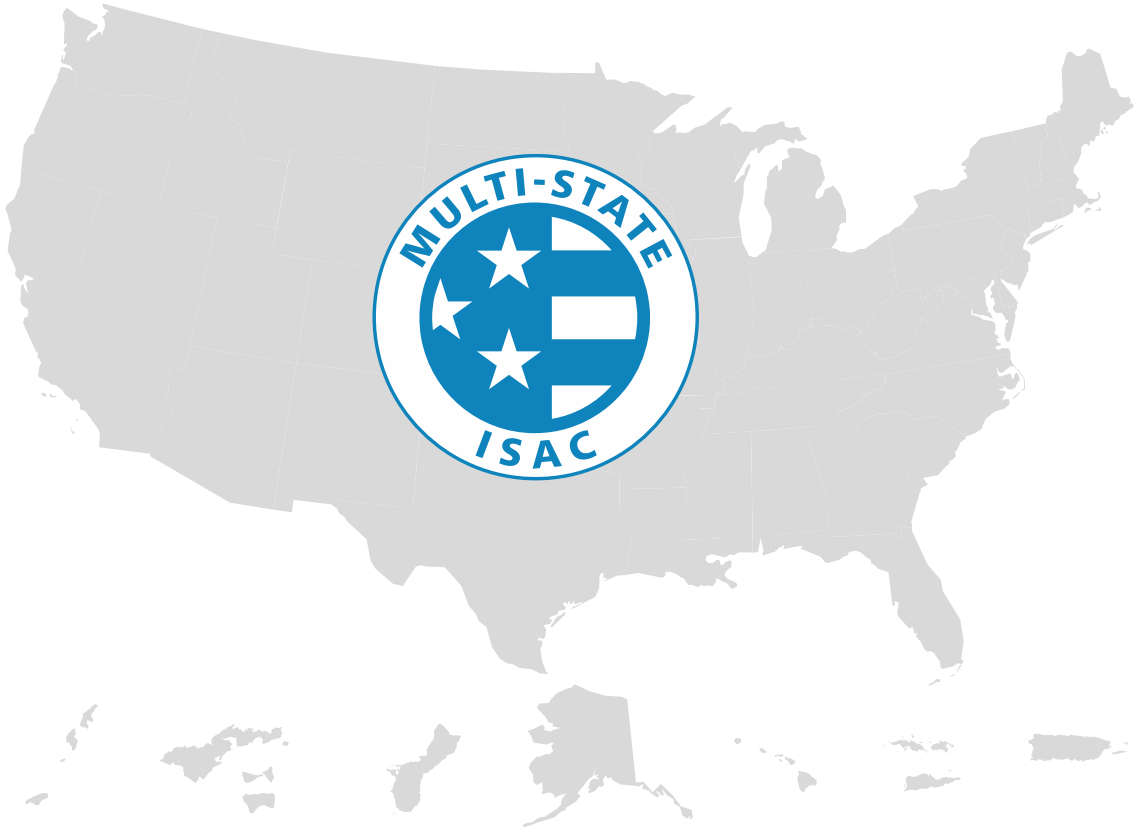
Eugene Kipniss
Director of Strategic Enablement
518-466-1066
Eugene.Kipniss@cisecurity.org

MS-ISAC® 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



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

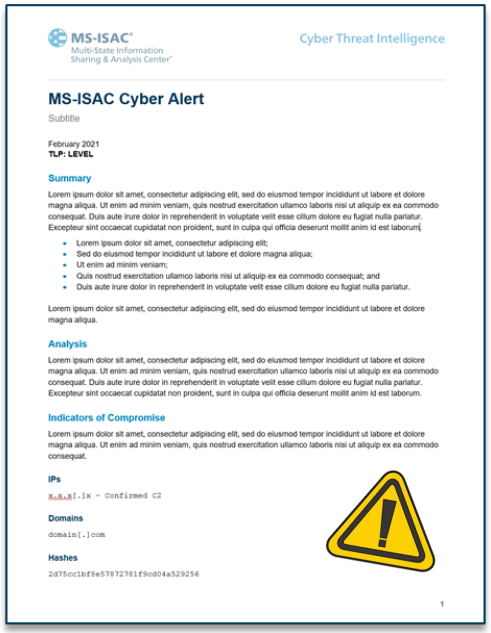
Elections Infrastructure ISAC®

Proactive and Everyday Resources

Cyber Threat Intelligence Products

Advisories & Alerts

- Ad Hoc
- Urgent Actions
- Prevalent Threats


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

Cyber Threat Intelligence

MS-ISAC Cyber Alert

Subtitle

February 2021
TLP: LEVEL

Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- Lorem ipsum dolor sit amet, consectetur adipiscing elit;
- Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua;
- Ut enim ad minim veniam;
- Quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat; and
- Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Indicators of Compromise

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

IPs

X.X.X.[.]x - Confirmed C2

Domains

domain[.]com

Hashes

2d75cc1bf8e57872781f9cd04a529256

1

Reports

- Assessment Based
- Probability Focused
- Analytic Confidence


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

Cyber Threat Intelligence
Long-Form Analytic Report

Cyber Threats to the Healthcare Industry

Analysis Across Trends from 2019-2021

February 2021 • LFAR-2021-0002
TLP: WHITE

Executive Summary

Protected health information (PHI) represents highly valuable data for cybercriminals on dark web markets. Constrained financial resources, system sprawl, and varied cybersecurity awareness among staff are primary factors for the majority of healthcare-related breaches. In 2019, attacks against healthcare institutions increased by 75%, and these trends will likely increase due to pandemic-related telework vulnerabilities; increasing integration of innovative technology into legacy systems; and profitable return for exfiltrated data within the healthcare sector. This publication aims to illuminate current targeted data and identify key cybersecurity trends between 2019-2020 to highlight major threats and vulnerabilities for healthcare industries in 2021.

Key Findings

An increase in ransomware campaigns and secondary infections, through long-term campaigns against digital healthcare supply chains, marks a notable shift from 2019-2020. COVID-19 vaccine research makes an attractive target for nation-state cyber threat actors (CTAs), while COVID-19-themed phishing lures offer cybercriminals an opportunity to capitalize on hospitals in need of personal protective equipment (PPE), such as N95 masks.

- Estimated total financial losses for U.S. health systems and facilities at $323.1 billion in 2020. [1]
- Seventy-five percent increase in reports of ransomware attacks on healthcare entities in 2019.[2]
- Stolen medical records can sell for 10 to 20 times more than credit card or social security numbers. [3]
- COVID-19-related phishing attempts increased by 700% worldwide in 2020.[4]

Substantive Analysis

Most successful data breaches stem from human error or adversaries preying upon human behavioral patterns of trust, fear, and urgency. [5] With hospitals and healthcare providers rushing to acquire PPE, contain COVID-19 within their facilities, and minimizing staff to reduce spread, cybercriminals are provided many windows of opportunity to leverage human error. Errors can range from misconfigured systems, susceptibility to phishing, and improperly secured data. The Multi-State Sharing and Analysis Center's (MS-ISAC) Cyber Threat Intelligence (CTI) team assesses with high confidence cybercriminals will likely increase targeting hospitals and healthcare providers in 2021. The CTI team bases this assessment on current reported profitable returns for PHI,[6] wider attack surfaces due to integration of legacy systems with internet-of-things (IoT) devices; increased telemedicine practices; and the cost associated with an inability to care for patients[7] or store limited vaccine supply. [8]

Targeted Data

Medical identity theft, which includes using a victim's personal information to fraudulently obtain medical services or prescriptions alongside standard identity theft actions, represents a critical threat to patients and providers

1

Strategic Assessments

- Deeply Researched
- Forward Looking
- Trends & Patterns


TLP: AMBER

Quarterly Threat Report

This proprietary document is based on the Quarter 1 2021 security event data.

MULTI-STATE ISAC

Multi-State Information Sharing and Analysis Center

TLP: AMBER

Briefs & Blogs

- Simple or Complex
- Technically Focused
- Threat Driven


CIS. Center for Internet Security®

Cybersecurity Best Practices | Cybersecurity Tools | Cybersecurity Threats

Home • Resources • Blog • Why TikTok is the Latest Security Threat

Why TikTok is the Latest Security Threat

TikTok and Data Collection

Collection of PII and User Data

Violations of COPPA

Censorship

What Can Be Done?

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

Nationwide Cybersecurity Review (NCSR)

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

No cost

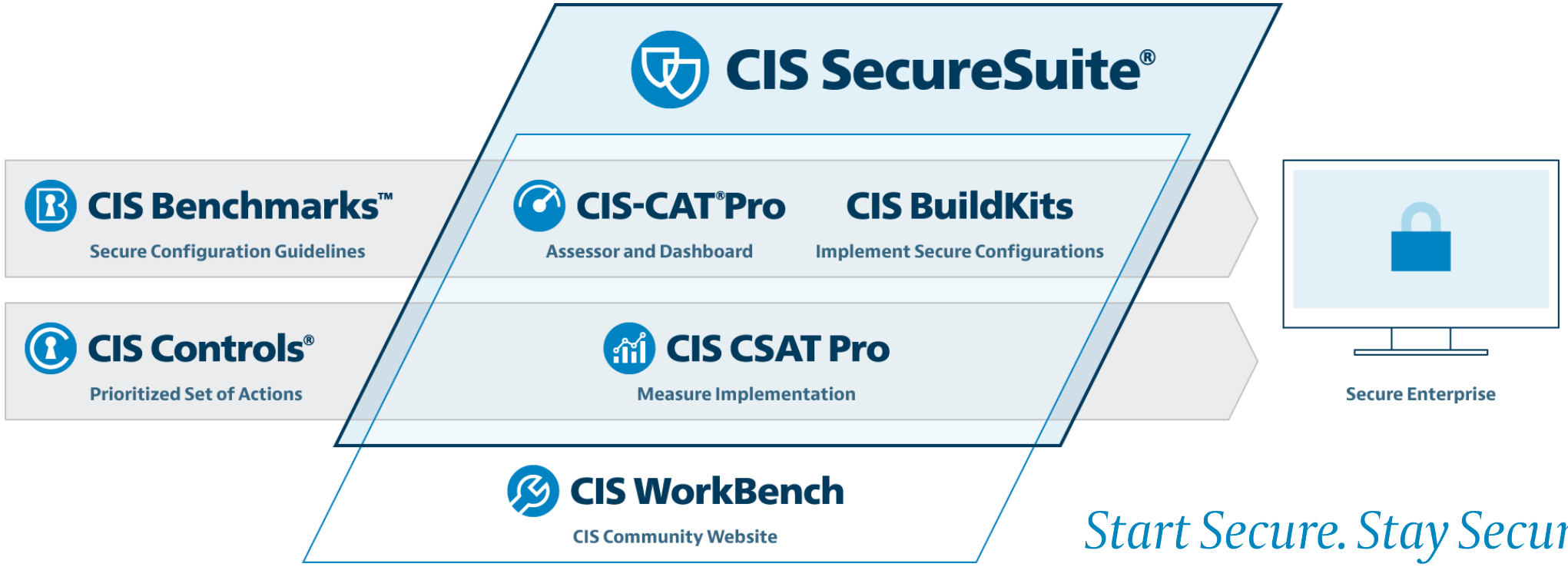
Anonymous

Self-Assessment

SCORE	MATURITY LEVEL	The recommended minimum maturity level is set at a score of 5, indicated by the red horizontal line below
7	Optimized	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy	Your organization has a formal policy in place that has been approved by senior management.
2	Informally Done	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.
1	Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.

CIS SecureSuite®

FreeSecureSuite@cisecurity.org



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

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

Elections Infrastructure ISAC®

In Case of Cyber Emergency - Break Glass

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

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

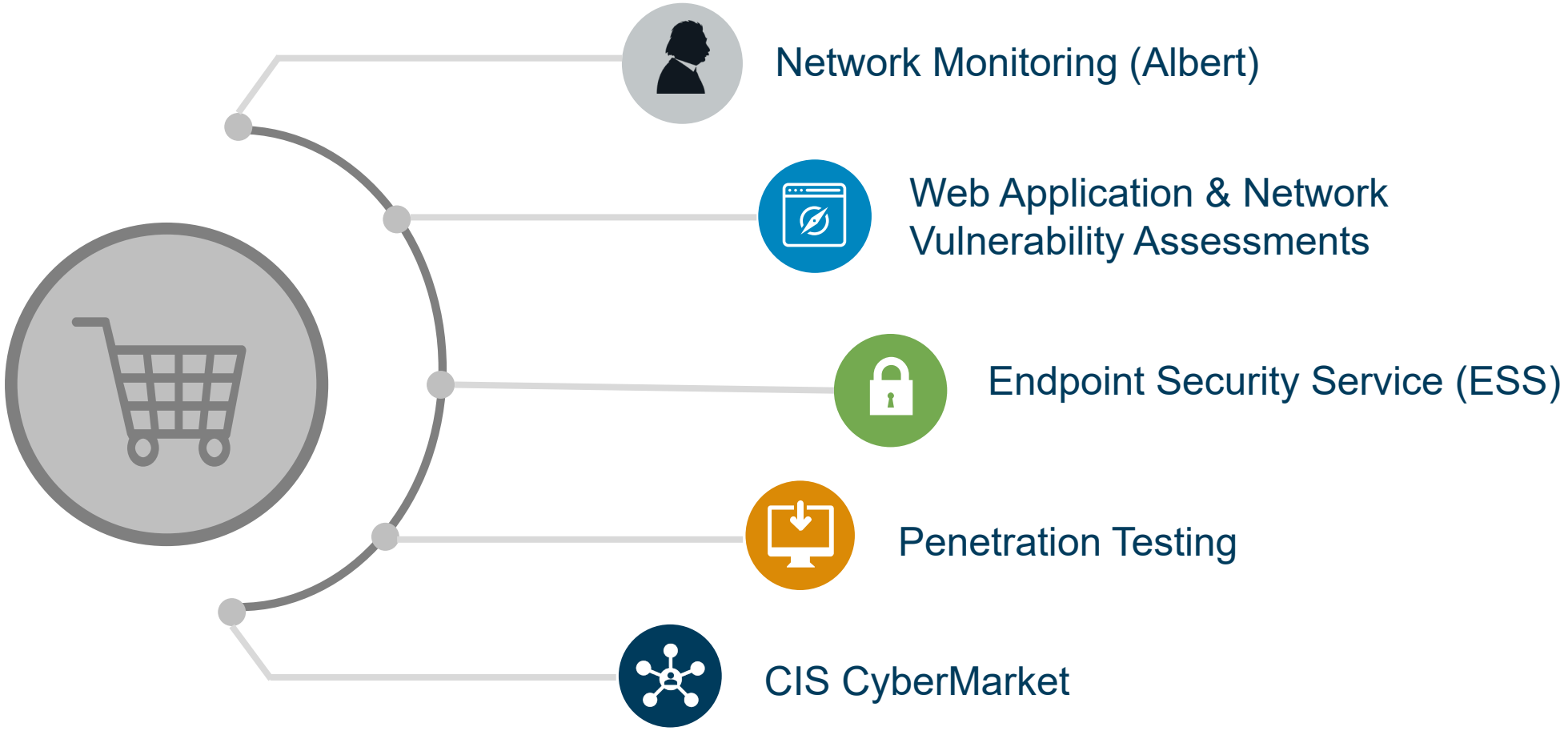
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC®

Other Services and Quick Links

Fee Based Services

Services@cisecurity.org



How to access MS-ISAC resources

Register for MS-ISAC Membership	https://learn.cisecurity.org/ms-isac-registration
MS-ISAC 24x7 Security Operations Center	1-866-787-4722 | SOC@cisecurity.org | info@cisecurity.org
Register for MDBR	https://mdbr.cisecurity.org/
Connect to Real-Time Indicator Feeds	https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds/

Benefits of MS-ISAC Membership

No Cost Services

→ 24×7×365 Security Operations Center (SOC)
→ Passive IP & Domain Monitoring
→ Malicious Domain Blocking & Reporting (MDBR)
→ Cybersecurity exercises
→ Cybersecurity advisories
→ Cyber event notifications
→ Education and awareness materials
→ CIS SecureSuite® Membership
→ Incident response resources

access, including portals for communication and document sharing

→ Real-Time Intelligence Sharing
→ Nationwide Cybersecurity Review (NCSR)
→ Discounts on training
→ Vulnerability assessment services

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

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

Thank You!