



**MS-ISAC<sup>®</sup>**

Multi-State Information  
Sharing & Analysis Center<sup>®</sup>

# MS-ISAC Services Overview

*Eugene Kipniss*

*Director of Strategic Enablement*

*518-466-1066*

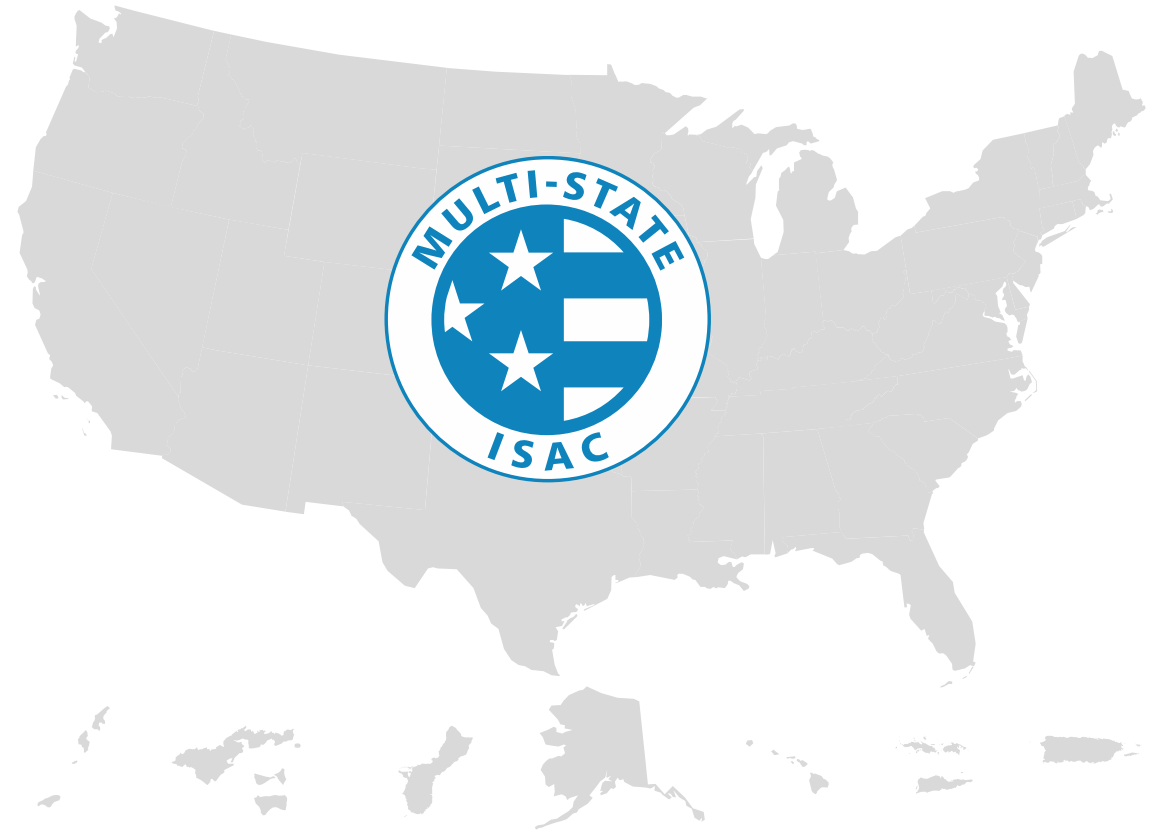
*[Eugene.Kipniss@cisecurity.org](mailto:Eugene.Kipniss@cisecurity.org)*

Confidential & Proprietary

## 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>





# Proactive and Everyday Resources

## Advisories & Alerts

- Ad Hoc
- Urgent Actions
- Prevalent Threats

## Reports

- Assessment Based
- Probability Focused
- Analytic Confidence

## Strategic Assessments

- Deeply Researched
- Forward Looking
- Trends & Patterns

## Briefs & Blogs

- Simple or Complex
- Technically Focused
- Threat Driven

**MS-ISAC Cyber Alert**

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.

**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**

Malicious IP - Confirmed C2

**Domains**

domain[.]com

**Hashes**

2d750c18fe657827181f90d484529256

**Cyber Threats to the Healthcare Industry**

Analysis Across Trends from 2019-2021

February 2021 • L-FAR-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 network vulnerabilities, increasing integration of innovative technology into legacy systems, and profitable return for sophisticated 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 \$123.1 billion in 2020.<sup>1</sup>
- Seventy-five percent increase in reports of ransomware attacks on healthcare entities in 2019.<sup>2</sup>
- Stolen medical records can sell for 10 to 20 times more than credit card or social security numbers.<sup>3</sup>
- COVID-19-related phishing attempts increased by 700% worldwide in 2020.<sup>4</sup>

**Substantive Analysis**

Most successful data breaches stem from human error or adversaries preying upon human behavioral patterns of trust, fear, and urgency.<sup>5</sup> 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 returns for PHI,<sup>6</sup> 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' or store limited vaccine supply.<sup>7</sup>

**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.

**Quarterly Threat Report**

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

Multi-State Information Sharing and Analysis Center

TLP: AMBER

**Why TikTok is the Latest Security Threat**

TikTok is a widely popular social-media platform owned by the Chinese technology company ByteDance. Though its stated intention is to share short dance and lip-sync videos, it has become a substantial player in the targeted advertising business in recent years.

**TikTok and Data Collection**

TikTok gained an edge through its ability to collect sensitive data about users, even when those users either saved or shared their content. This presents a security threat for users due to the 2017 Chinese National Intelligence Law, which states that "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law."<sup>1</sup>

**Collection of PII and User Data**

The data TikTok collects from users contains sensitive information and is often shared without the user's explicit knowledge. This data includes device type and model, operating system (OS) version, mobile carrier, browsing history, age, and the names and types, frequency patterns or patterns, network connections, and geolocation (GPS) location history (which describes the collection and analysis of data pertaining to identifiable information (PII) as well as user data collected from other sources. This data can include age, image, personal contacts, relationship status, preferences, and app usage. The content of this report and information about when messages and sent, received and read.<sup>2</sup> In aggregate, TikTok's data collection is more extensive than other apps.

To use the platform, users grant the app access to the microphone and camera. Multiple reports allege that TikTok also collects biometric data from users, including facial analysis for face scans, voice recognition, and fingerprint (FIS) for user facial recognition software to superimpose images on users faces for use in videos. Unlike other data that is collected, biometrics represent the physical user and are generally permanent. Biometrics are therefore of high intelligence value. There is direct evidence that TikTok is giving this data to the Chinese government, and the evidence of its national intelligence capabilities. It is to provide the data to the government.

While TikTok claims that user data is stored in the U.S. and Singapore, TikTok's parent company servers are all located in China and the app itself contains references to China-based infrastructure. While it is unclear if Chinese officials would have access to the data stored in the U.S., all data stored within China may be shared with the Chinese government for intelligence purposes. Because of this, users should assume that their data is being aggregated and shared with the Chinese government.

Security and privacy concerns stem largely from the vague definition of the law and the promise that the app will protect those who do it. Suspected use of propaganda to further China's political interests, coupled with the creation of an unregulated information marketplace, has made TikTok a hot topic for the U.S. government and cybersecurity community alike. Unlike Google, the U.S. does not have laws forcing tech to prohibit the collection, sale, and use of such personal data. Making TikTok able to continuously scrape user data with little regard or oversight.

**Violations of COPPA**

TikTok collects data from all age groups and is doing so regularly violates the Children's Online Privacy Protection Act of 1986 (COPPA). Under COPPA, "operators of child-directed apps cannot lawfully obtain the PII of children under 13 years of age without first obtaining verifiable consent from parents."<sup>3</sup> In 2019, most case against ByteDance alleges that users children under the age of 13 were not asked to provide any parental consent to use TikTok.<sup>4</sup> (ByteDance settled the case and agreed to adding in parental control, however, as of May of this year, multiple consumer groups have advised the Federal Trade Commission that TikTok continues to violate COPPA.)<sup>5</sup>

**Censorship**

Moderation guidelines for TikTok were issued in late 2019 highlighting the app's censorship of any content critical of Chinese state interests. According to the leaked documents, the company instructs their moderators to remove any verifiable content related to topics sensitive to the Chinese Communist Party (CCP) including Taiwan, Hong Kong, Xinjiang, Tibet, and any content critical of the U.S. (see year 1 U.S. Senator posted a TikTok video regarding a "TikTok ban" that actually meant to bring attention to Chinese censorship of religious freedom).

While the app is not removed, and though it may only temporarily, the behavior aligns with China's national interests without regard for freedom of expression.

**What Can Be Done?**

The U.S. military and private companies, such as Amazon, are among those currently banning TikTok on business devices (10) regardless of an organization's position on TikTok specifically. In response, the guidelines for use further in the App Store for iOS (11) for business devices, but those who would like to take a step further, social media apps can be easily blocked by category or by specific infrastructure, such as internet disconnect and domain names.

The MS-ISAC Cyber Threat Intelligence (CTI) team recommends state, local, tribal, and territorial (SLTT) government entities and all community members include information about what is collected should be avoided. In the case of TikTok, CTI recommends parents, teachers, and local leaders talk to young adults, teenagers, and children who may be using the app about the dangers it poses to their personal security. Through education and awareness, all are able to limit the use of personal data in nefarious ways.

# 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





**No cost**



**Anonymous**



**Self-Assessment**

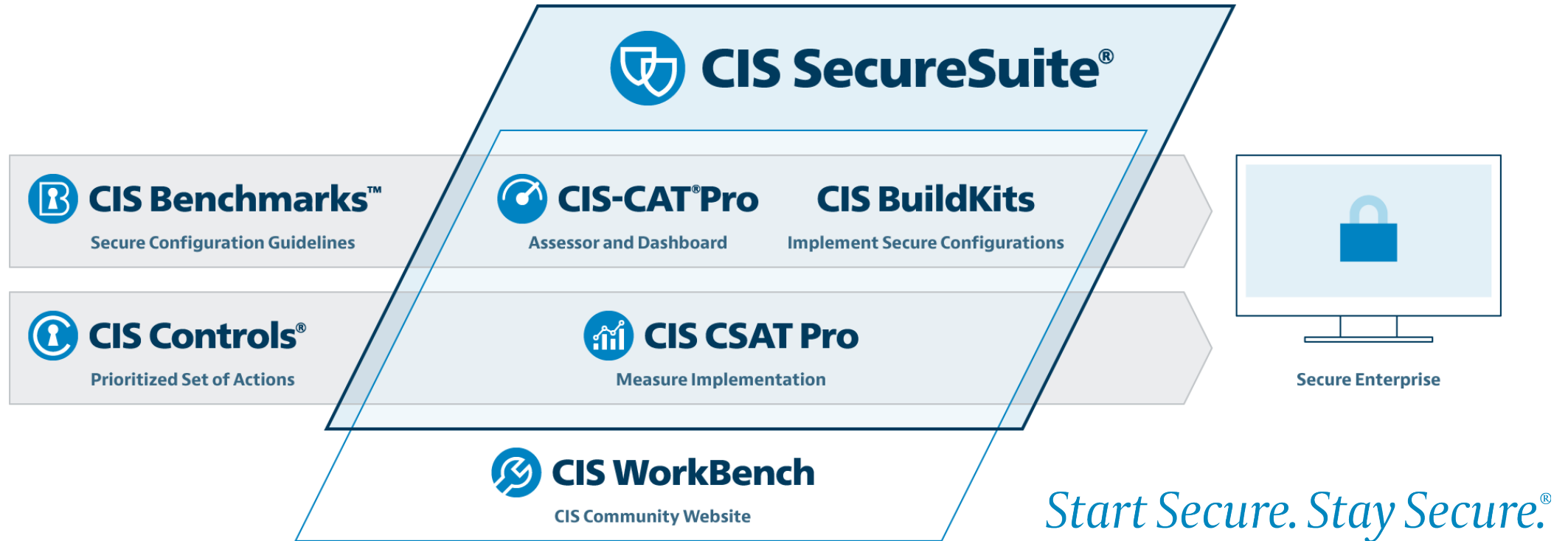
Confidential & Proprietary

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<sup>®</sup>

[FreeSecureSuite@cisecurity.org](mailto:FreeSecureSuite@cisecurity.org)



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

Confidential & Proprietary

TLP:WHITE



# In Case of Cyber Emergency - Break Glass





## 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](mailto:soc@cisecurity.org)**



Incident Response

Malware Analysis

Log Analysis

To report an incident or  
request assistance:

Phone: 1-866-787-4722

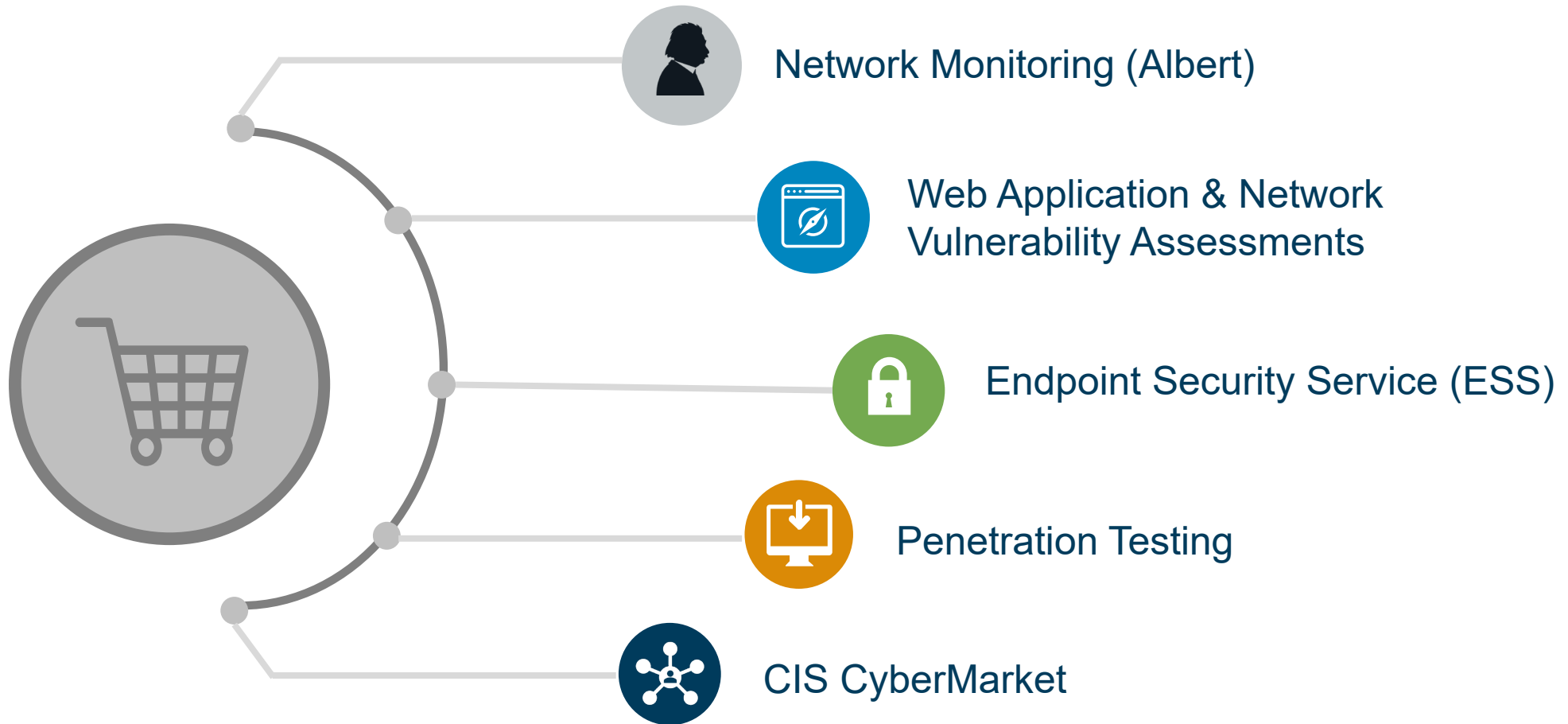
Email: [soc@cisecurity.org](mailto:soc@cisecurity.org)



## Other Services and Quick Links

# Fee Based Services

[Services@cisecurity.org](mailto:Services@cisecurity.org)



Confidential & Proprietary



# 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](mailto:SOC@cisecurity.org) | [info@cisecurity.org](mailto: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/>

## 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<sup>®</sup>**

Multi-State Information  
Sharing & Analysis Center<sup>®</sup>

**Thank You!**