



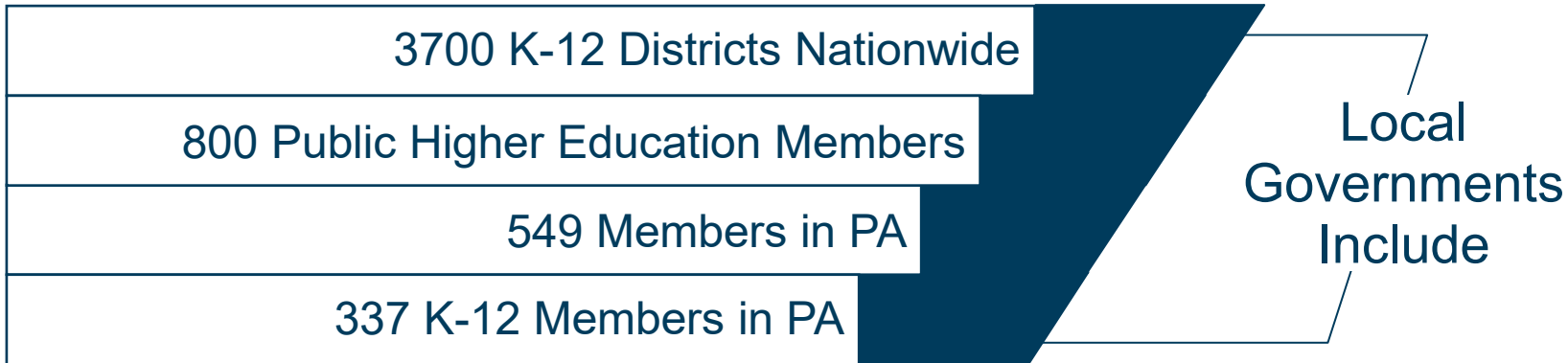
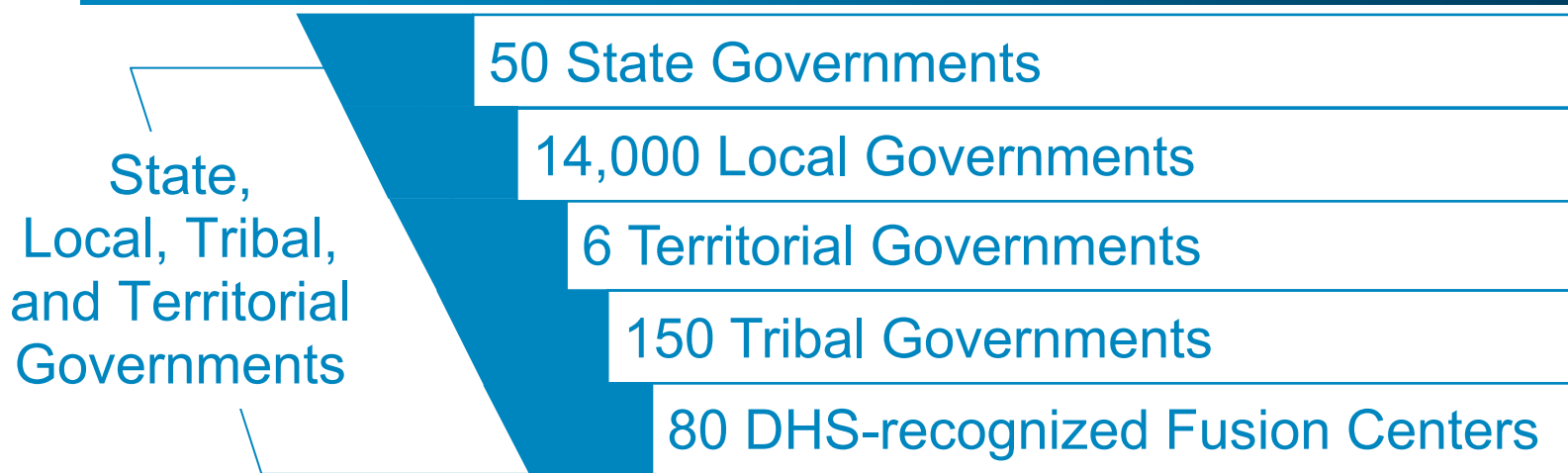
MS-ISAC®

Multi-State Information
Sharing & Analysis Center®

No-Cost Resources with the MS-ISAC

Kyle Bryans

MS-ISAC Regional Engagement Manager





MS-ISAC®

Center for Internet Security (CIS)

Nonprofit leading the global community to secure our connected world

Home of the MS-ISAC and EI-ISAC.



Confidential & Proprietary



Benefits of MS-ISAC Membership

No Cost Benefits To You

- 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
- Malicious Code Analysis Platform (MCAP)
- Monthly newsletters, webinars and threat briefings
- Homeland Security Information Network (HSIN)
access, including portals for communication and document sharing
- Deloitte Cyber Detect Cyber Respond Portal
- Nationwide Cybersecurity Review (NCSR)
- Discounts on training
- Vulnerability assessment services

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



Support

**Network
Monitoring
Services
+
Research and
Analysis**



Analysis & Monitoring

**Threats,
Vulnerabilities
+
Attacks**



Reporting

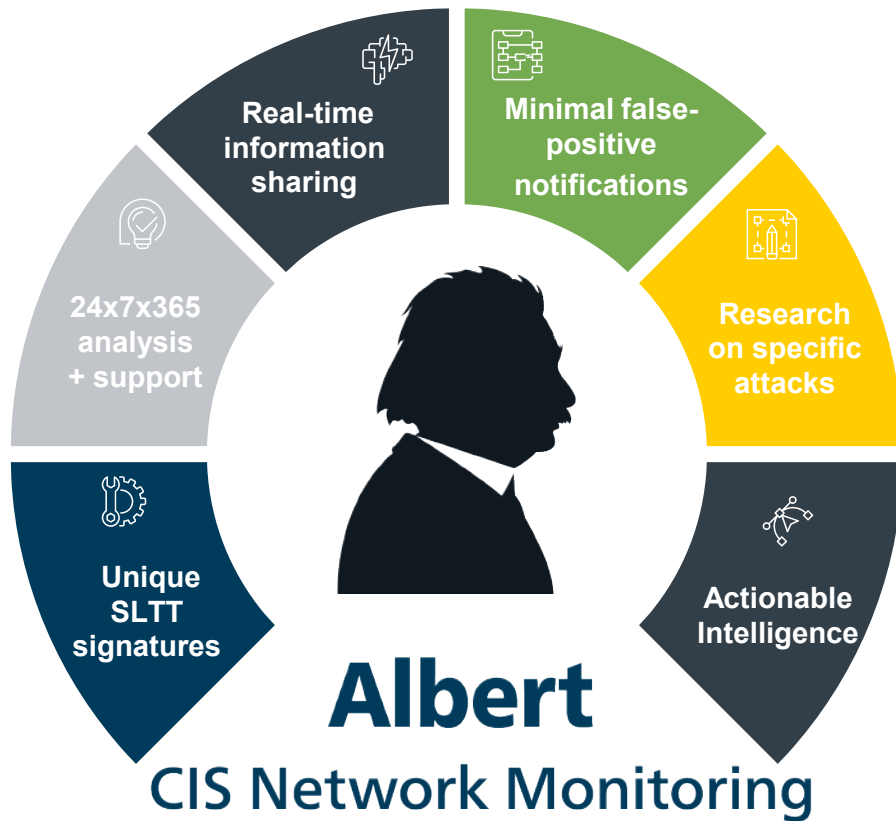
**Cyber Alerts &
Advisories
Web Defacements
Account
Compromises**



**To report an incident or
request assistance:**

Phone: 1-866-787-4722

Email: soc@cisecurity.org





Monitoring of IP Range & Domain Space



IP Monitoring

- Signs of Compromise
- Malicious Activity



Domain Monitoring

- Notifications on compromised user credentials

**Send Public IPs and Domains
to soc@cisecurity.org**



Malicious Domain Blocking and Reporting (MDBR)

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





Malicious Domain Blocking and Reporting (MDBR)

How does it work?

- Proactively blocks network traffic to known harmful web domains.
- Weekly reports sent to organization.

Register for MDBR:

- <https://mdbr.cisecurity.org/>

For more information, review the FAQ:

- <https://www.cisecurity.org/ms-isac/services/mdbr/mdbr-faq/>





MS-ISAC®

CIS SecureSuite Membership



Start Secure. Stay Secure.®

Confidential & Proprietary

TLP:WHITE



MS-ISAC®

CIS SecureSuite Membership

Getting Started is Easy!

1. Log into CIS Workbench:

- <https://workbench.cisecurity.org>

2. Download CIS-CAT Pro Assessor to scan against your target system's configuration:

- <https://workbench.cisecurity.org/files/2151>

3. Learn more – visit the Support Center:

- <https://workbench.cisecurity.org/support-center>

• Contact Us:

- freesequiresuite@cisecurity.org

Cyber Incident Response Team (CIRT)

24x7x365



Incident Response

Malware Analysis

Log Analysis

To report an incident or
request assistance:

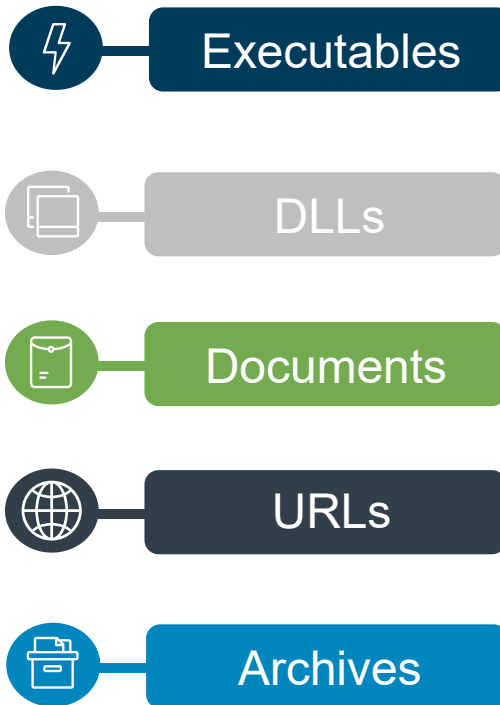
Phone: 1-866-787-4722

Email: soc@cisecurity.org

Malicious Code Analysis Platform (MCAP)

**A web based service used
to submit and analyze
suspicious files**

**To request an account:
mcap@cisecurity.org**



Cyber Threat Intelligence Products

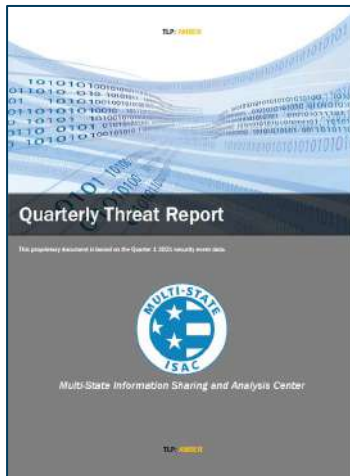
Reports

- Assessment Based
- Probability Focused
- Analytic Confidence



Strategic Assessments

- Deeply Researched
- Forward Looking
- Trends & Patterns



Briefs & Blogs

- Simple or Complex
- Technically Focused
- Threat Driven



Confidential & Proprietary

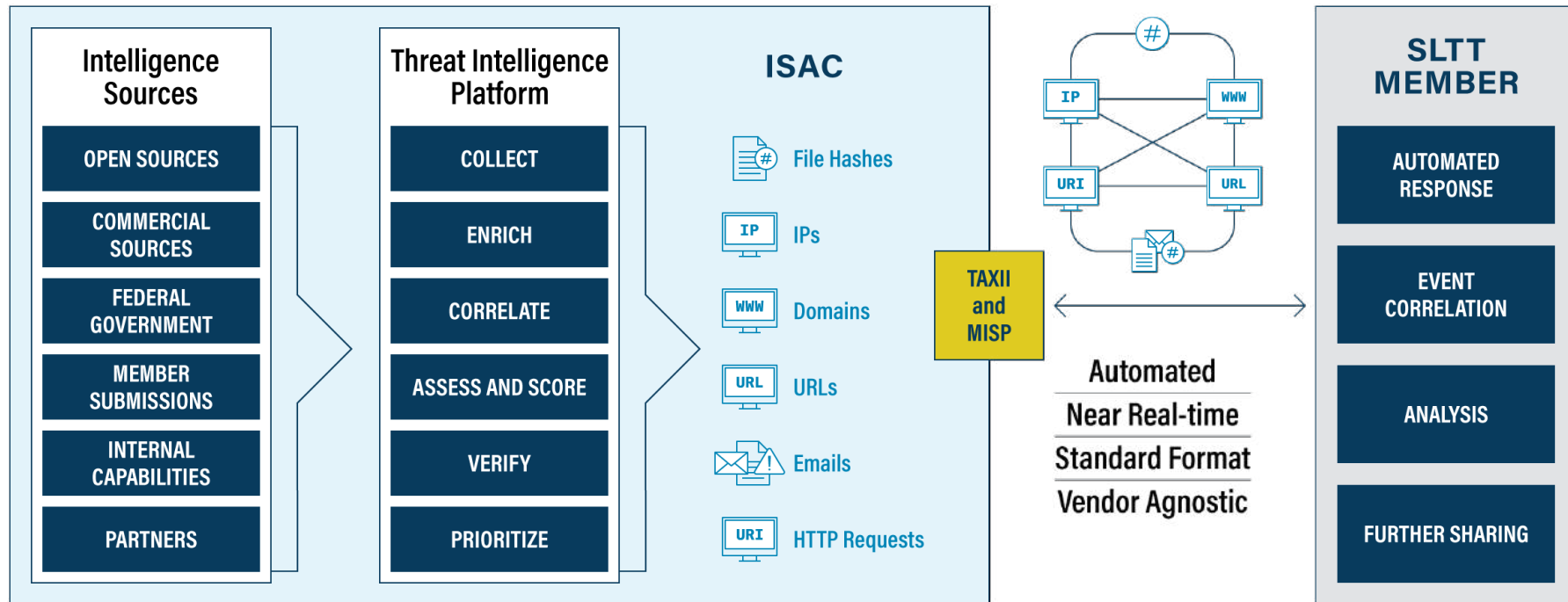
TLP:WHITE



MS-ISAC®

Indicator Sharing Program

Indicator.Sharing@cisecurity.org



Confidential & Proprietary

TLP:WHITE



Deloitte's Cyber Detect & Respond Portal

New Service

- **Secure, online platform for obtaining industry-leading Cyber Threat Intelligence (CTI)**
- **In-depth analysis & recommendations from worldwide network of Cyber threat analysts**
- **Enables a “pull” or “push” approach for obtaining CTI tailored to organization's specific IT environment & cyber threat landscape.**



Deloitte's Cyber Detect & Respond Portal

Register Now

- **Register for access to the portal:**
 - <https://cti.cisecurity.org/>
- **Portal user guide:**
 - <https://learn.cisecurity.org/Deloitte-Portal-Reference-Guide>
- **Webinar recording for in-depth walkthrough of portal:**
 - <https://cisecurity.wistia.com/medias/be7aqeyylu>



MS-ISAC®

MS-ISAC Advisories & Cyber Alerts

MA MS-ISAC Advisory Michael Aliperti Thu 3:38
 UPDATED - MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5 BIG-IP and BIG-IQ Products Could Allow for Arbitrary Code Exe...

Retention Policy Default 2 year move to archive (2 years) Expires 3/25/2023
 ⓘ This message was sent with High importance.

Action Items + Get more add-in

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
 2021-035 - UPDATED


DATE(S) ISSUED:
 03/10/2021
 03/20/2021 - UPDATED
 03/25/2021 - UPDATED

SUBJECT:
 Multiple Vulnerabilities in F5 BIG-IP and BIG-IQ Products Could Allow for Arbitrary Code Execution

OVERVIEW:
 Multiple vulnerabilities have been discovered in F5 products, the most severe of which could allow for remote code execution.

- BIG-IP and BIG-IP Advanced WAF/ASM are a family of products covering software and hardware designed around application availability, access control, and security solutions.
- BIG-IQ enables administrators to centrally manage BIG-IP infrastructure across the IT landscape. It discovers, tracks, manages, and monitors physical and virtual BIG-IP devices - in the cloud, on premise, or co-located at your preferred datacenter.

Successful exploitation of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.




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 inure 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 inure 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 inure 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.x - Confirmed C2

Domains

domain[.]com

Hashes

2d75cc1bf8e57872781f9cd04a529256



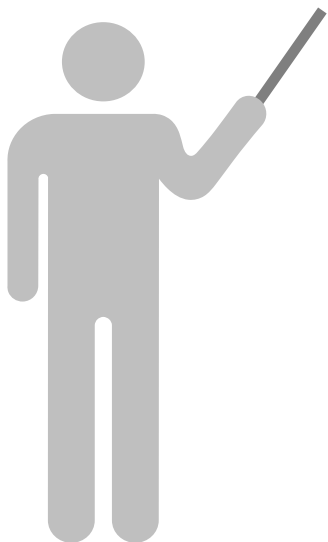
Confidential & Proprietary

TLP:WHITE



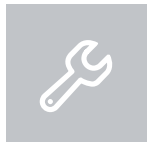
MS-ISAC®

Cybersecurity Awareness Month



How Can You Participate?

- Create a Public Awareness Campaign
- Visit: www.cisecurity.org/ms-isac/ms-isac-toolkit



MS-ISAC Toolkit Resources

- > Make it Official
- > Train the End-User
- > Bring Security Home
- > Train Your Staff
- > Become More Mature
- > Best of the Web Contest



For More Information

- Contact: info@cisecurity.org

Confidential & Proprietary

TLP:WHITE



Nationwide Cybersecurity Review

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.

- Annual Self-Assessment
- NIST Framework
- Cybersecurity Roadmap

For More
Information:

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



Best Practice Resources

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

- **NCSR Results Overview: Peer Group Slick Sheets**
 - State
 - Local
 - Tribal
 - Territory
- **Policy Template Guide**
- **Cybersecurity Resources Guide**
- **Supply Chain Cybersecurity Resources Guide**
- **First Steps Within a Cybersecurity Program**



ISAC Working Groups and Communities

ISAC
Working
Groups



- **Business Resiliency**
- **Metrics**
- **K-12**
- **Leadership Mentoring**
- **Education & Awareness**

**Keep cybersecurity at
the forefront of your
workforces' minds!**



Written for the end-user

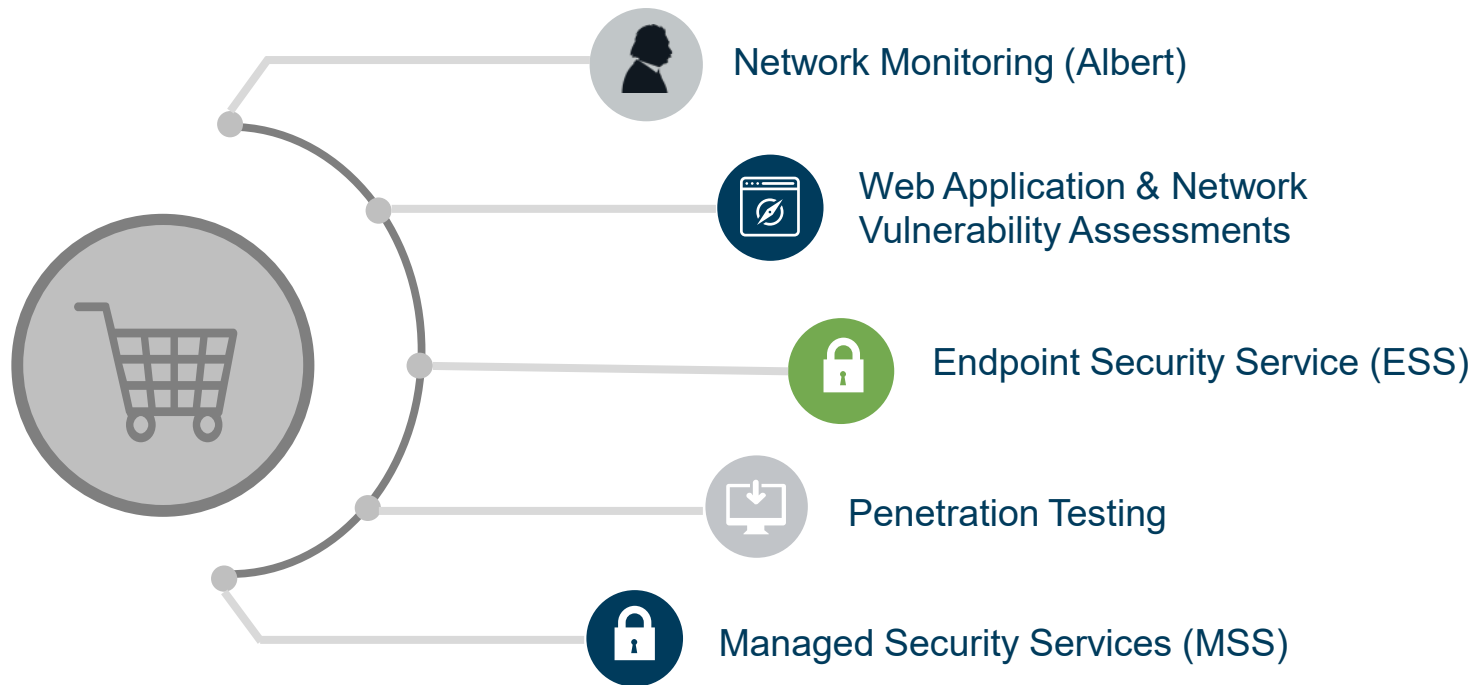


Template Format



Re-brand & re-distribute
as your own







**ANY
QUESTIONS?**





Thank you!

Kyle Bryans

MS-ISAC Regional Engagement Manager

518-880-0747

Kyle.Bryans@cisecurity.org