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

20 YEARS AS YOUR TRUSTED CYBER DEFENSE COMMUNITY
MS-ISAC® Multi-State Information Sharing & Analysis Center®

Higher Ed Threat Brief

Timothy Davis

Sr. Elections CTI Analyst

518-279-5806

Timothy.Davis@cisecurity.org

Confidential & Proprietary

Threat Landscape Overview

- **Opportunistic/Low-Hanging Fruit**
  - Ransomware most impactful
  - Phishing/Spear Phishing (credential harvesting attempts)
  - Malspam (emails with malware laden attachments or links)
  - Exploitation of exposed or vulnerable ports and services (Zero-day exploits)
- **Nation-States or Supporting Groups**
  - Disruptive operations (e.g., DDoS)
  - Destructive operations (e.g., Wipers)
  - Supply chain compromises (e.g., SolarWinds)
  - Information gathering

Higher Education

Why Do Cyber Threat Actors Target Higher Ed?

- **Large amount of Personal Identifiable Information (PII)**
- **Sensitive research/intellectual property**
- **Constant need for system availability**
- **High number of untrained users**
- **Use of legacy/outdated systems**

Threat Highlight

Vulnerabilities and Zero Day Exploits

- **Zero Day exploits**
  - Vulnerability that was previously undisclosed
  - Sometimes made public before a patch is available
  - Attackers can leverage to better access systems undetected
  - Examples include exploitations against Log4j, Microsoft Exchange, MOVEit
- **Attackers are likely to leverage Zero Day exploits to access many organizations and avoid detection**
  - State-affiliated actors and ransomware groups exploit zero-days
  - Trend is highly-likely to continue in 2024

Threat Highlight

Generative AI

- **Tools used to produce various types of content**
  - “Synthetic Media”
  - Text
  - Images/audio/video
  - Code
- **New ways to quickly learn from large datasets**
  - Large Language Models (LLMs)
  - Exact data sources may not be known
- **More details in the prompt = better content generation**

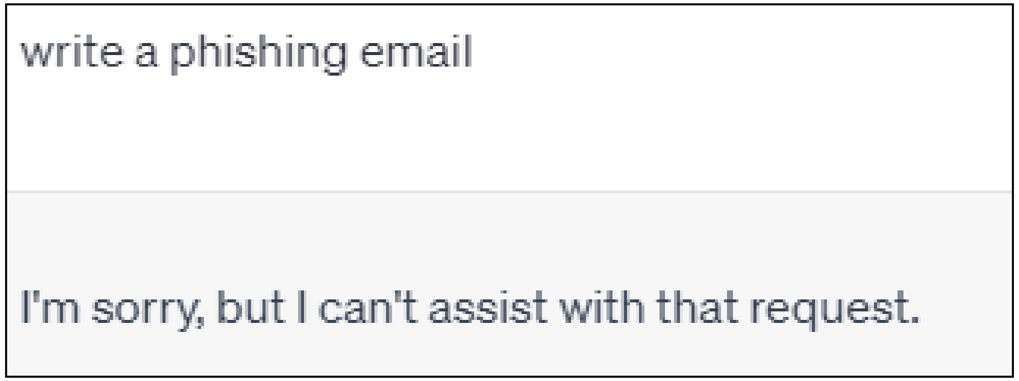
Source: OpenAI

Source: Google Bard

Threat Highlight

Generative AI - Phishing

- **Platforms can generate professional-sounding content**
- **Cyber Threat Actors (CTAs) can leverage this**
  - Not as simple as “write a phishing email”
  - Changing prompts results in content
  - More details in the prompt = better content generation



write a phishing email

I'm sorry, but I can't assist with that request.

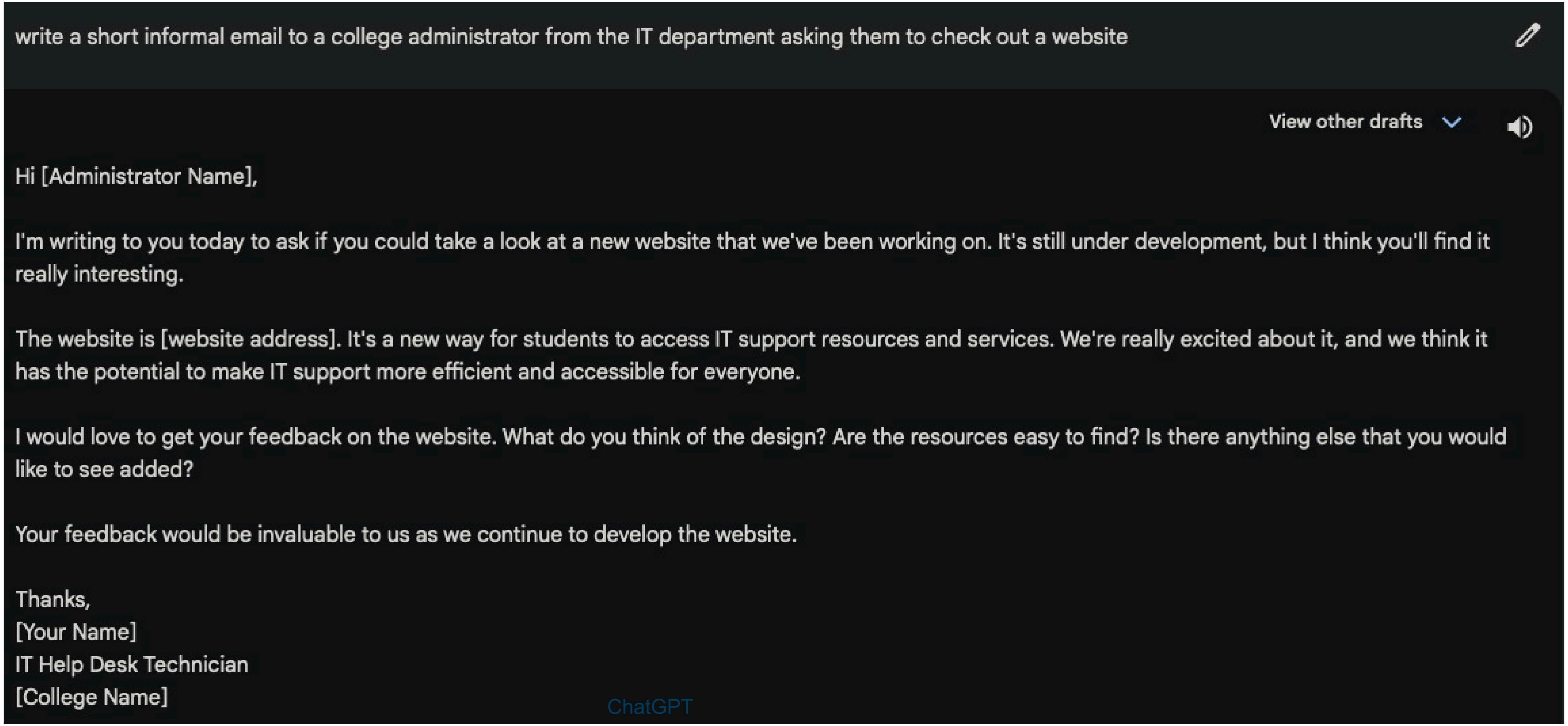
ChatGPT

TLP:CLEAR

MS-ISAC®

Threat Highlight

Generative AI – Phishing Example (Google Bard)



write a short informal email to a college administrator from the IT department asking them to check out a website

Hi [Administrator Name],

I'm writing to you today to ask if you could take a look at a new website that we've been working on. It's still under development, but I think you'll find it really interesting.

The website is [website address]. It's a new way for students to access IT support resources and services. We're really excited about it, and we think it has the potential to make IT support more efficient and accessible for everyone.

I would love to get your feedback on the website. What do you think of the design? Are the resources easy to find? Is there anything else that you would like to see added?

Your feedback would be invaluable to us as we continue to develop the website.

Thanks,
[Your Name]
IT Help Desk Technician
[College Name]

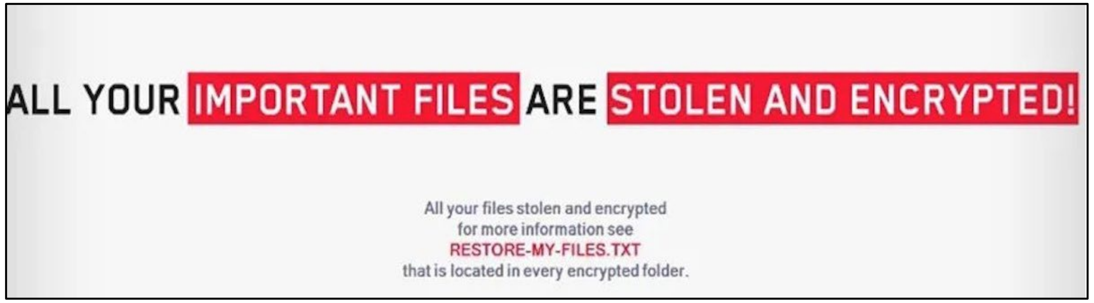
ChatGPT

Google Bard

Threat Highlight

Ransomware

- **Malware that encrypts data, preventing legitimate access**
  - Attackers may steal data and threaten to leak it instead of encrypting systems
- **Attacker will not release data until a payment is made**
  - No guarantee that if you pay you will receive the decryption key, or data will not be leaked
  - Double extortion (encrypted and data stolen)
- **Increasingly common to see ransoms of 7 figures (even for SLTTs)**



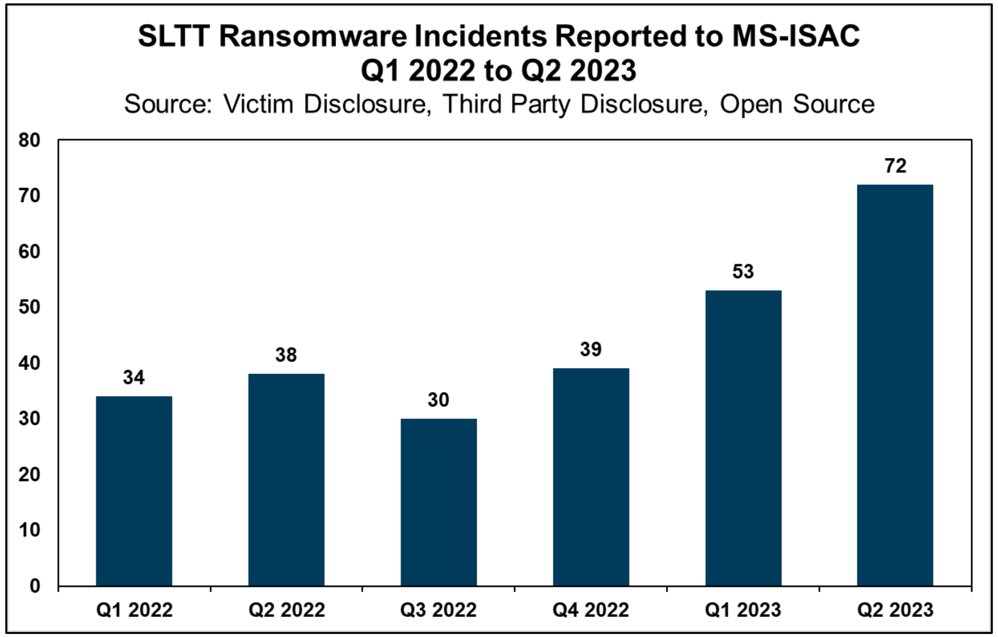
ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Threat Highlight

Ransomware

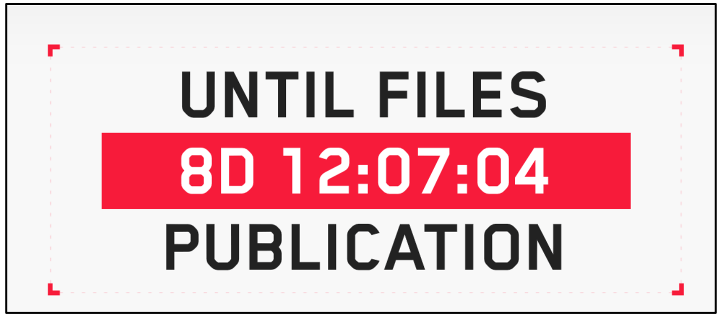
- **Ransomware reporting increasing**
  - 74% increase in SLTT ransomware incidents reported to MS-ISAC from Q1-Q2 2022 to Q1-Q2 2023
- **Chainalysis midyear report**
  - Q1-Q2 2022: $280 million
  - Q1-Q2 2023: $449 million
  - Average ransom payment has increased
- **Top variants reported to MS-ISAC in Q2:**
  - Royal
  - LockBit 3.0
  - Akira


SLTT Ransomware Incidents Reported to MS-ISAC
Q1 2022 to Q2 2023
Source: Victim Disclosure, Third Party Disclosure, Open Source

Threat Highlight

Data Exfiltration

- **Data Theft**
  - Student and staff information (social security numbers, bank information, etc)
- **Harvesting of PII,**
  - Possible use in later campaigns
- **Cyber Espionage**
  - Theft of intellectual property, research, etc.
- **Motivations**
  - Financial
  - Information disclosure
  - Increase credibility within community



UNTIL FILES
8D 12:07:04
PUBLICATION

Recommendations

- **Apply patches as they become available**
- **Inventory management**
  - Hardware and software and version
  - Private and confidential data
- **Monitor system and network traffic for anomalies**
- **Defense-in-Depth**
  - CIS Security Controls
  - Multi-Factor Authentication

Recommendations

- **#StopRansomware Guide**
  - https://www.cisa.gov/stopransomware/ransomware-guide
  - Backups are critical
  - Offline (separate from the network), frequent
  - Attackers target backups stored on the network
- **Centralized logging**
  - Out of band
  - Attackers wipe logs anytime they can
- **Review your incident response plan**

ANY QUESTIONS?

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

20 YEARS AS YOUR TRUSTED CYBER DEFENSE COMMUNITY

Thank You!

Timothy Davis

Sr. Elections CTI Analyst

518-279-5806

Timothy.Davis@cisecurity.org

Confidential & Proprietary

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

MS-ISAC

Current Threats and Incident Response

Megan Incerto
Regional Engagement Manager, MS-ISAC
518-640-3655
Megan.Incerto@cisecurity.org

Timothy Davis
Sr. Elections CTI Analyst
518-279-5806
Timothy.Davis@cisecurity.org

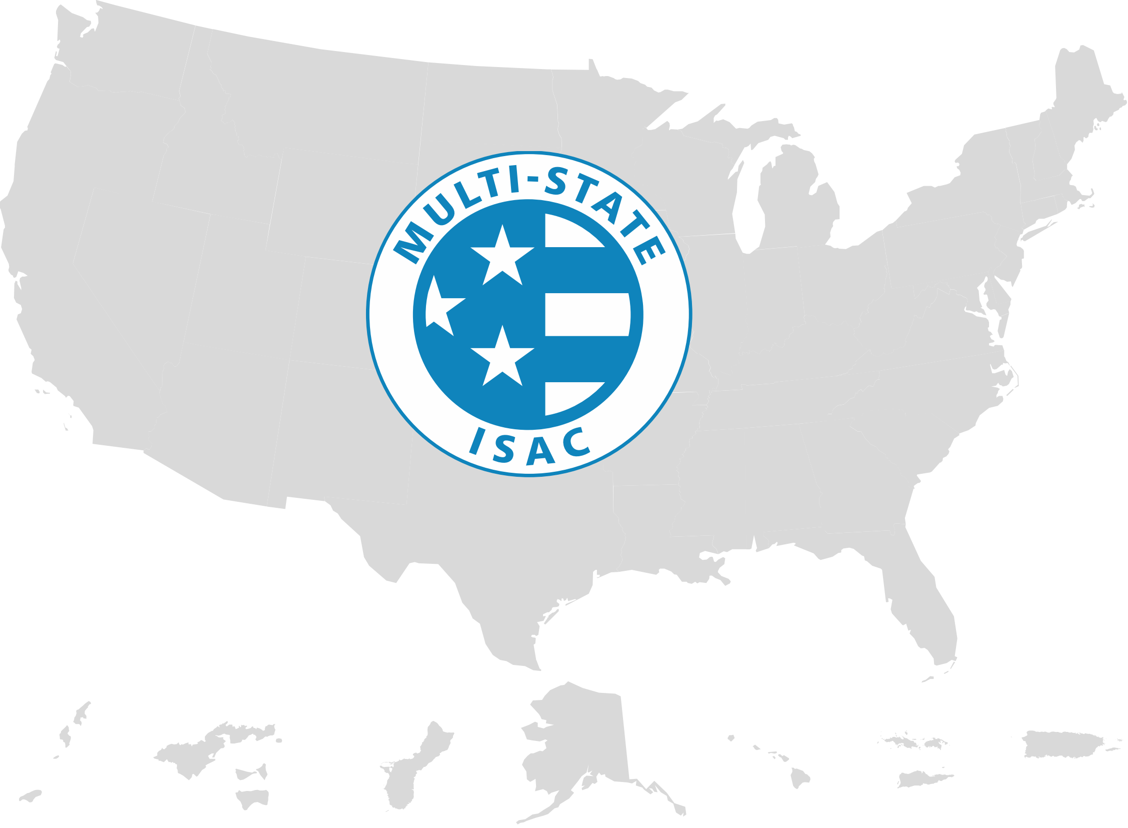
Confidential & Proprietary

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



Who We Serve: MS-ISAC

147
New Members
Since
August 28

15,967
Total
Members

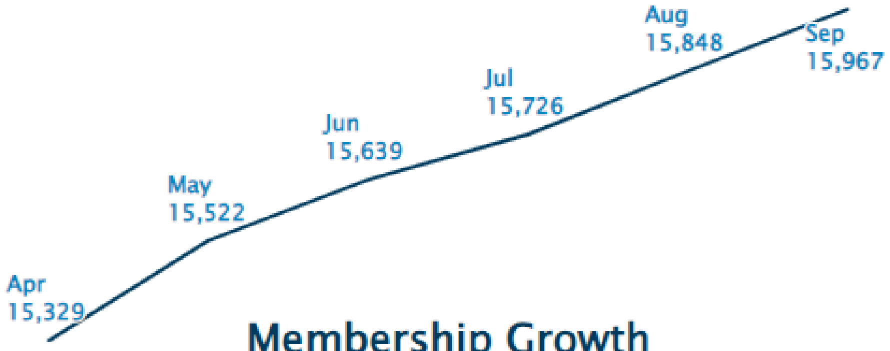
50 States

80 Fusion Centers

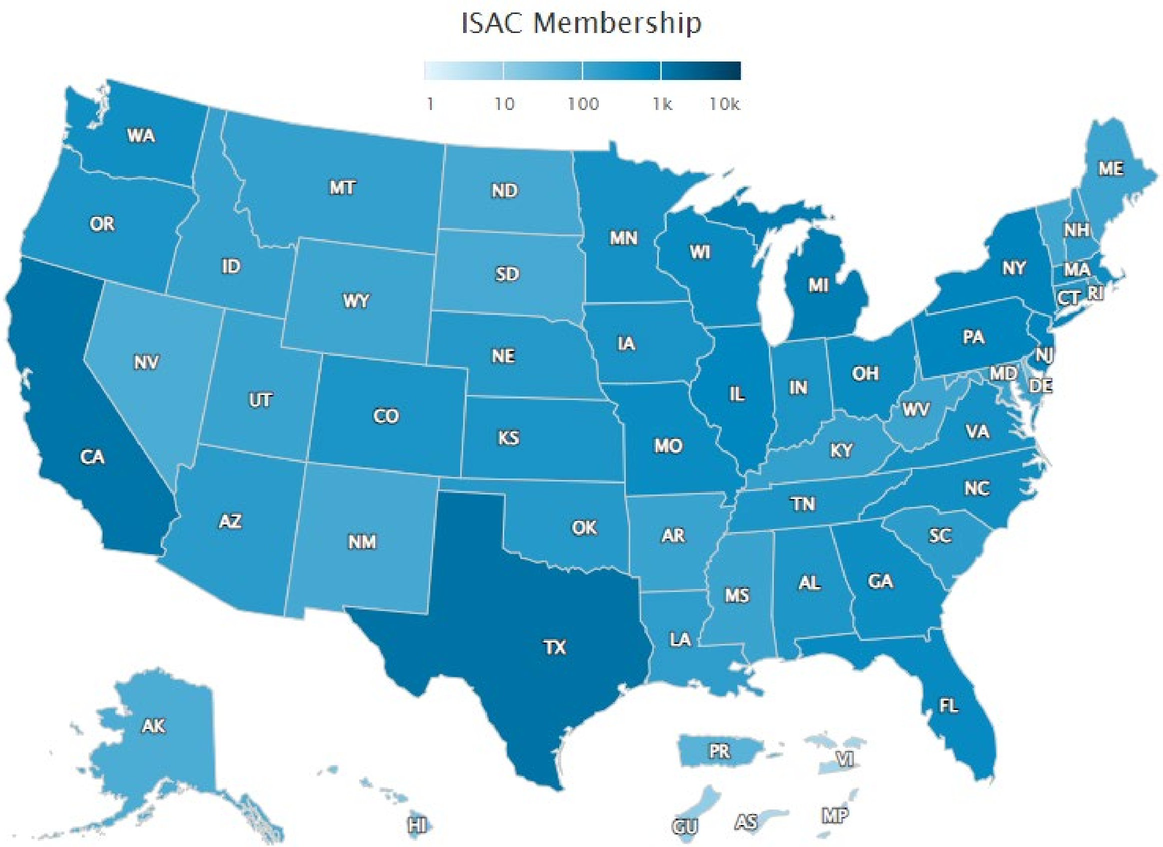
200 Tribal

6 Territory

15,631 Other

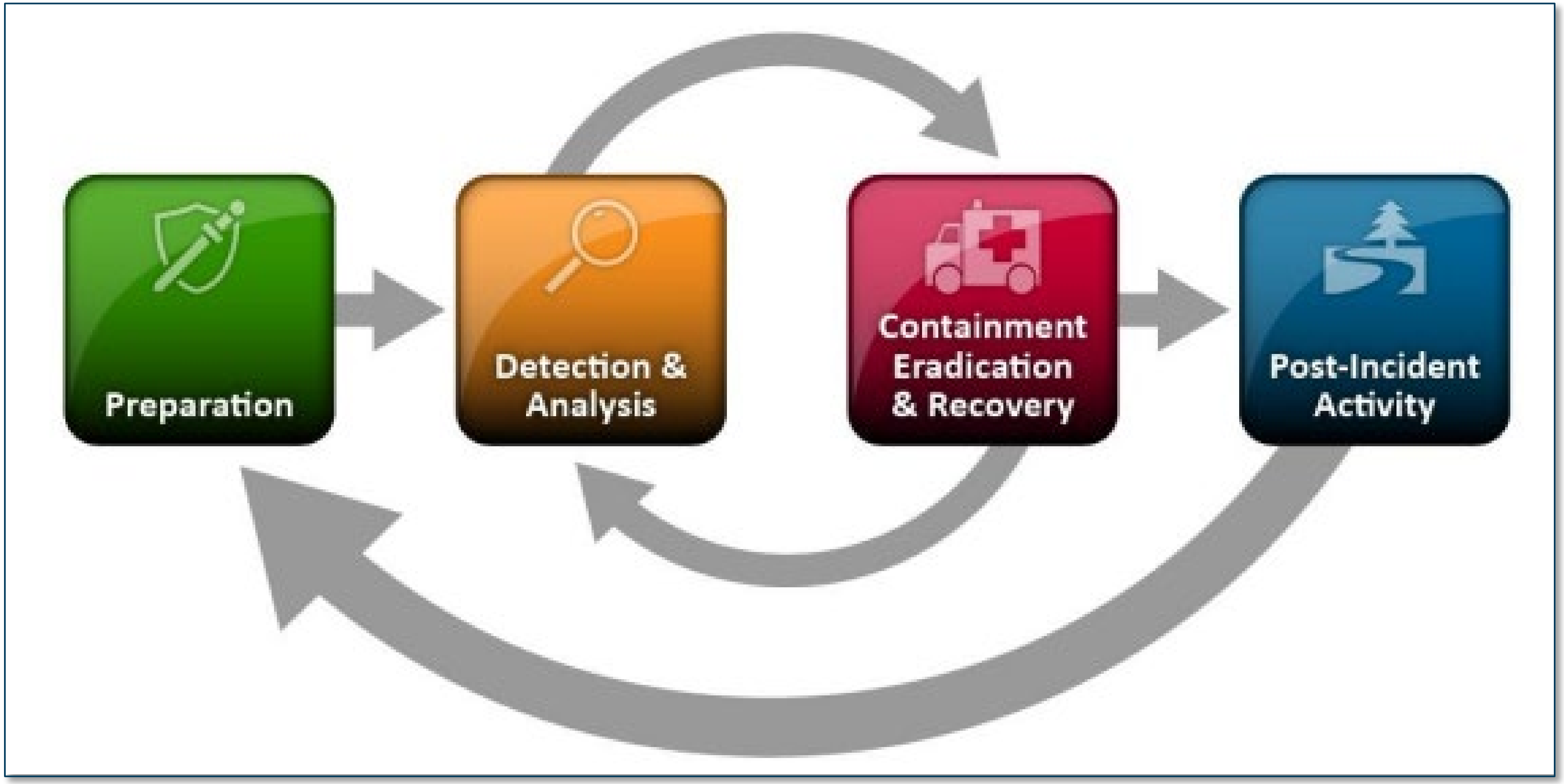


Membership Growth



MS-ISAC®

NIST Incident Response Lifecycle



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

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

Preparation

MS-ISAC: Focused Visibility

Joint #StopRansomware Advisory and K12 Report

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

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

#StopRansomware: Vice Society

K-12 Report

A Cybersecurity Assessment of the 2021-2022 School Year

CIS Center for Internet Security®

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

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

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

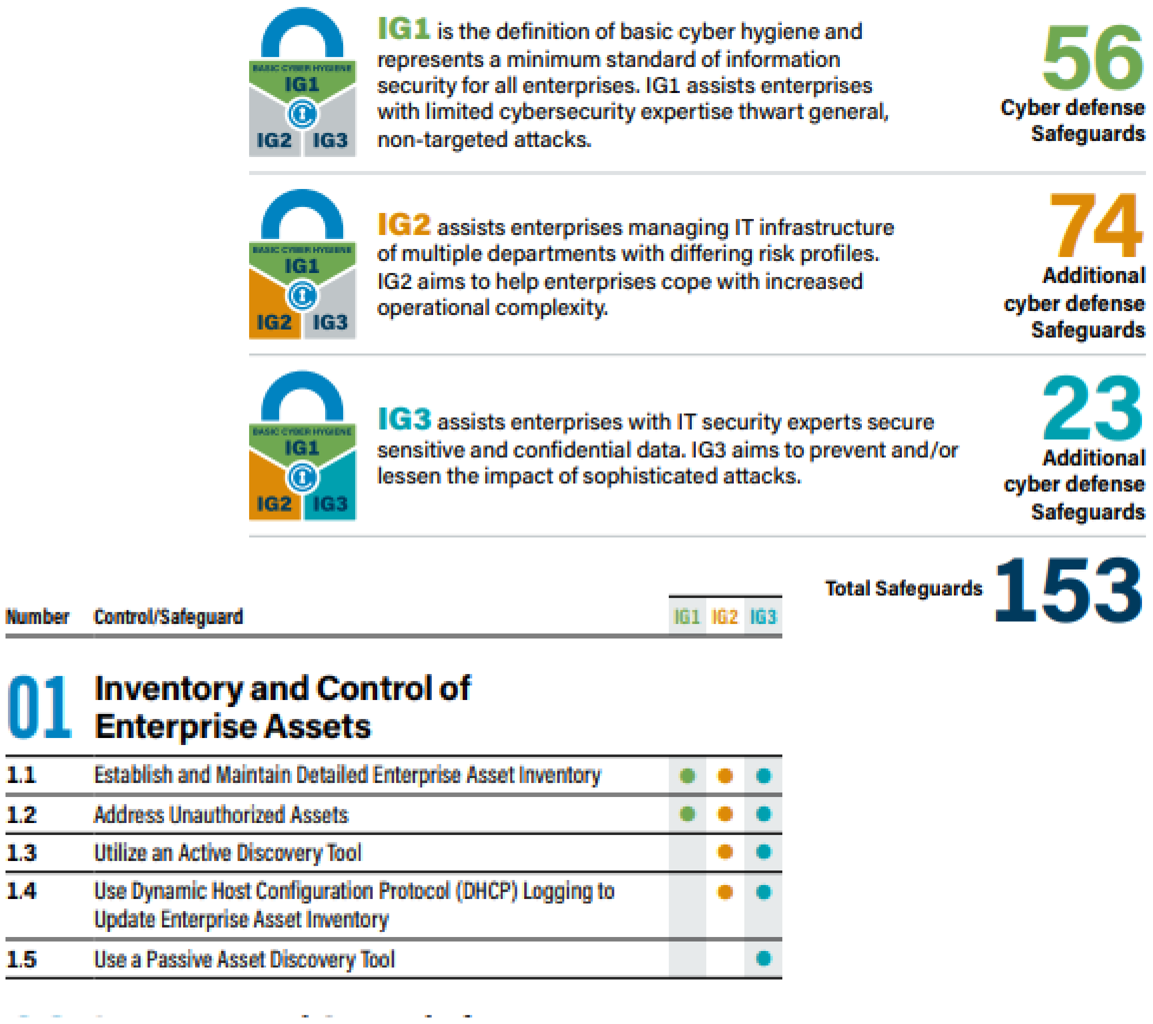
CIS Controls v8

- CONTROL 01 Inventory and Control of Enterprise Assets
- CONTROL 02 Inventory and Control of Software Assets
- CONTROL 03 Data Protection
- CONTROL 04 Secure Configuration of Enterprise Assets and Software
- CONTROL 05 Account Management
- CONTROL 06 Access Control Management
- CONTROL 07 Continuous Vulnerability Management
- CONTROL 08 Audit Log Management
- CONTROL 09 Email and Web Browser Protection
- CONTROL 10 Malware Defenses
- CONTROL 11 Data Recovery
- CONTROL 12 Network Infrastructure
- CONTROL 13 Network Monitoring and Defense
- CONTROL 14 Security Awareness and Skills Training
- CONTROL 15 Service Provider Management
- CONTROL 16 Applications Software Security
- CONTROL 17 Incident Response Management
- CONTROL 18 Penetration Testing

MS-ISAC®

CIS Controls™

- **Implementation Groups (IG) to the CIS Controls:**
  - IG's – are the recommended guidance to prioritize implementation of the CIS Controls.
  - IGs are divided into three groups, based on the risk profile and resources an enterprise has available to them to implement the CIS Controls



IG1	**IG1** is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.	**56** Cyber defense Safeguards
IG2	**IG2** assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.	**74** Additional cyber defense Safeguards
IG3	**IG3** assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.	**23** Additional cyber defense Safeguards

Total Safeguards **153**

Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

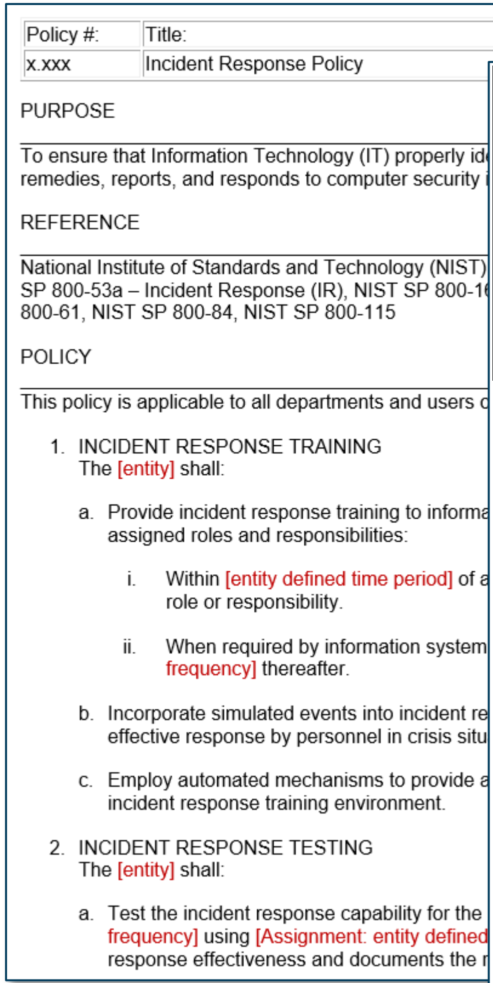
Conduct a Cyber Assessment

What Does an Assessment Tell You?

- **Identifies your current cybersecurity maturity**
- **Highlights areas to prioritize**
- **Assists with creating a 3-5 year roadmap**
- **Get started with a Foundational Assessment**
  - foundationalassessment@cisecurity.org

NATIONWIDE
CYBERSECURITY
REVIEW

Do You Have a Plan?



Policy #:	Title:	Effective Date:
x.xxx	Incident Response Policy	MM/DD/YY

PURPOSE

To ensure that Information Technology (IT) properly id
remedies, reports, and responds to computer security i

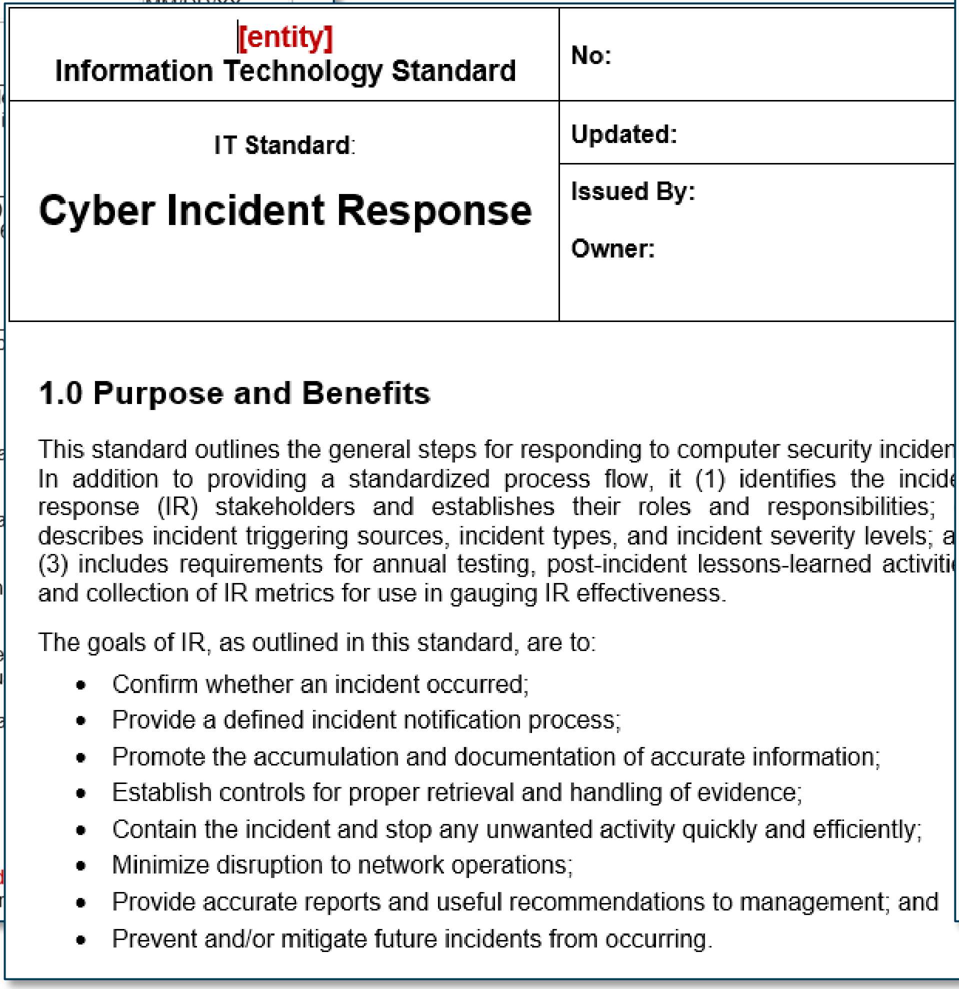
REFERENCE

National Institute of Standards and Technology (NIST)
SP 800-53a – Incident Response (IR), NIST SP 800-1
800-61, NIST SP 800-84, NIST SP 800-115

POLICY

This policy is applicable to all departments and users o

1. INCIDENT RESPONSE TRAINING
   The [entity] shall:
   a. Provide incident response training to informa
      assigned roles and responsibilities:
      i. Within [entity defined time period] of a
         role or responsibility.
      ii. When required by information system
          frequency] thereafter.
   b. Incorporate simulated events into incident re
      effective response by personnel in crisis situ
   c. Employ automated mechanisms to provide a
      incident response training environment.
2. INCIDENT RESPONSE TESTING
   The [entity] shall:
   a. Test the incident response capability for the
      frequency] using [Assignment: entity defined
      response effectiveness and documents the r



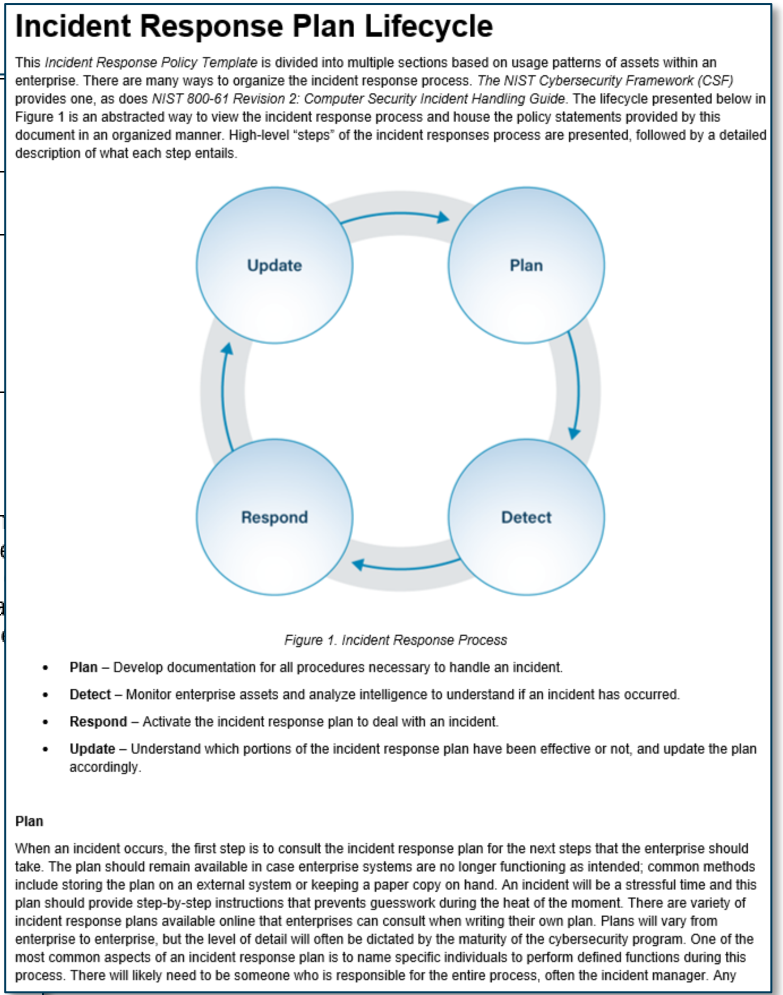
[entity] **Information Technology Standard**	**No:**
IT Standard: **Cyber Incident Response**	**Updated:** **Issued By:** **Owner:**

1.0 Purpose and Benefits

This standard outlines the general steps for responding to computer security inciden
In addition to providing a standardized process flow, it (1) identifies the incide
response (IR) stakeholders and establishes their roles and responsibilities;
describes incident triggering sources, incident types, and incident severity levels; a
(3) includes requirements for annual testing, post-incident lessons-learned activiti
and collection of IR metrics for use in gauging IR effectiveness.

The goals of IR, as outlined in this standard, are to:

- Confirm whether an incident occurred;
- Provide a defined incident notification process;
- Promote the accumulation and documentation of accurate information;
- Establish controls for proper retrieval and handling of evidence;
- Contain the incident and stop any unwanted activity quickly and efficiently;
- Minimize disruption to network operations;
- Provide accurate reports and useful recommendations to management; and
- Prevent and/or mitigate future incidents from occurring.



Incident Response Plan Lifecycle

This *Incident Response Policy Template* is divided into multiple sections based on usage patterns of assets within an enterprise. There are many ways to organize the incident response process. *The NIST Cybersecurity Framework (CSF)* provides one, as does *NIST 800-61 Revision 2: Computer Security Incident Handling Guide*. The lifecycle presented below in Figure 1 is an abstracted way to view the incident response process and house the policy statements provided by this document in an organized manner. High-level "steps" of the incident responses process are presented, followed by a detailed description of what each step entails.

Figure 1. Incident Response Process

- **Plan** – Develop documentation for all procedures necessary to handle an incident.
- **Detect** – Monitor enterprise assets and analyze intelligence to understand if an incident has occurred.
- **Respond** – Activate the incident response plan to deal with an incident.
- **Update** – Understand which portions of the incident response plan have been effective or not, and update the plan accordingly.

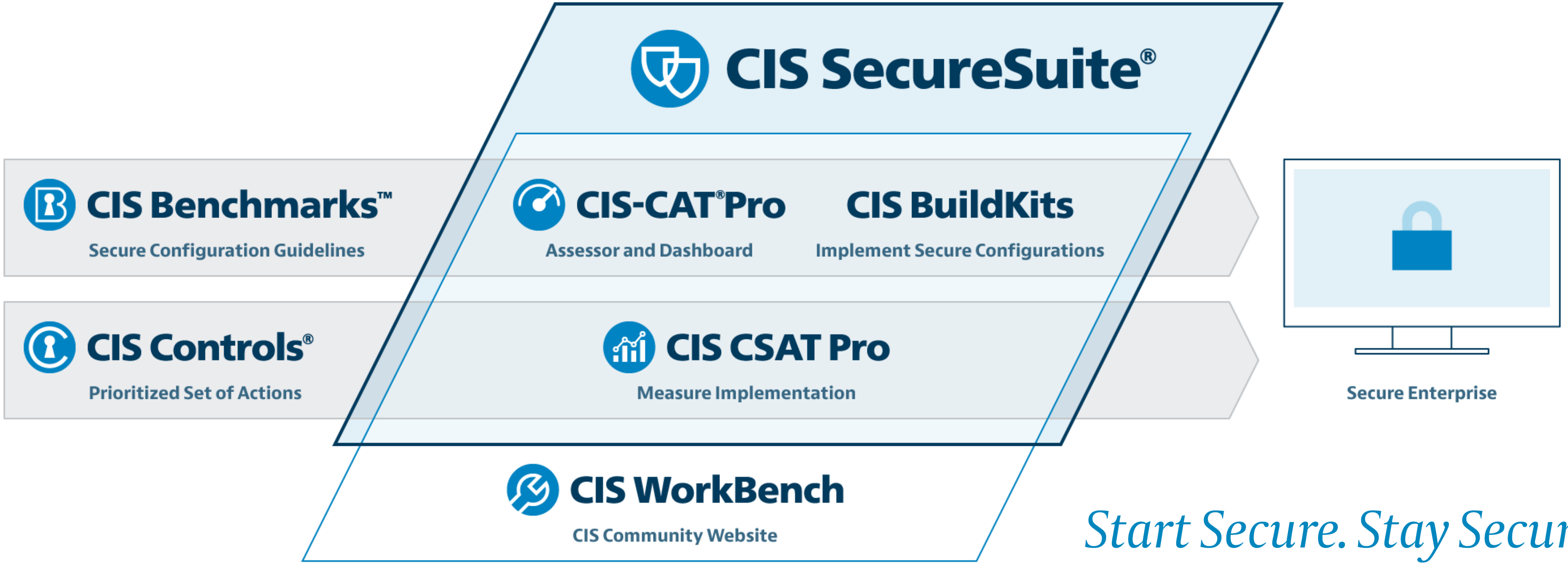
Plan

When an incident occurs, the first step is to consult the incident response plan for the next steps that the enterprise should take. The plan should remain available in case enterprise systems are no longer functioning as intended; common methods include storing the plan on an external system or keeping a paper copy on hand. An incident will be a stressful time and this plan should provide step-by-step instructions that prevents guesswork during the heat of the moment. There are variety of incident response plans available online that enterprises can consult when writing their own plan. Plans will vary from enterprise to enterprise, but the level of detail will often be dictated by the maturity of the cybersecurity program. One of the most common aspects of an incident response plan is to name specific individuals to perform defined functions during this process. There will likely need to be someone who is responsible for the entire process, often the incident manager. Any

MS-ISAC®

CIS SecureSuite®

FreeSecureSuite@cisecurity.org



CIS SecureSuite®

CIS Benchmarks™
Secure Configuration Guidelines

CIS-CAT®Pro
Assessor and Dashboard

CIS BuildKits
Implement Secure Configurations

CIS Controls®
Prioritized Set of Actions

CIS CSAT Pro
Measure Implementation

CIS WorkBench
CIS Community Website

Secure Enterprise

Start Secure. Stay Secure.®

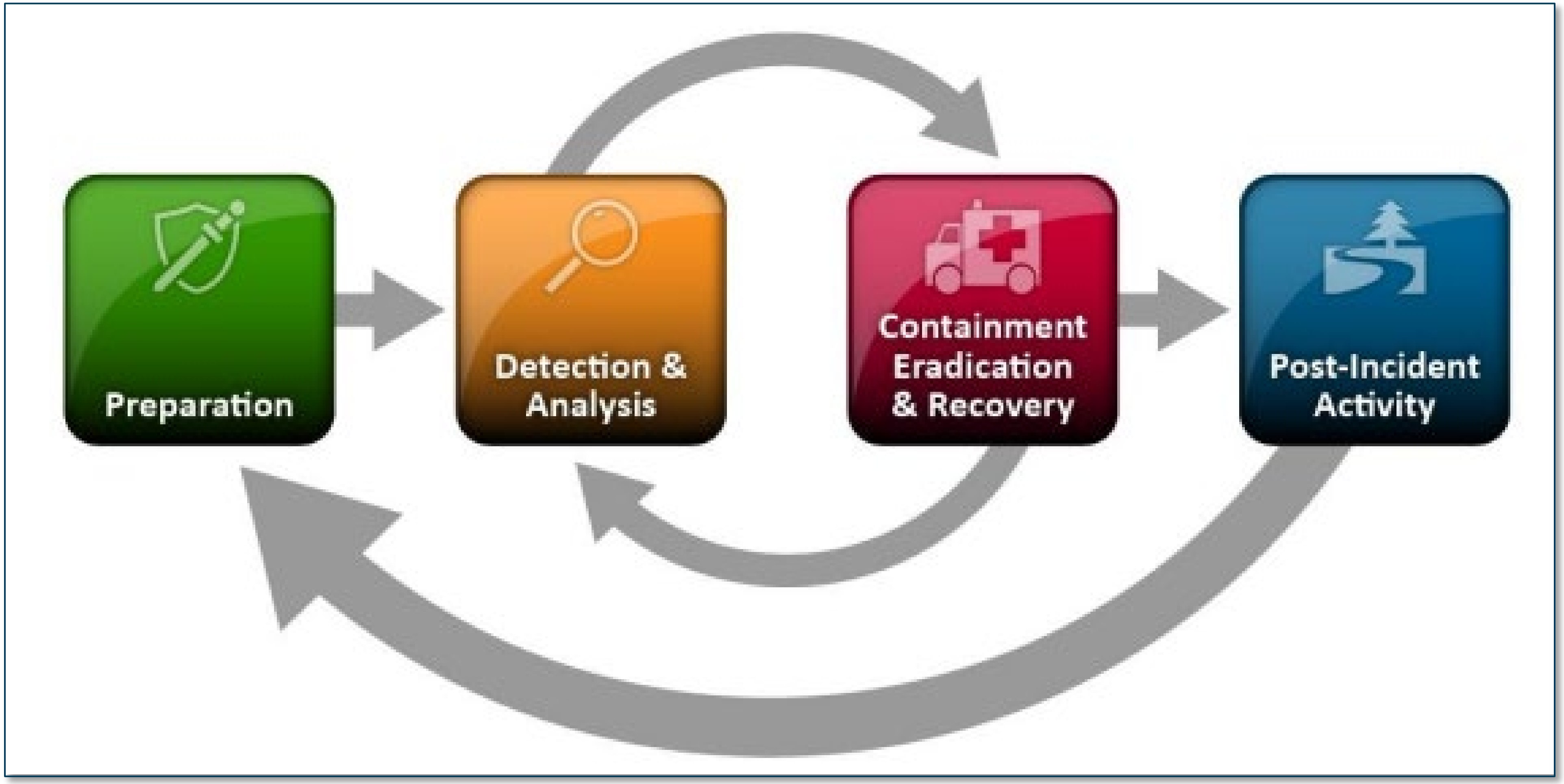
https://www.cisecurity.org/cis-securesuite/member-webinars

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

Detection and Analysis

Confidential & Proprietary

NIST Incident Response Lifecycle



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

MS-ISAC®

Security Operations Center

24x7x365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises

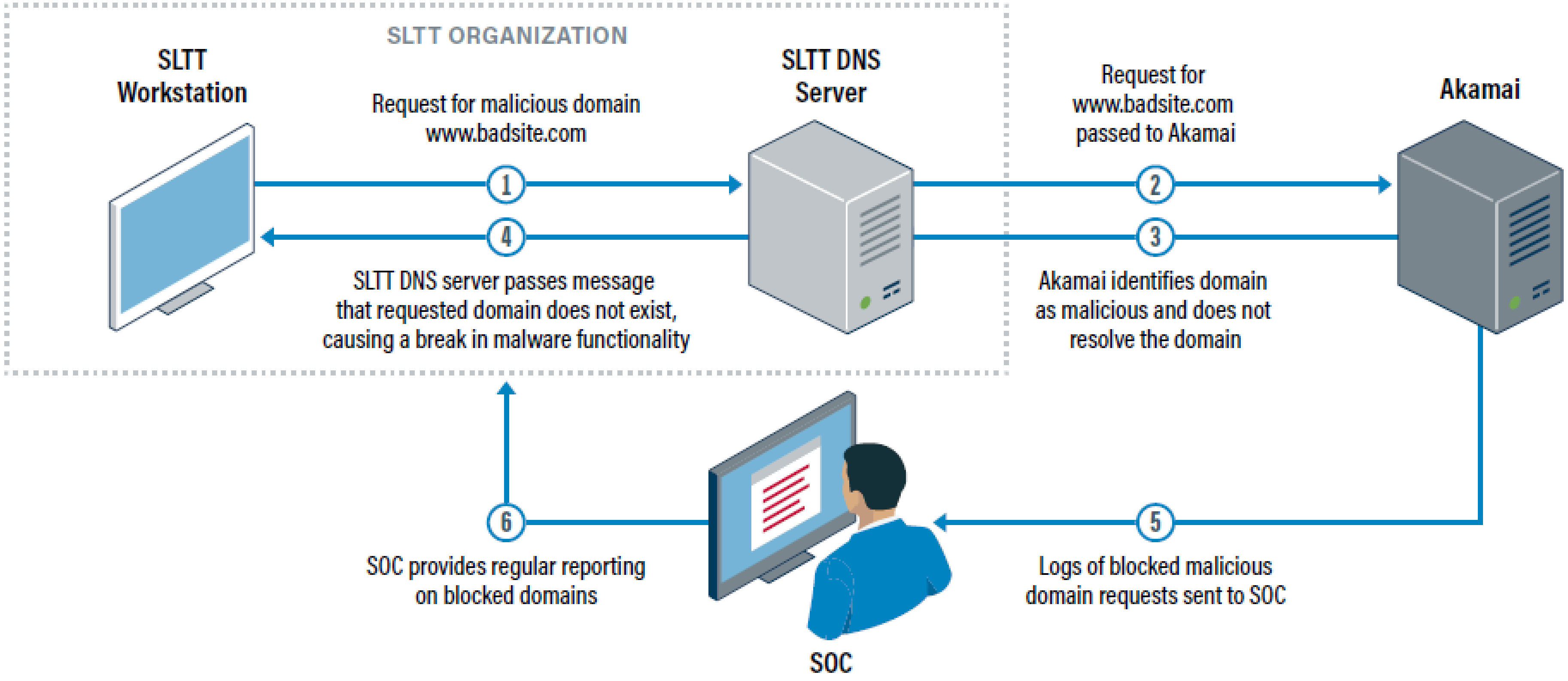
To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Malicious Domain Blocking and Reporting (MDBR)

↓ Malicious Domain Blocking and Reporting Data Flow



1. Request for malicious domain www.badsite.com
2. Request for www.badsite.com passed to Akamai
3. Akamai identifies domain as malicious and does not resolve the domain
4. SLTT DNS server passes message that requested domain does not exist, causing a break in malware functionality
5. Logs of blocked malicious domain requests sent to SOC
6. SOC provides regular reporting on blocked domains

MS-ISAC®

Malicious Code Analysis Platform (MCAP)

A web based service used to submit and analyze suspicious files

To request an account:
mcap@cisecurity.org

- Executables
- DLLs
- Documents
- URLs
- Archives

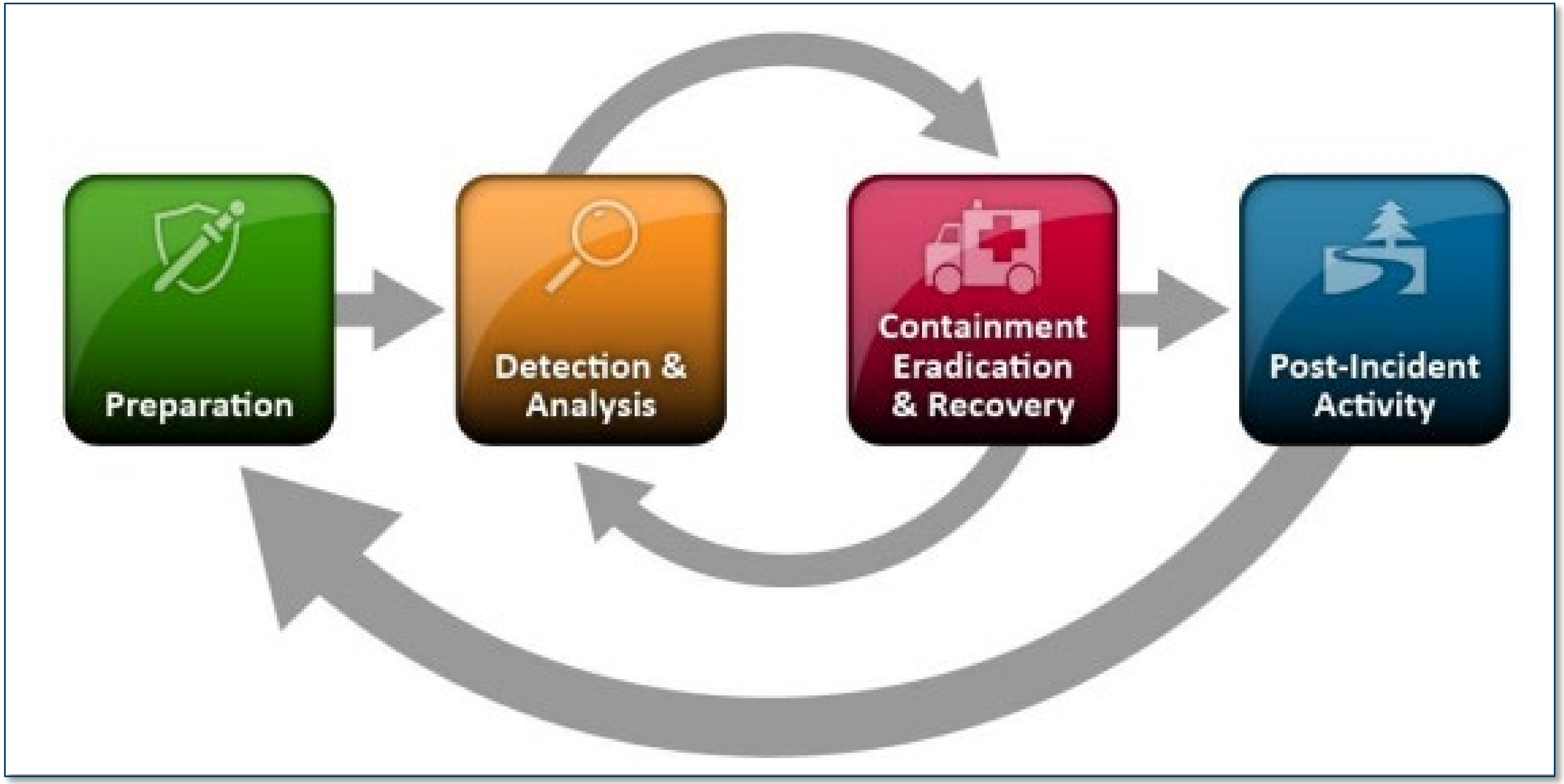
MS-ISAC®

Multi-State Information
Sharing & Analysis Center®

Containment and Eradication

Confidential & Proprietary

NIST Incident Response Lifecycle



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

What is Cyber Incident Response?

SOC@cisecurity.org

- Digital Forensics
- Log Review
- Device Triage
- Monitoring
- Mitigation

Elements of Cyber Incident Response

- Scope of Impact
- Incident Timeline
- Root Cause
- Remediation Recommendations
- Lessons Learned

Goals of Cyber Incident Response

MS-ISAC®

Cyber Incident Response Team (CIRT)

What to Report

Incident Response Checklist Tips

- Who experienced the incident
- What sort of incident occurred
- How and when the incident was initially detected
- What response actions have already been taken
- Who has been notified

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Snapshot of a Cyber Incident

soc@cisecurity.org

What Happened?

July 2022, a MS-ISAC member 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 data to understand threat actor actions and IOCs; provided scripts to the member to determine if identified IOCs were present; also provided guidance to assist with ongoing recovery efforts.

The Impact

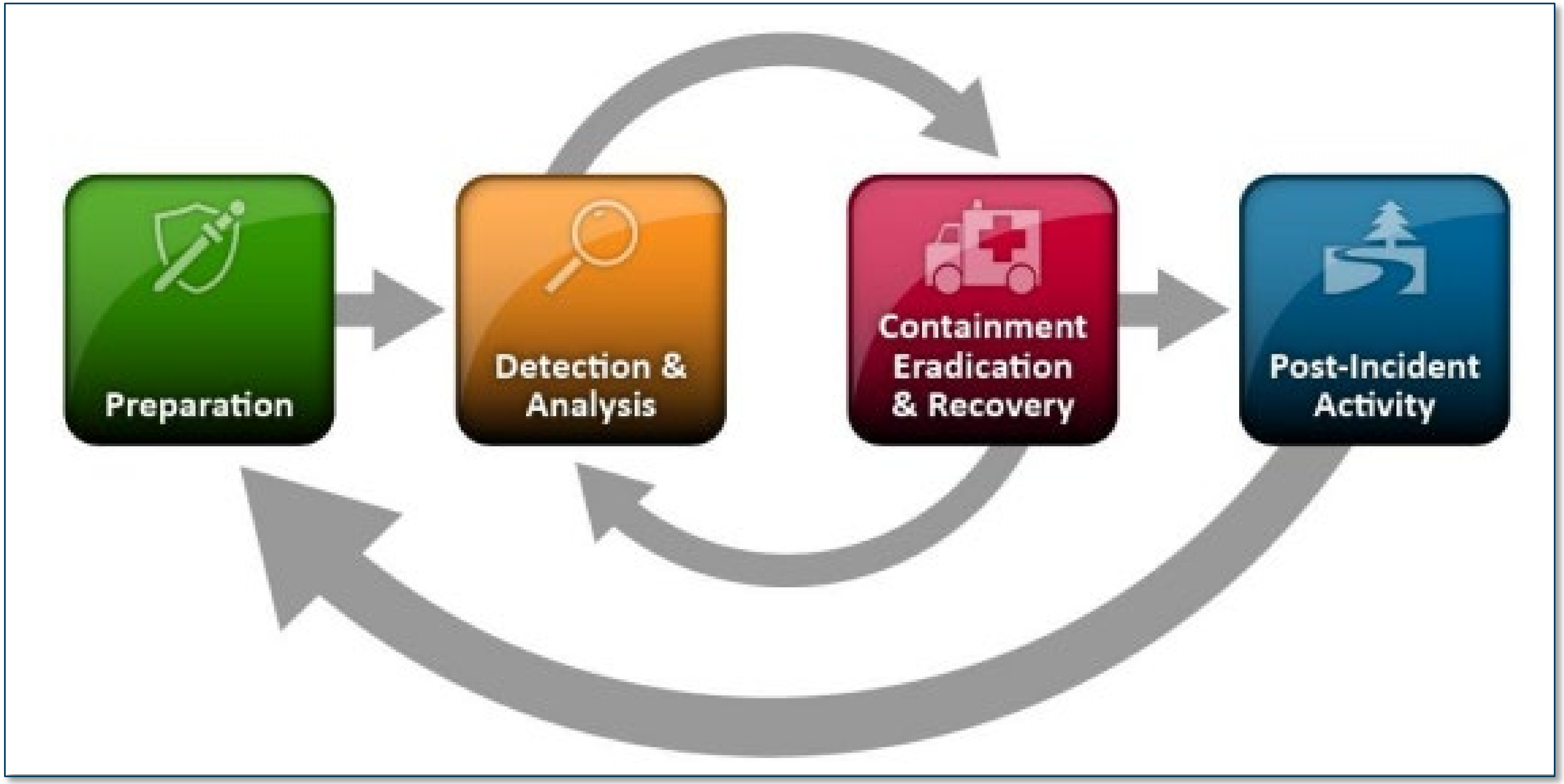
The member said MS-ISAC response was instrumental in understanding the incident timeline, developing IOCs, and obtaining necessary guidance to help restore the network.

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

Post Incident Activity

Confidential & Proprietary

NIST Incident Response Lifecycle



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Post Incident Checklist

Lessons Learned

- How well did the policy/plan work?
- What could have been done better?
- Who was missing from the contact list?
- What is needed to prepare better for next time?
- **Root Cause Analysis**
  - Who, What, Where, Why, How the incident happened?

Recommendations

What to do Today, Tomorrow and Beyond

- **Today**: Join an ISAC
  - MS-ISAC: https://learn.cisecurity.org/ms-isac-registration
- **Tomorrow**: Establish an Incident Response (IR) and Data Backup plan
  - *CIS Control #17: https://learn.cisecurity.org/cis-controls-download*
- **Next Week**: Obtain vulnerability scans and/or enroll in MDBR
  - *https://www.cisa.gov/cyber-hygiene-services*
  - *https://www.cisecurity.org/ms-isac/services/mdbr*
- **Future**: Review the CISA-MS-ISAC Joint Ransomware Guide
  - *https://www.cisa.gov/resources-tools/resources/stopransomware-guide*

ANY QUESTIONS?

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

Thank You!

Megan Incerto

Regional Engagement Manager, MS-ISAC

Megan.Incerto@cisecurity.org | *518-640-3655*

Confidential & Proprietary