

# CYBERSECURITY RESOURCES

## Joseph Flores

Cyber Security Advisor (CSA) for Massachusetts  
Cybersecurity and Infrastructure Security Agency (CISA)



CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY

# Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP  
DEVELOPMENT



INFORMATION AND  
DATA SHARING



CAPACITY BUILDING



INCIDENT  
MANAGEMENT  
& RESPONSE



RISK ASSESSMENT  
AND ANALYSIS



















NETWORK DEFENSE



EMERGENCY  
COMMUNICATIONS

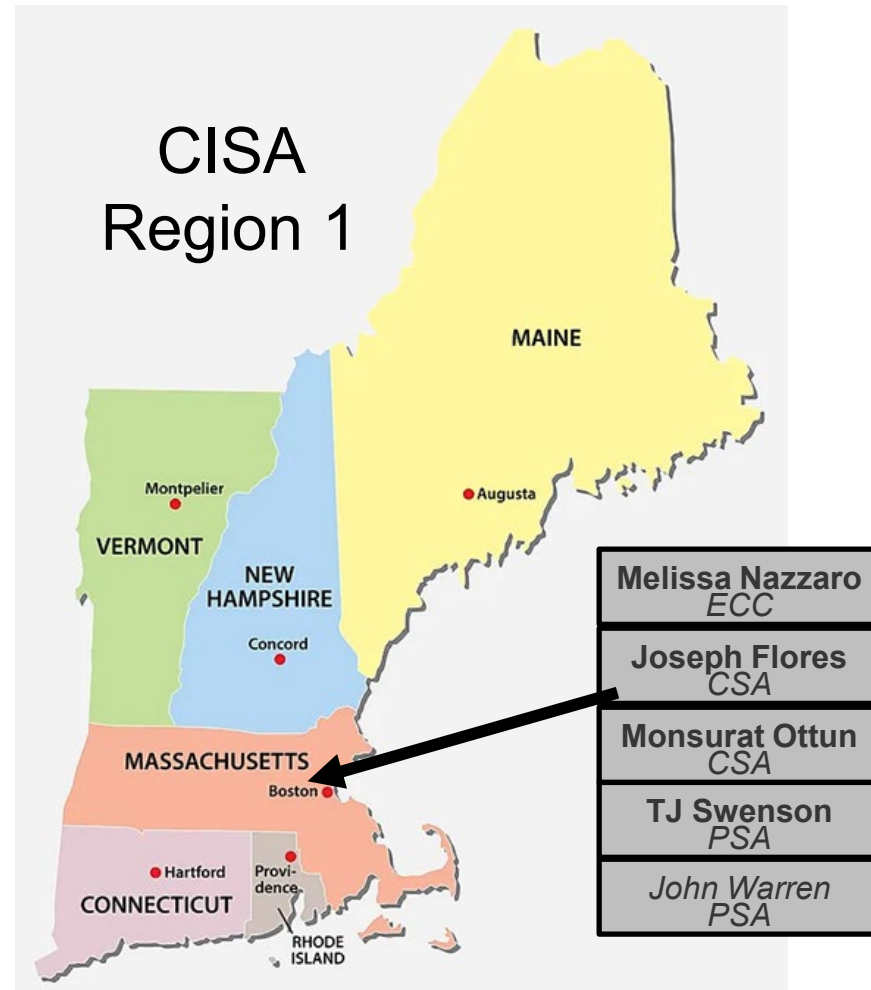
# 16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

# Local Resources

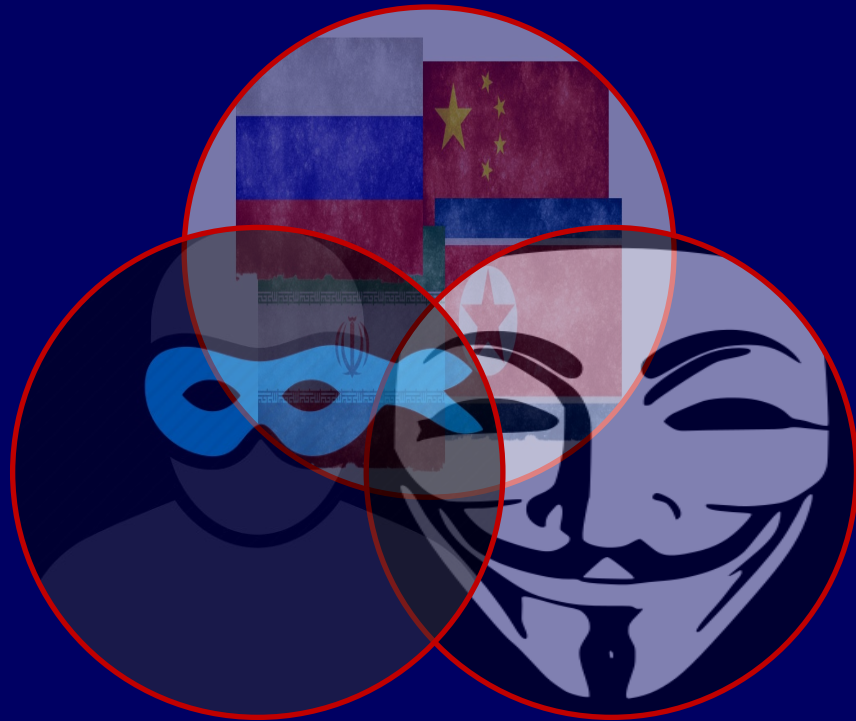
In support of the mission, CISA has assigned Cyber Security Advisors (CSAs), Protective Security Advisors (PSAs), Emergency Communications Coordinators (ECCs) to each state. Their role is to:

- Develop and maintain relationships with public and private sector critical infrastructure entities and serve as a link to CISA's resources.
- Conduct and coordinate assessments, training, and other DHS products and services.
- Provide a vital link for information sharing in steady state and incident response.

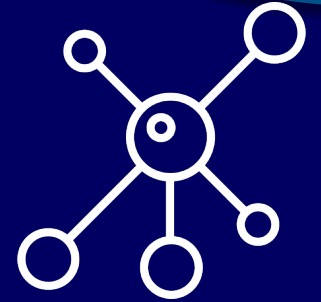


Joseph Flores  
November 12, 2024

# Global Cyber Threat Environment Themes



- Data as a Commodity
- Interconnected Systems Increase Threat Environment
- Remote Monitoring and Management Tools (Remoting in)
- Operational Technology Issues/ IOT (Integrators)
- Artificial Intelligence
- Insider Threats
  
- Hacking as a Service (HaaS)
  - Ransomware, DDOS Attacks
  - Initial Access Brokers
- Software Vulnerabilities (patching lag)
- Ubiquity of Malicious Tools
  - Ease of Use
  - Destructive Capabilities
- 3<sup>rd</sup> Party Software Risks
- Cloud Sprawl/Risk
- Supply Chain Campaigns and Zero Day Markets
  - External Dependency Management



# Understanding your Threats

## Motives Abound!

### Advanced Persistent Threats

#### Motive:

Persistence (preparation for future disruption/destruction)

Strategic Advantages

Espionage

### Grey Middle

- Gov/Ransomware Group Integration

### Ransomware Groups

#### Motive:

Money

Money

Money

Possibly Power/Stature/PR but leading back to Money

### Insider Threats:

#### Motive:

Money

Anger

Retribution

Earn Cred with a future position



# Example Educational Sector Critical Assets

## People

Students, Administration, Communities

## Infrastructure and Facilities

School Campuses, Buses, Transportation Vehicles, Sports and Recreation Facilities

Labs, Work Centers, and Workshops / “Shops”



## Data & Information

Personally Identifiable Information (PII): Names, Addresses, Social Security Numbers, Course & Transportation Schedules, and Contact Information

Personal Health Information (PHI): Medical records, treatment plans

Financial Information: Staff payroll, accounting, student payment / lunch accounts

Policies and Procedures: Security Policies, Student Disciplinary Measures

## Technology

Hardware: Computers, Servers, Communication Equipment, Smart Classroom Devices (Projectors, Boards, etc.), Power Supply Equipment, HVAC equipment, physical security equipment (cameras, metal detectors, alarms/alert systems), mass/emergency notification systems

Network: Wired and Wireless– Firewalls, DMZ, Routers, Switches



# You have a lot going on

## Platforms supported

### Cloud



### Application



### Server



### Desktop



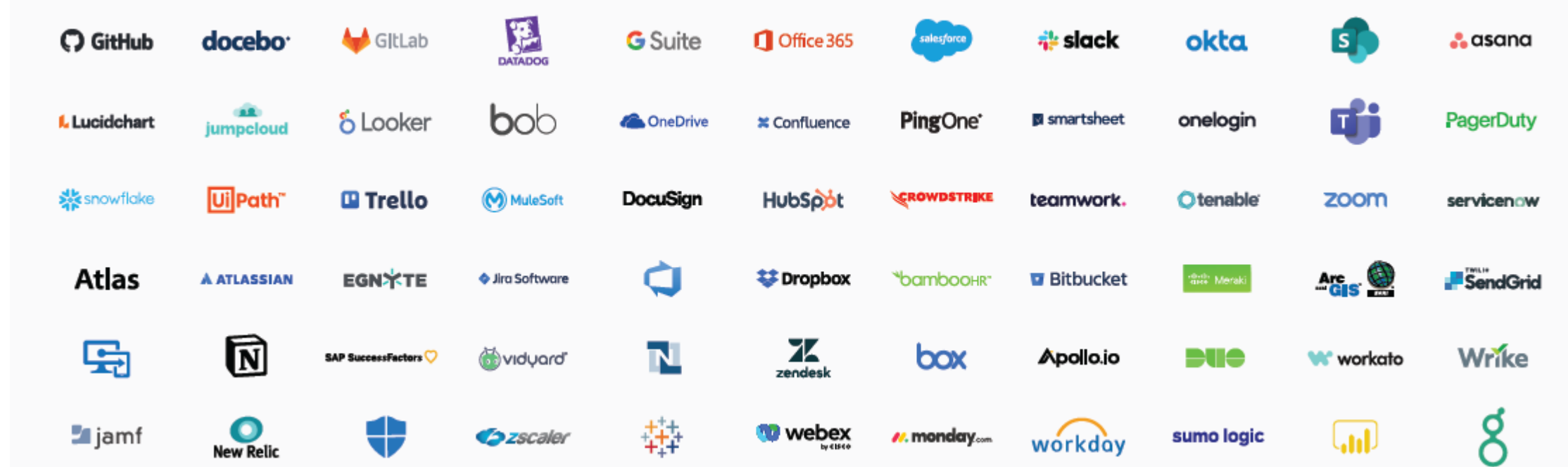
### Application Server



### Network devices



### Database





# CISA Services



# CISA Assessments

CISA assessments and cybersecurity services are available at **no cost** to Critical Infrastructure partners.

CISA does not share attributable information without written and agreed consent from the stakeholder.

## PROTECTED CRITICAL INFRASTRUCTURE INFORMATION Requirements for Use

This document contains Protected Critical Infrastructure Information (PCII). In accordance with the provisions of the Critical Infrastructure Information Act of 2002 (the “CII Act”), (6 U.S.C. §671- 674), PCII is exempt from release under the Freedom of Information Act (5 U.S.C. §552) and similar State and local disclosure laws. Unauthorized release may result in criminal and administrative penalties. Safeguard and disseminate in accordance with the CII Act, the implementing Regulation at 6 C.F.R. Part 29 (the “Regulation”) and PCII Program requirements.

**By reviewing this cover sheet and accepting the attached PCII you are agreeing not to disclose it to other individuals without following the access requirements and to abide by the guidance contained herein. Your acceptance provides immediate access only to the attached PCII.**

**If not a PCII Authorized User, you are required to complete the training within 30 days of receipt of this information.**

Go to <https://www.cisa.gov/pcii-authorized-user-training> for training. Contact [pcii-assist@hq.dhs.gov](mailto:pcii-assist@hq.dhs.gov) for assistance.

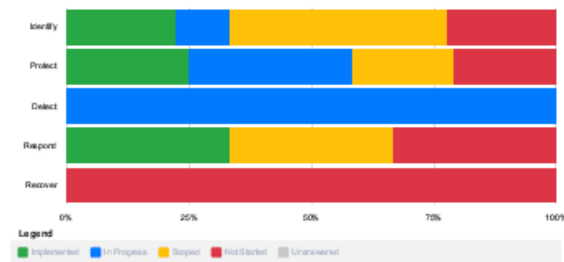


## CYBERSECURITY PERFORMANCE GOALS (CPG)



### Performance Summary

This chart shows the answer distribution for each of the Security Practice categories.



### Chart Detail

This table indicates the answer distribution percentages for each category as indicated in the chart above.

Category	Implemented	In Progress	Scoped	Not Started	Unanswered
Identify	22.22%	11.11%	44.44%	22.22%	0.00%
Protect	25.00%	33.33%	20.83%	20.83%	0.00%
Detect	0.00%	100.00%	0.00%	0.00%	0.00%
Respond	33.33%	0.00%	33.33%	33.33%	0.00%
Recover	0.00%	0.00%	0.00%	100.00%	0.00%

- Ransomware Resiliency Assessment (RRA)
  - NIST Cybersecurity Framework
  - Network Diagram/Components Based Assessment
  - CISA CRR/CIS/EDM Maturity Level Assessments
  - New Minimum Viable Resilience Assessment (MVRA)-Draft
  - Many More...
- Provides a systematic, disciplined, and repeatable method for assessing infrastructure;
  - Controls priority list provided using feedback from cybersecurity experts on actual reported incidents;
  - Compare multiple assessments to establish a baseline and determine trends;
  - Saves significant time and money by eliminating the need to research each government and industry standard in order to understand your cybersecurity posture;
  - Includes professionally designed reports and a customized System Security Plan based upon the results of the assessment;



# Cybersecurity Assessments



# Assessment Results

## DOMAIN 1: ASSET MANAGEMENT



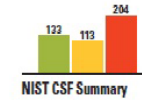
The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 - Identify & prioritize critical services
- Goal 2 - Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 - Establish the relationship between assets and the services they support
- Goal 4 - Manage the asset inventory
- Goal 5 - Manage access to assets
- Goal 6 - Prioritize & manage information assets
- Goal 7 - Prioritize & manage facility assets

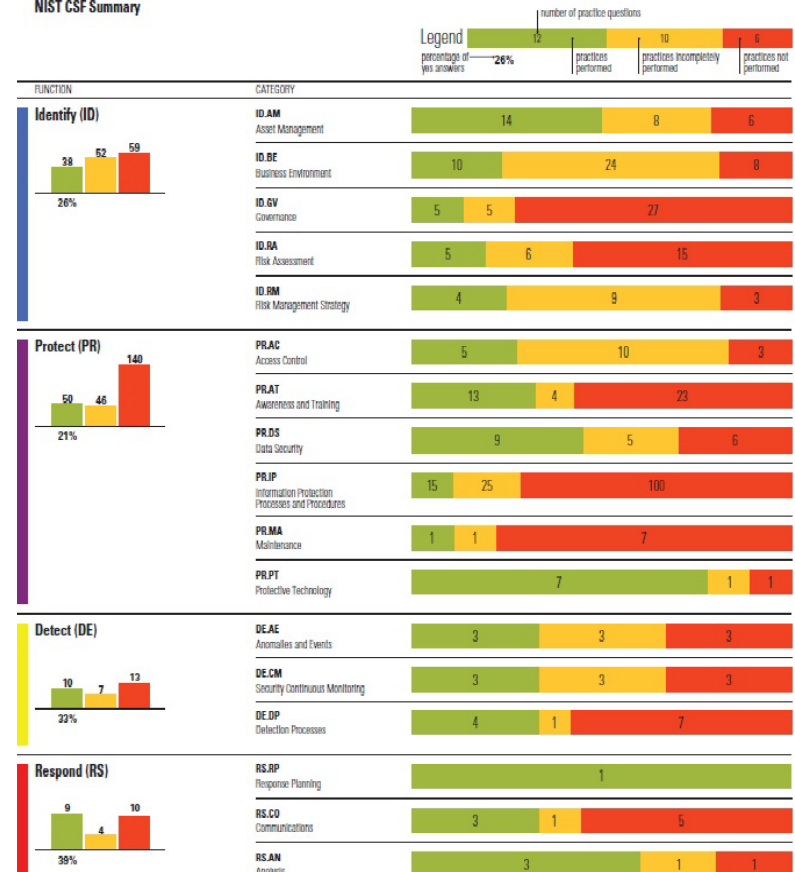
The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 - Identify & prioritize services.		
1.	Are services identified? [SC:SG2.SP1]	Yes
2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	Incomplete
Option(s) for Consideration:		
Q1	Additional Reference: NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	
Q2	CERT-RMM Reference: [SC:SG4.SP1] Prioritize and document the list of critical services that must be provided if a disruption occurs. Consideration of the consequences of the loss of critical organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to critical services are identified and analyzed in risk assessment activities. The organization must consider this information when prioritizing high-value services. Additional Reference: NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 16-18)	

Goal 2 - Inventory assets, and establish the authority and responsibility for these assets.		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Yes
	Information	Yes
	Technology	Yes
	Facilities	Yes
2.	Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Incomplete
3.	Do asset descriptions include both owners and custodians of assets? [ADM:SG1.SP3]	
	People	Yes



## NIST Cybersecurity Framework Summary



# HQ Shared Cyber Services

- Cyber Hygiene Scanning (CyHy)
- Web Application Scanning (WAS)
- Remote Penetration Testing (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)
- Validated Architecture Design (VADR)

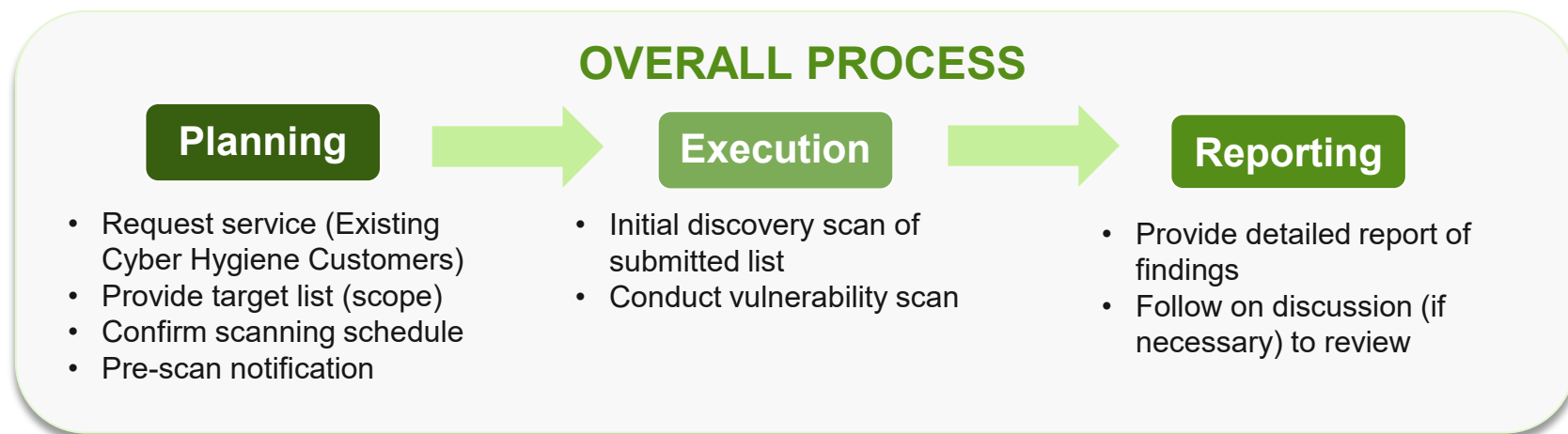
CyHy Scanning is the only **Highly Scalable Service**.

**Ask your CSA about the potential and availability of the other services if interested.**

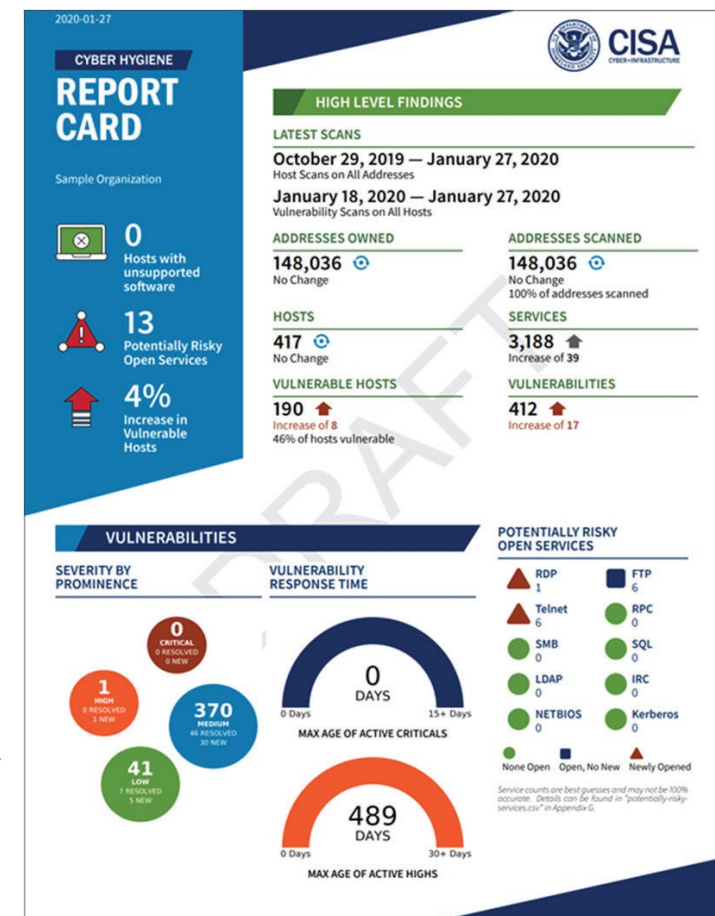


# Cyber Hygiene (CyHy) Scanning...and WAS

Continually assess Internet-accessible systems for known vulnerabilities and provide actionable reports to partners. Can also do web application scanning.

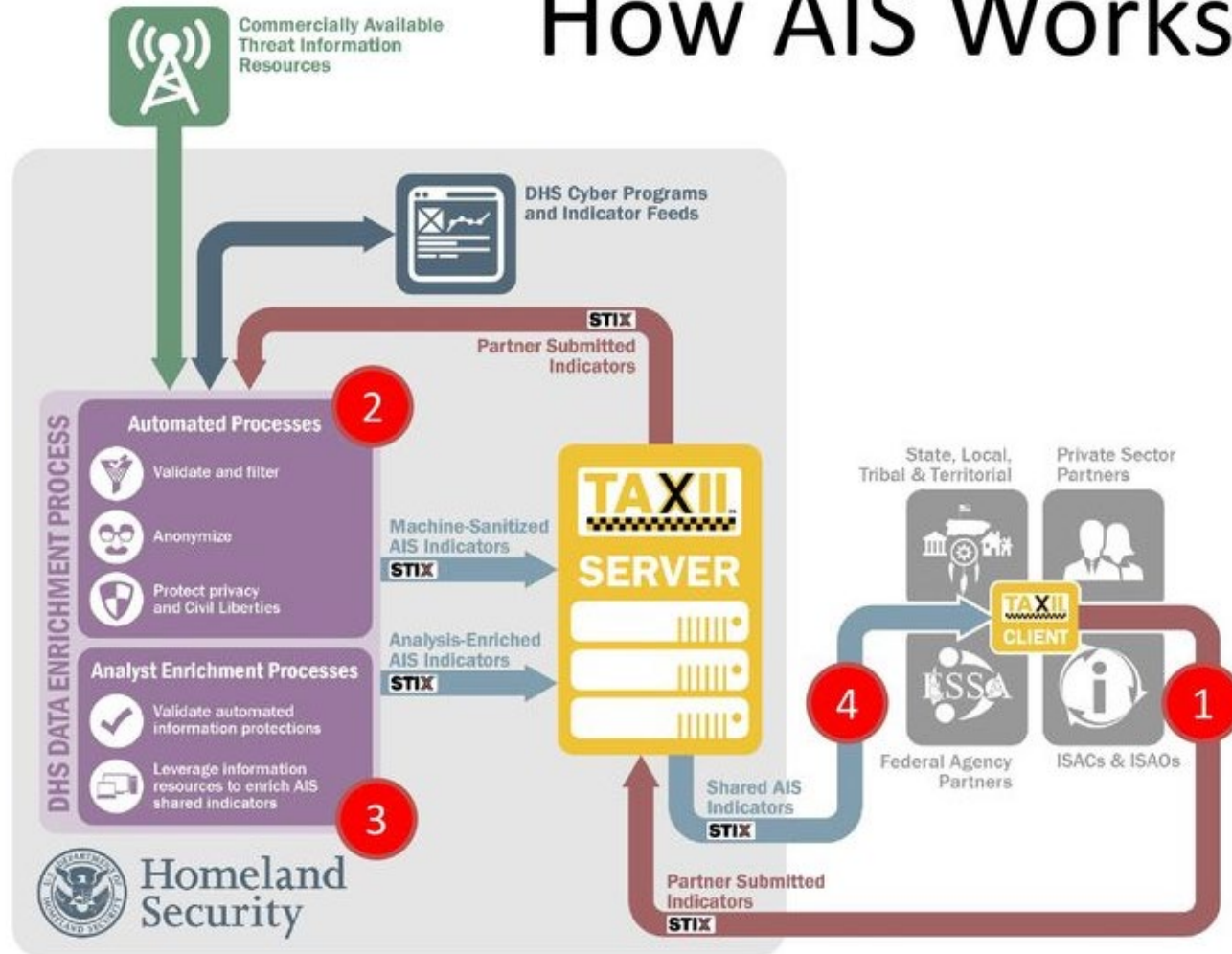


Email us at [vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov) with the subject line “Requesting Cyber Hygiene Services” to get started.



# Automated Indicator Sharing (AIS):

## How AIS Works

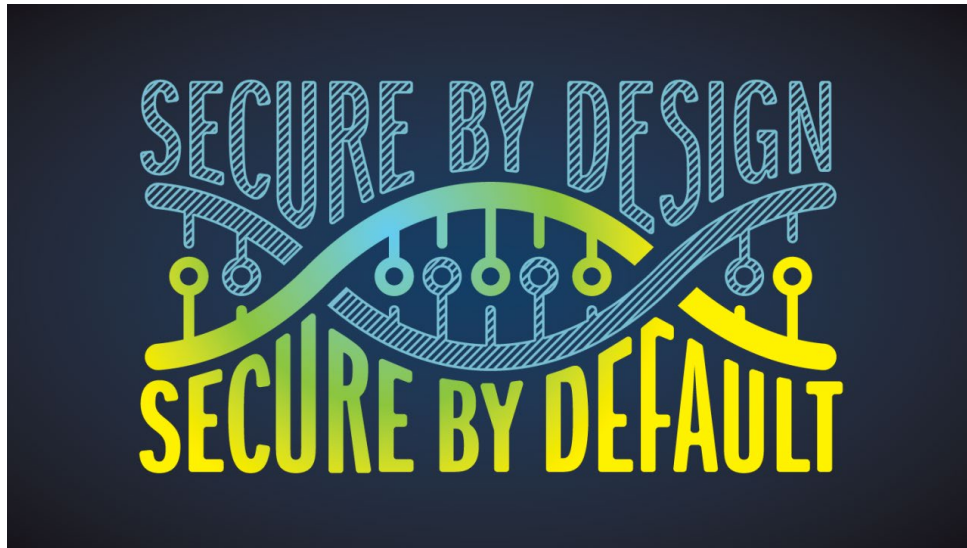


1. Entities format cyber threat indicators in STIX and submit via TAXII to DHS server.
2. Server code reviews submission to validate, anonymize (if requested), conduct automated privacy review and enrich.
3. Indicators requiring review go to DHS analysts.
4. Finally, indicators are published back out to everyone connected to the





# Supply Chain Risk Management



OTHER

Secure Software Development  
Attestation Form

Revision Date: March 18, 2024

PUBLICATION

Vendor Supply Chain Risk  
Management (SCRM) Template

Publish Date: April 12, 2021



# Leveraging the .gov Top-level Domain

## WELL-KNOWN



CISA administers the .gov top-level domain (TLD) which is used by all three branches of the US government and all 50 states.

## TRUSTED



- Having a .gov domain helps the public quickly identify your website as an official and trusted source of information.
- Having a .gov domain makes it more difficult for malicious cyber actors to impersonate you.
- It's free to register.

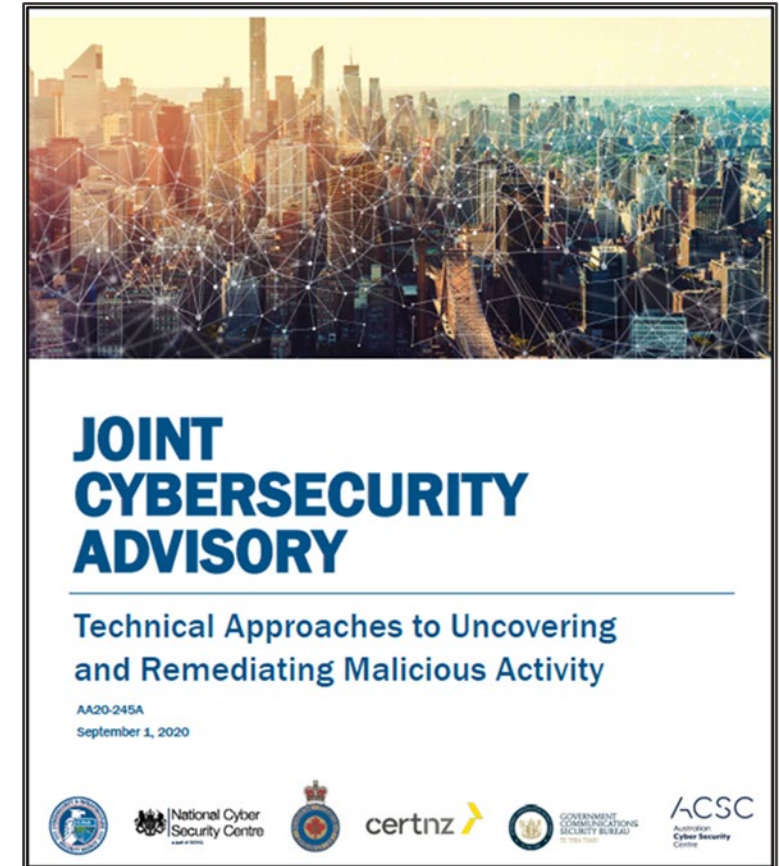
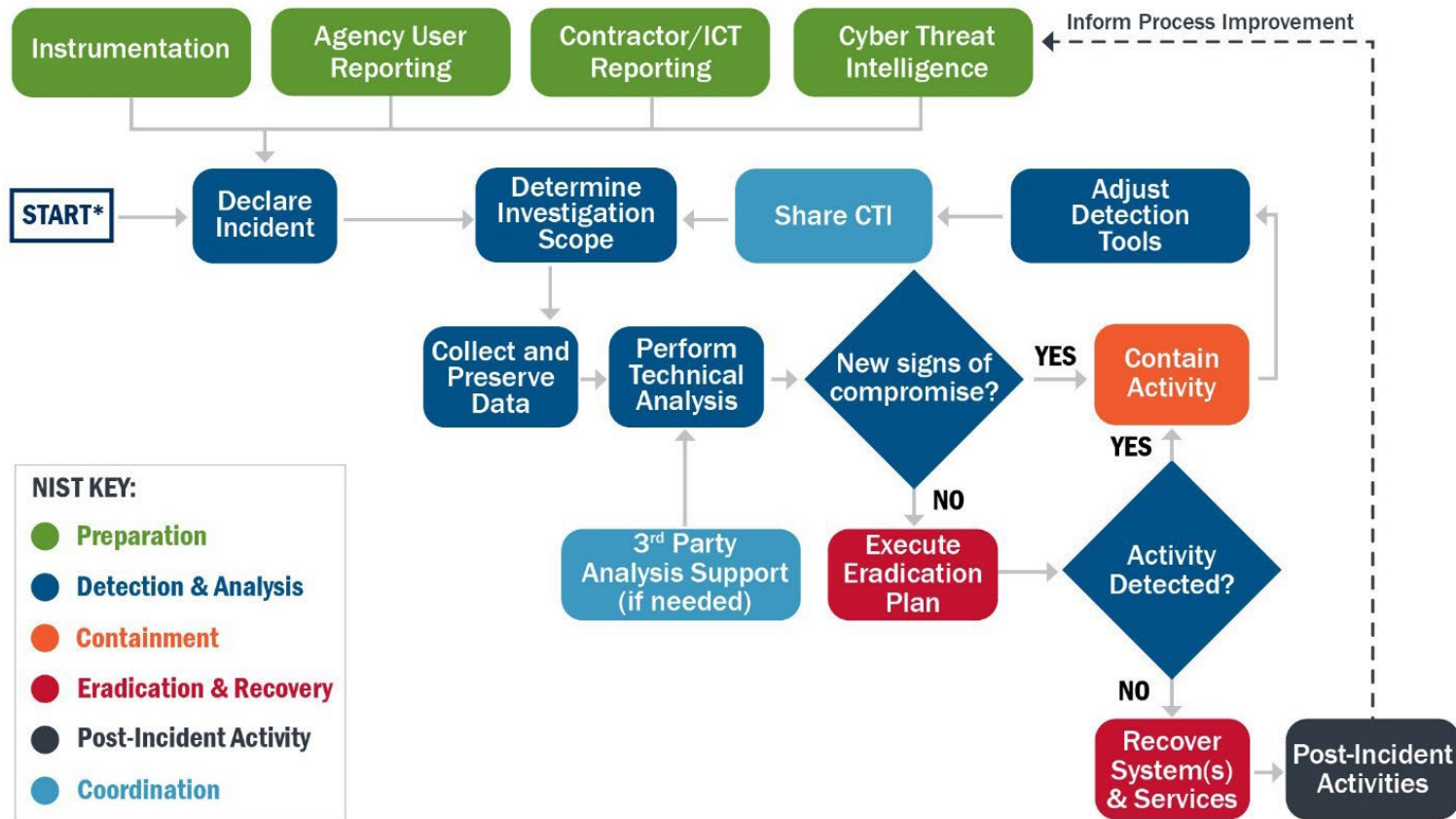
## SECURE



<https://get.gov/help/what-to-think-about-moving-to-gov/>



# Incident Response



## Incident and Vulnerability Response Playbook

Joseph Flores  
November 12, 2024

# Cybersecurity Resource Guides

CISA has detailed resource guides on our website for each of the 10 domains highlighted in our largest assessment, the Cyber Resilience Review (CRR).

## **Asset Management**

Know your assets being protected & their requirements, e.g., CIA

## **Risk Management**

Know and address your biggest risks that considers cost and your risk tolerances

## **Configuration and Change Management**

Manage asset configurations and changes

## **Service Continuity Management**

Ensure workable plans are in place to manage disruptions

## **Controls Management**

Manage and monitor controls to ensure they are meeting your objectives

## **Situational Awareness**

Discover and analyze information related to immediate operational stability and security

## **External Dependencies Management**

Know your most important external entities and manage the risks posed to essential services

## **Training and Awareness**

Ensure your people are trained on and aware of cybersecurity risks and practices

## **Incident Management**

Be able to detect and respond to incidents

## **Vulnerability Management**

Know your vulnerabilities and manage those that pose the most risk



# Email Distribution List



## NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations



Co-authored by:



January 25, 2023

## Protecting Against Malicious Use of Remote Monitoring and Management Software

Cybersecurity Advisories

<https://www.cisa.gov/about/contact-us/subscribe-updates-cisa>

Joseph Flores  
November 12, 2024



# Known Exploited Vulnerabilities List (KEVs List)

## Known Exploited Vulnerabilities Catalog

[Download CSV version](#)

[Download JSON version](#)

[Download JSON schema](#)

[Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin](#)

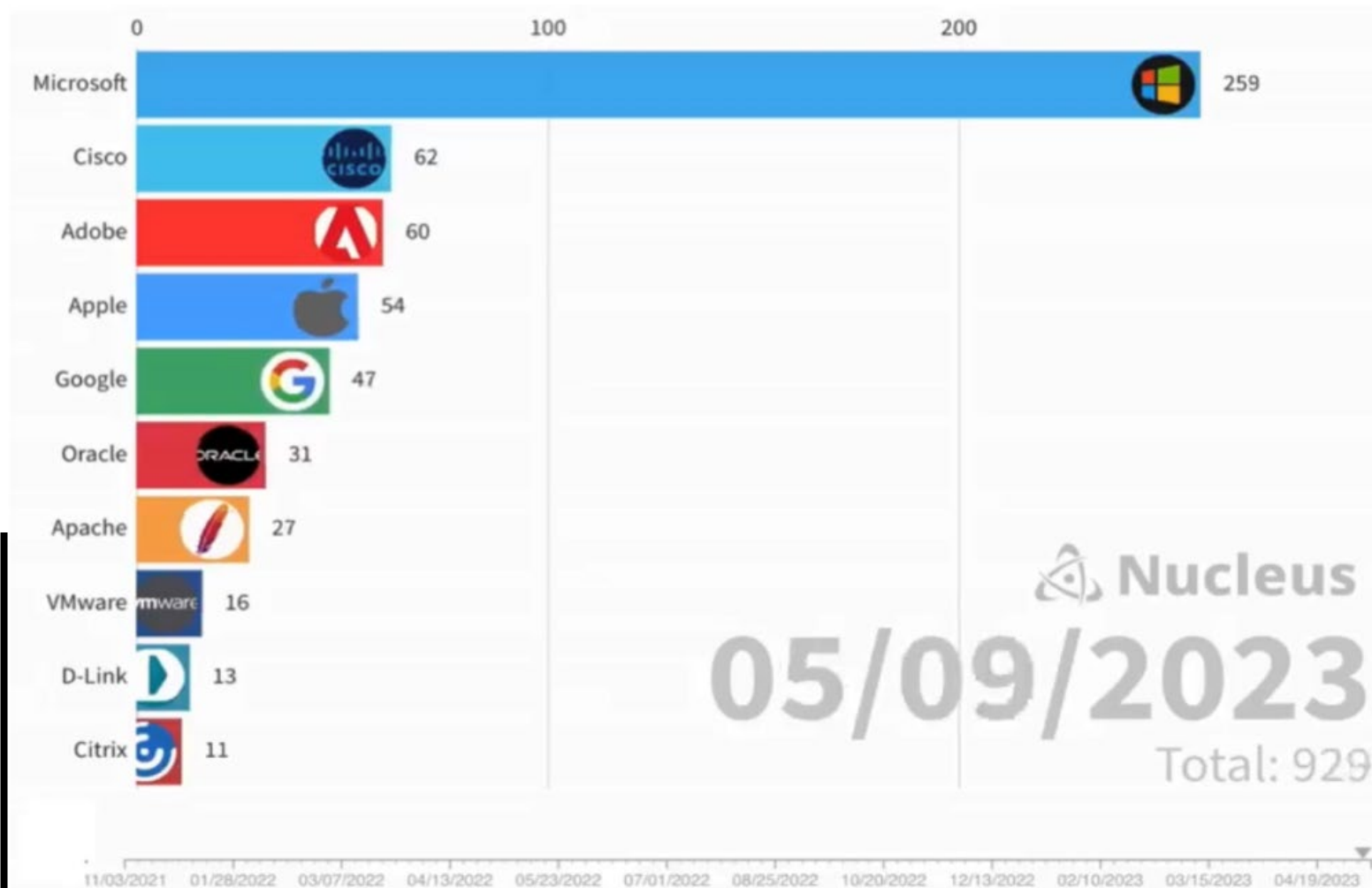
[Back to previous page for background on known exploited vulnerabilities](#)

Show  entries Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
<a href="#">CVE-2022-38180</a>	Microsoft	.NET Core and Visual Studio	Microsoft .NET Core and Visual Studio Denial of Service Vulnerability	2023-08-09	Microsoft .NET Core and Visual Studio contain an unspecified vulnerability that allows for denial of service.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-08-30	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38180">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-38180</a>
					Zyrel P660HN-T1A routers contain a			



# CISA Known Exploited Vulnerabilities (933)



# Information Sharing

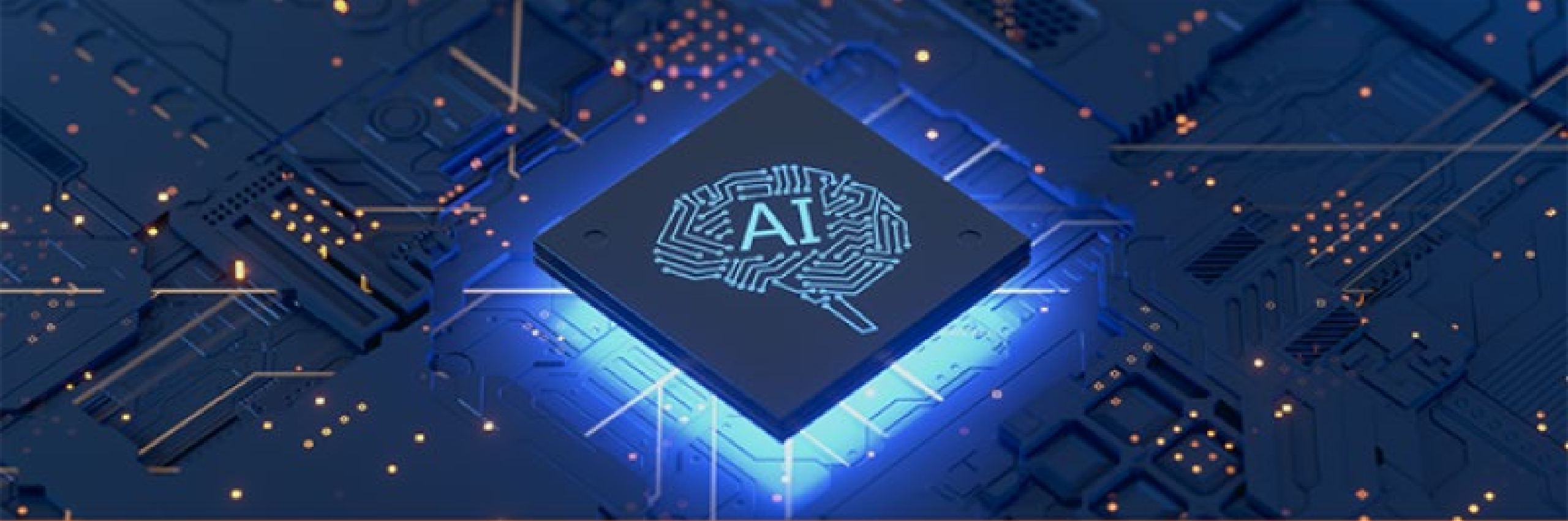
## Commonwealth Fusion Center (CFC)

- The State of MA fusion center works closely with local law enforcement, the federal government, private sector partners, and the other 80 fusion centers around the country to stay up to date on current threats and trends.
- Get added onto their distribution list so you can receive intelligence products from them.

## Homeland Security Information Network (HSIN)

- The Department of Homeland Security's official system for trusted sharing of Sensitive But Unclassified (SBU) information between federal, state, local, territorial, tribal, international and private sector partners.

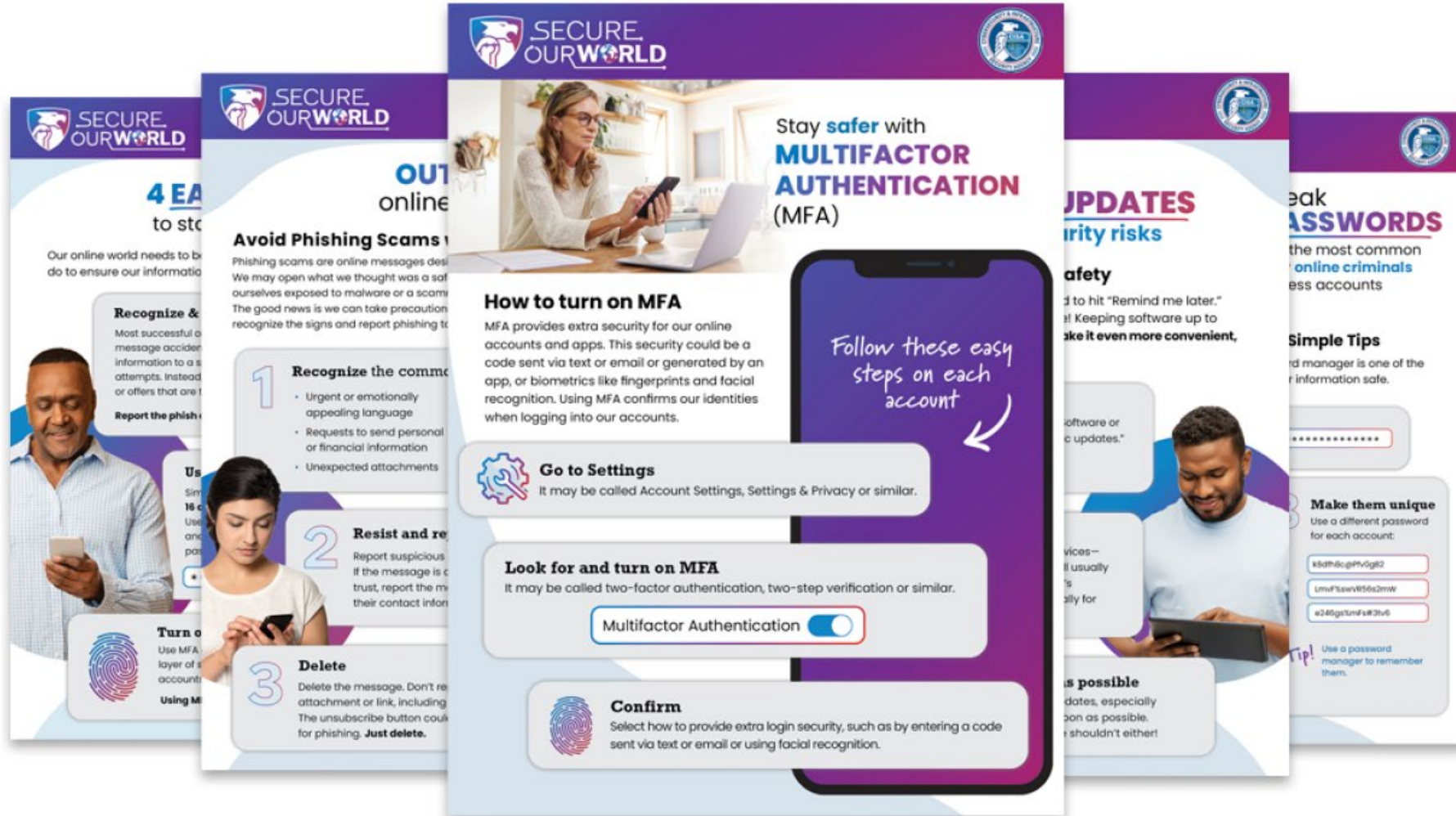




# CISA ROADMAP for AI

<https://www.cisa.gov/ai>





## Stay safer with MULTIFACTOR AUTHENTICATION (MFA)

Follow these easy steps on each account

- ### How to turn on MFA

MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.
- ### Go to Settings

It may be called Account Settings, Settings & Privacy or similar.
- ### Look for and turn on MFA

It may be called two-factor authentication, two-step verification or similar.

Multifactor Authentication
- ### Confirm

Select how to provide extra login security, such as by entering a code sent via text or email or using facial recognition.

## Avoid Phishing Scams

Phishing scams are online messages designed to trick you into giving up your information. We may open what we thought was a safe email or text message, but we could be exposing ourselves to malware or a scam. The good news is we can take precautions to recognize the signs and report phishing to the proper authorities.

- ### 1 Recognize the common signs

  - Urgent or emotionally appealing language
  - Requests to send personal or financial information
  - Unexpected attachments
- ### 2 Resist and report

Report suspicious messages. If the message is confirmed to be a scam, report the message to your contact information.
- ### 3 Delete

Delete the message. Don't re-download any attachments or links, including the unsubscribe button could be a sign of a phishing attempt. **Just delete.**

## Software Updates

### Security risks

Software updates are important for keeping your devices safe. Keeping software up to date helps protect your information. Make it even more convenient.

Software updates are important for keeping your devices safe. Keeping software up to date helps protect your information. Make it even more convenient.

## Strong Passwords

Strong passwords are one of the most common ways to protect your online accounts from criminals. Use a password manager to help you create and store strong passwords.

### Simple Tips

- Use a password manager to help you create and store strong passwords.
- Use a different password for each account.
- Make them unique. Use a different password for each account.

Tip! Use a password manager to remember them.

# Additional Resources

## Multi-State Information Sharing and Analysis Center (MS-ISAC)

- Has a variety of free resources available to its customers such as Malicious Domain Blocking and Reporting (MDBR) which is an Akamai DNS server that will stop your end users from visiting known malicious sites.
- <https://www.cisecurity.org/ms-isac>

## Center for Internet Security (CIS)

- CIS Benchmarks – 140+ configuration guidelines for various technology groups to safeguard systems against today’s evolving cyber threats.
  - <https://www.cisecurity.org/cis-benchmarks/>
- CIS SecureSuite Membership
  - Access to CIS Build Kits (GPOs, Linux scripts, and more) that enable rapid implementation of CIS Benchmark recommendations.
  - CIS-CAT Pro is a configuration assessment tool that checks conformance to the recommendations in the CIS Benchmarks



# Ransomware Pre-Warning Program and Victim Notifications

- Hundreds of Victim Notifications since 2023
  - Active network compromises of both Public and Private entities
  - Initial access and reconnaissance footholds where time is the critical factor
  - Pre-ransomware activity or pre-exploitation is most common
  - In most cases, we work in tandem FBI, USSS, or other USG entities
  - Notifications are discrete and likely require Out-of-Band (off-network) Communications
- Additionally, CSAs will communicate specific vulnerability warnings to Public and Private sector entities when information is obtained through CISA Internet facing scans or research and other cooperative 3<sup>rd</sup> party knowledge.



# Ransomware Pre-Warning Program and Victim Notifications

- **IGNITE REALTIME OPENFIRE VULNERABILITY NOTIFICATIONS**
  - Entities that are vulnerable to Openfire CVE-2023-32315 for regional notification on August 28th.
- **PALO ALTO PAN-OS RANSOMWARE VULNERABILITY WARNING PILOT NOTIFICATION**
  - Entities that are running vulnerable instances of Palo Alto's operating system for its next generation firewalls.
- **OUTDATED INSTANCES NOTIFICATIONS**
  - Tip from a trusted third party of entities running outdated and vulnerable instances of Microsoft Exchange, Ivanti MobileIron, SharePoint, and Fortigate.
- **U.S. QAKBOT NOTIFICATIONS**
  - CSD and IOD are collaborating with the FBI to assist in notifying Critical Infrastructure (CI) entities infected by Qakbot, a modular second-stage malware with backdoor capabilities that operates a significant botnet.



# CYBERSECURITY TOOLS



# Secure Cloud Business Applications (SCuBA)

The Secure Cloud Business Applications (SCuBA) project provides product-specific security baselines for critical business applications.

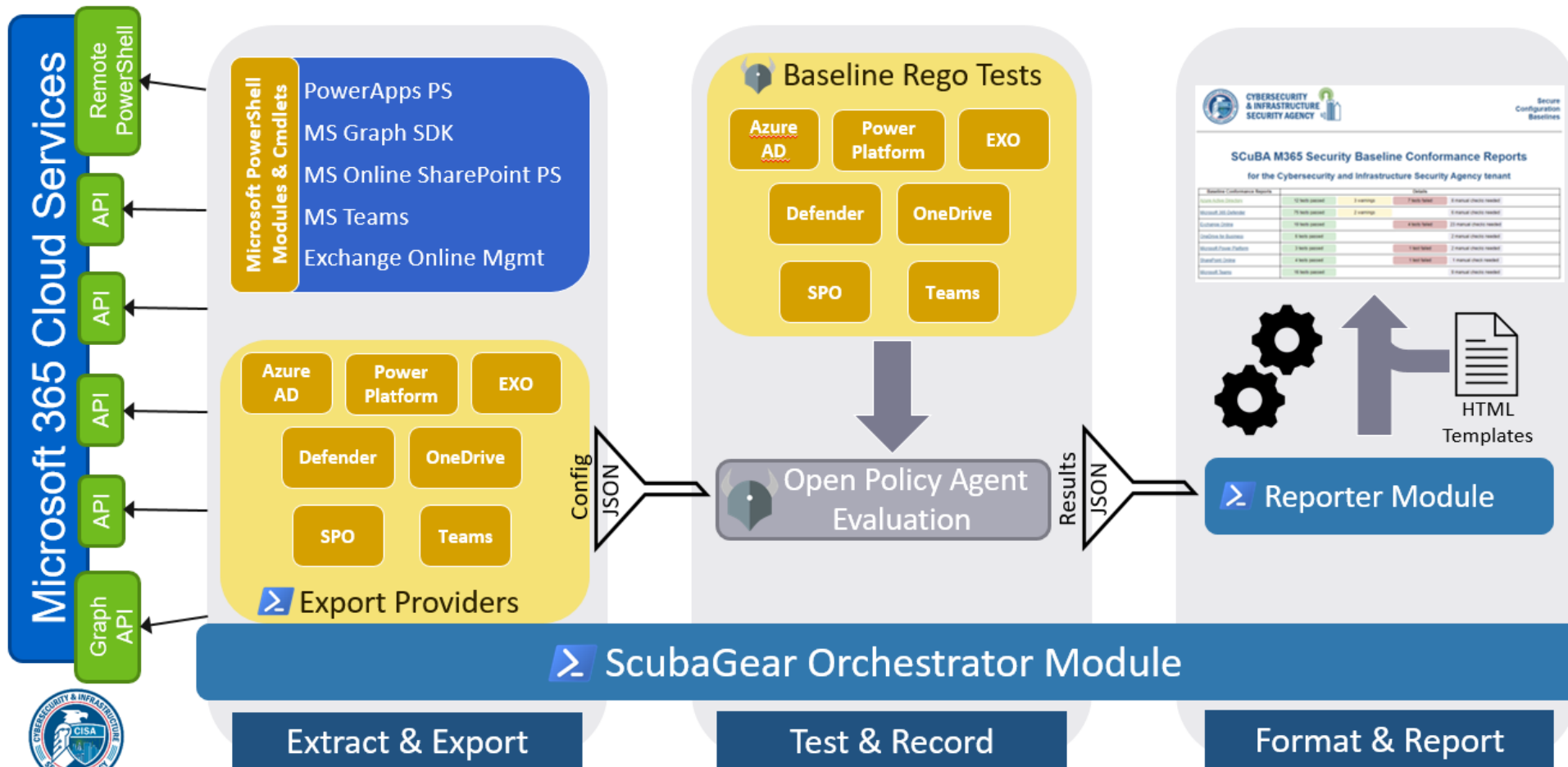


- ✓ Azure Active Directory
- ✓ Defender for Office 365
- ✓ Exchange Online
- ✓ OneDrive for Business
- ✓ Power BI
- ✓ Power Platform
- ✓ SharePoint Online
- ✓ Teams

- ✓ Gmail
- ✓ Google Meet
- ✓ Common Controls
- ✓ Drive/Docs
- ✓ Meet
- ✓ Calendar
- ✓ Groups
- ✓ Sites

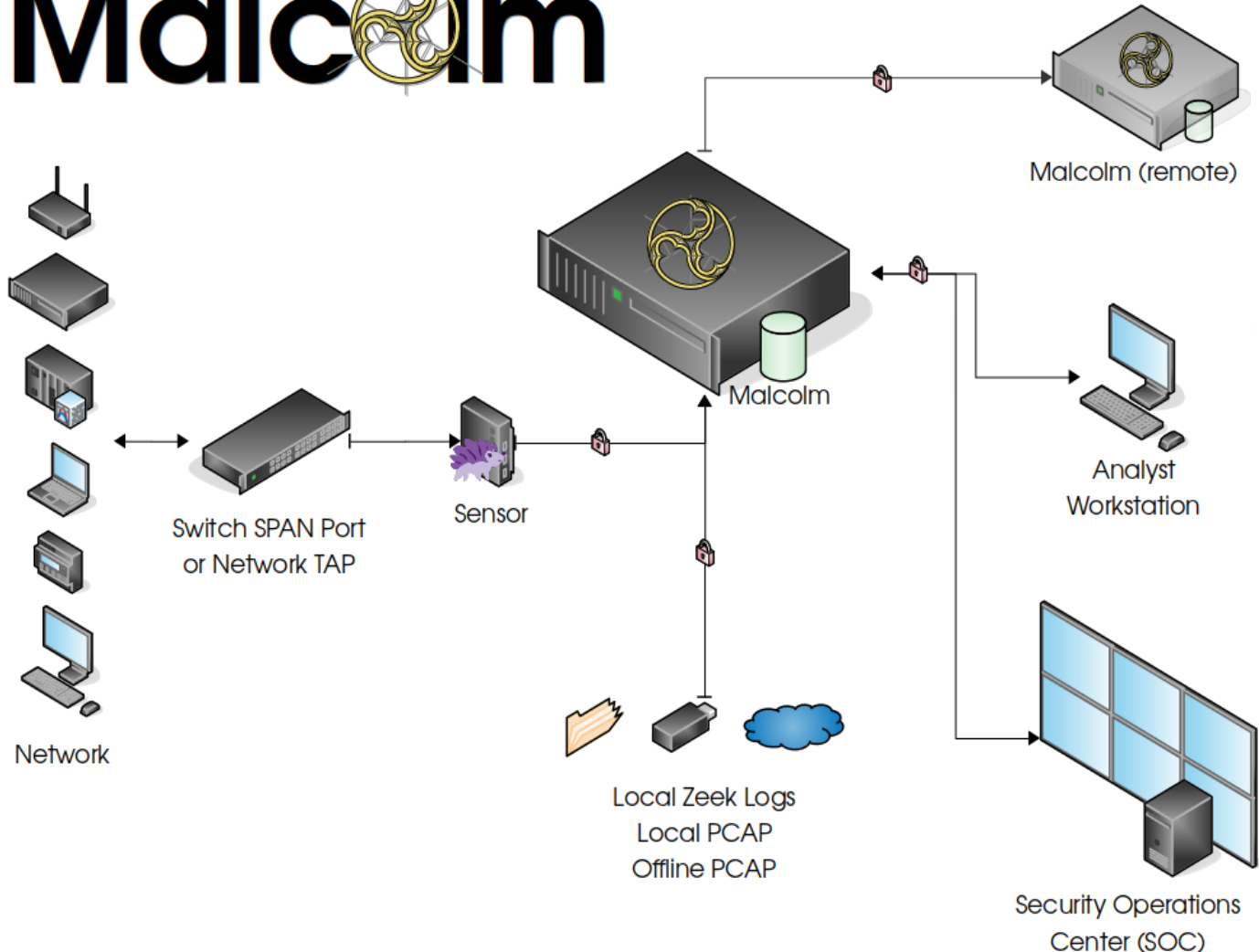


# ScubaGear Baseline Assessment Tool

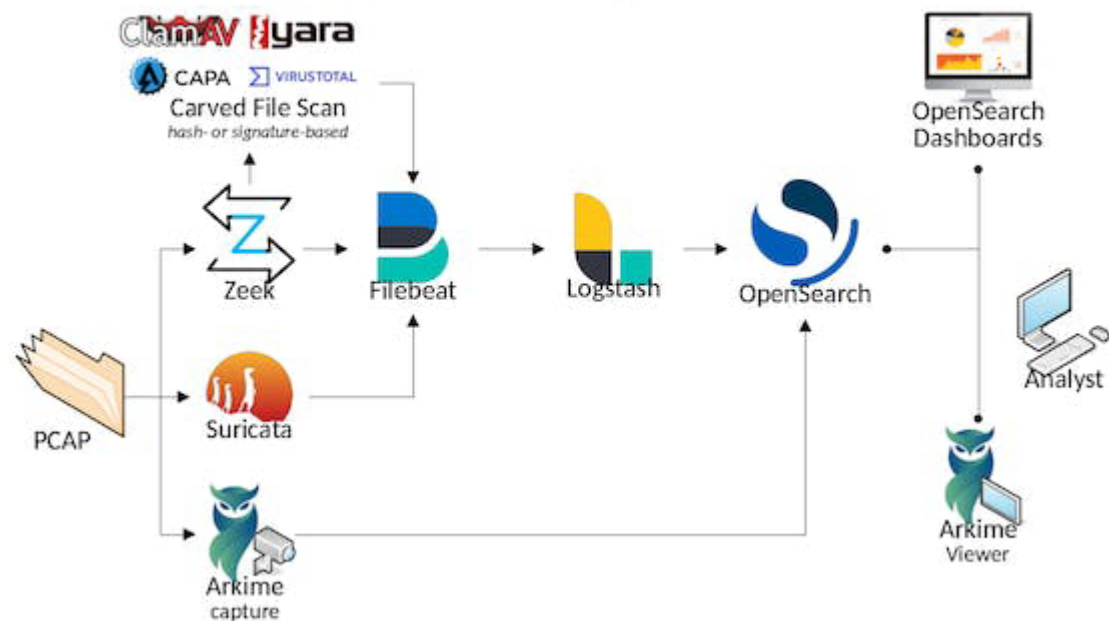


# Malcom - Network Traffic Analysis

# Malcolm



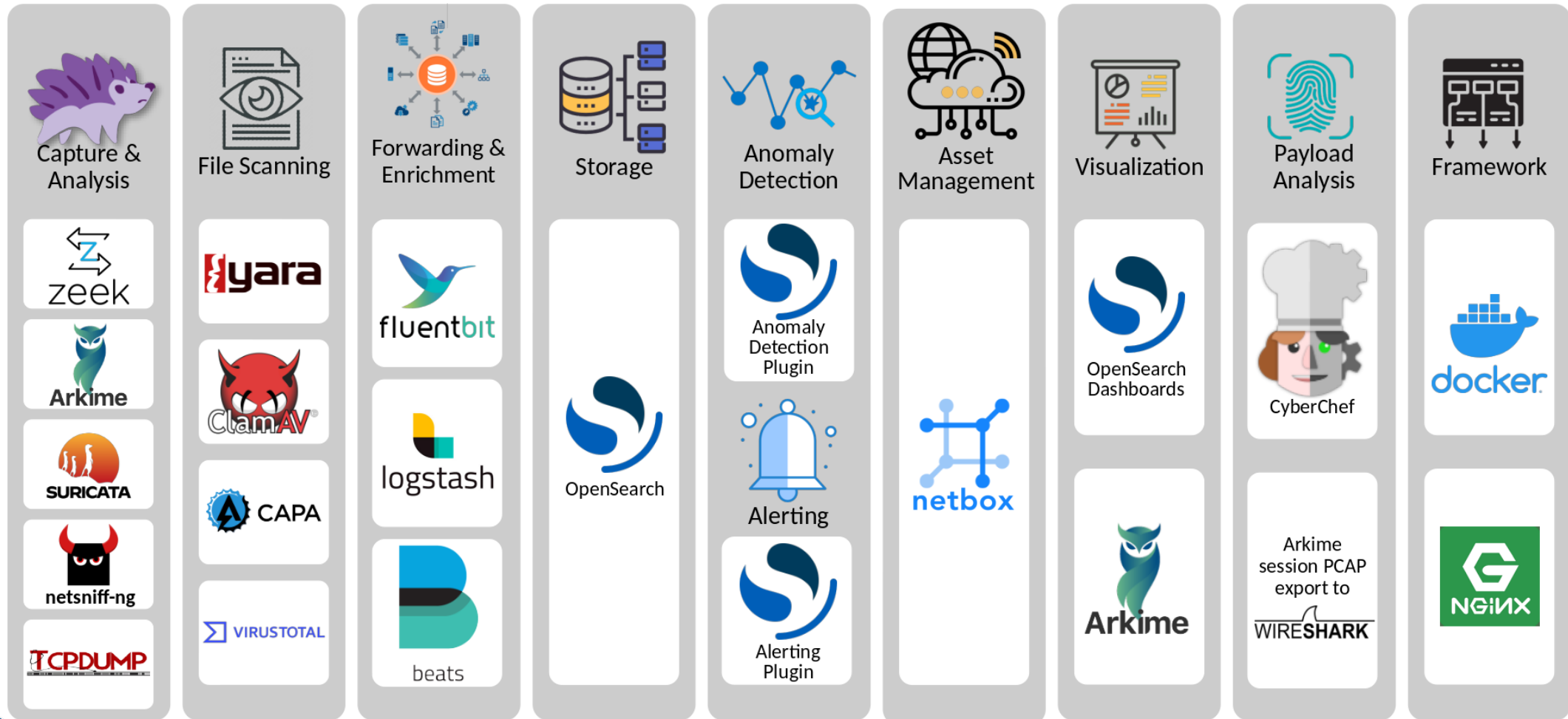
## Data Pipeline



Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files), Zeek logs and Suricata alerts.



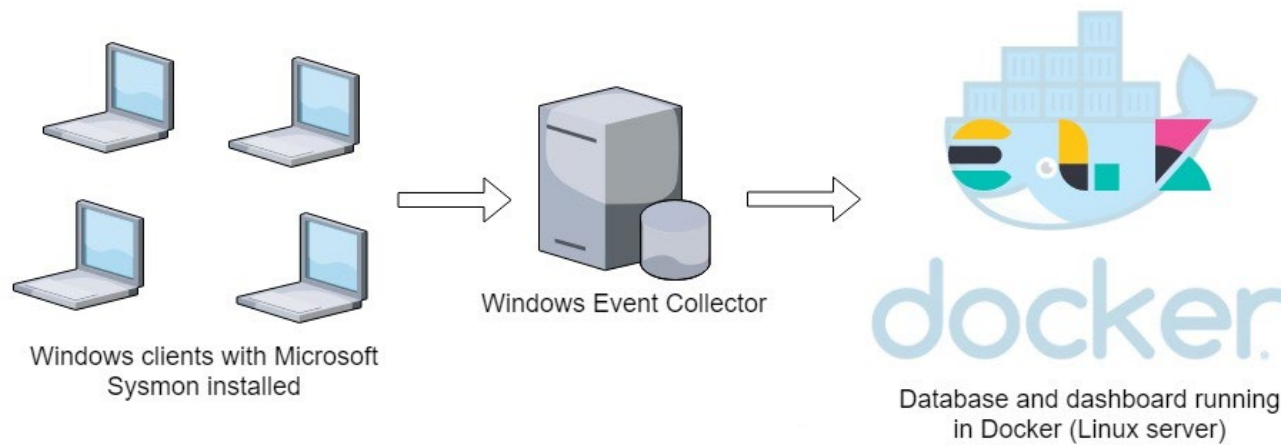
# Malcom - Network Traffic Analysis



# Logging Made Easy (LME)

LME provides centralized security logging for Windows clients and should be used if:

- You don't have a SOC, SIEM or any monitoring in place at the moment.
- You lack the budget, time or understanding to set up your own logging system.
- You recognize the need to begin gathering logs and monitoring your IT.



# Logging Made Easy (LME)

## CLIENTS



### Description

An arbitrary number of machines to be monitored using LME

### Operating System

Windows

### Software Used by LME

Sysmon

## EVENT COLLECTOR



### Description

A server for collecting and forwarding logs from the client

### Operating System

Windows

### Software Used by LME

Winlogbeat

## ELK SERVER



### Description

A server for storing and analyzing the logs

### Operating System

Linux

### Software Used by LME

Docker, git, Elasticsearch, Logstash, and Kibana



# Logging Made Easy (LME)

The screenshot displays the Elastic Security Rules management interface. The left sidebar contains navigation options: Security, Dashboards, Alerts, Findings, Timelines, Cases, Explore, and Intelligence. The main content area is titled 'Rules' and includes a search bar for 'Rule name, index pat'. Below the search bar, there are buttons for 'Import value lists', 'Import rules', and 'Create new rule'. A table lists various rules with the following columns: Rule, Risk score, Severity, Last run, Last response, Last updated, and Enabled. A context menu is open over the first rule, showing options: Enable, Duplicate, Index patterns, Tags, Add rule actions, Update rule schedules, Apply Timeline template, Export, Disable, and Delete. The table data is as follows:

Rule	Risk score	Severity	Last run	Last response	Last updated	Enabled
Threat Intel Hash Ind	99	Critical	17 minutes ago	Succeeded	17 minutes ago	Enabled
Network Connection	21	Low	2 minutes ago	Succeeded	18 minutes ago	Enabled
Kerberos Traffic from	47	Medium	2 minutes ago	Succeeded	18 minutes ago	Enabled
Potential Antimalwar	73	High	2 minutes ago	Succeeded	18 minutes ago	Enabled
Unusual Network Activity from a Windows System Bi...	47	Medium	2 minutes ago	Succeeded	18 minutes ago	Enabled
Suspicious Process Access via Direct System Call	73	High	2 minutes ago	Succeeded	18 minutes ago	Enabled
Uncommon Registry Persistence Change	47	Medium	2 minutes ago	Warning	17 minutes ago	Enabled
Elastic Agent Service Terminated	47	Medium	2 minutes ago	Warning	18 minutes ago	Enabled
Renamed Autolt Scripts Interpreter	47	Medium	2 minutes ago	Succeeded	18 minutes ago	Enabled



# Hunt and Incident Response Tool

Untitled Goose Tool is a robust and flexible hunt and incident response tool that can export and review a variety of key data.

- **Azure Active Directory (AAD) sign-in and audit logs**
- **Microsoft 365 (M365) unified audit log (UAL)**
- **Azure activity logs**
- **Microsoft Defender for Internet of Things (D4IoT) alerts**
- **Microsoft Defender for Endpoint (MDE) data for suspicious activity**



Ingest the JSON results into a Security Information and Event Management (SIEM) tool, web browser, text editor, or a database.



# Malware Next-Gen



**Malware**  
NEXT-GEN

User Feedback

Search...



Search Entire Database  If selected search will take more time.

Submit [My Submissions](#) [All Submissions](#)

Analyst Tools ▼



## Quick Submit

File Upload

URL

Choose File No file chosen

One file per submission.

File size limit is 100MB.

Archive submission must contain 1-10 files.

Traffic Light Protocol

● TLP: GREEN

● CLEAR

Disclosure is not limited

● GREEN

Limited disclosure, restricted to the community

● AMBER

Limited disclosure, restricted to participants' organization and its clients

● AMBER+STRICT

Limited disclosure, restricted to participants' organization

● RED

Not for disclosure, restricted to participants only

Comments

0/500 Incident ID

Comments

Incident ID

SUBMIT

## My Submissions

Submitted ↓	SID
> 2024-04-17 17:41:06Z	83a2acd8-e590-454b-a
> 2023-10-30 12:50:56Z	77818922-1171-474f-b

Last Name	Organization	Status	User	TLP
Palmbach	Cybersecurity and Infrastructure Security Agency (CISA)	Completed	david.palmbach@cisa.dhs.gov	<span style="color: green;">●</span>
Palmbach	Cybersecurity and Infrastructure Security Agency (CISA)	Completed	david.palmbach@cisa.dhs.gov	<span style="color: green;">●</span>

Rows per page: 10 1-2 of 2


Rows per page: 10 1-2 of 2



Joseph Flores  
November 12, 2024

# Malware Next-Gen

MIFR Raw Analysis Dropped Files Virus Details Submit Feedback



- Summary
- Static Analysis
- Dynamic Analysis
- Network Activity
- MITRE ATT&CK Characterization
- Mitigation
- STIX 2.1

## Malware Initial Findings Report (MIFR)

06211d1c-a34c-4003-9650-969341939aa9

TLP:GREEN

### Notifications

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise. This document is marked TLP:GREEN--Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: When "community" is not defined, assume the cybersecurity/cyber defense community. For more information on the Traffic Light Protocol (TLP), see <https://www.us-cert.gov/tp>.

### Summary

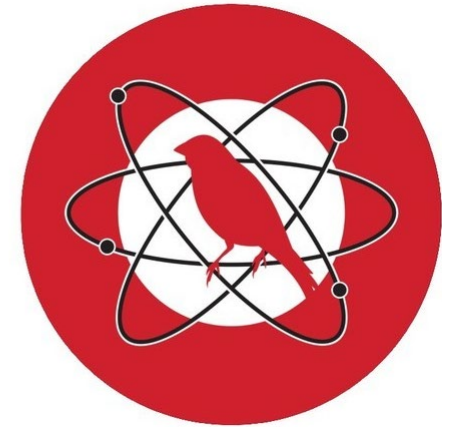
Submitted File	
Filename	TEST.docx



# List of Free Cybersecurity Tools



**Atomic Red Team**



**OpenVAS**

Open Vulnerability Assessment Scanner



Windows Sysinternals



<https://www.cisa.gov/free-cybersecurity-services-and-tools>

Joseph Flores  
November 12, 2024



# CYBERSECURITY TRAINING AND EXERCISES



# Cybersecurity Training



**FedVTE** FEDERAL  
VIRTUAL  
TRAINING  
ENVIRONMENT



# Incident Response Training Series

## Awareness Webinars (100)

- Defending Internet Accessible Systems
- Preventing Web and Email Server Attacks
- Preventing DNS Infrastructure Tampering
- Understanding Indicators of Compromise
- Defend Against Ransomware Attacks
- Introduction to Log Management
- Using the CISA Incident Response Playbook at Your Organization
- *Introduction to Network Diagramming*
- *Instrumenting the Environment to Detect Suspicious and Malicious Activity*

## Cyber Range Training (200)

- Defending Internet Accessible Systems
- Preventing Web and Email Server Attacks
- Preventing DNS Infrastructure Tampering
- Understanding Indicators of Compromise
- Defend Against Ransomware Attacks
- Introduction to Log Management
- Using the CISA Incident Response Playbook at your Organization



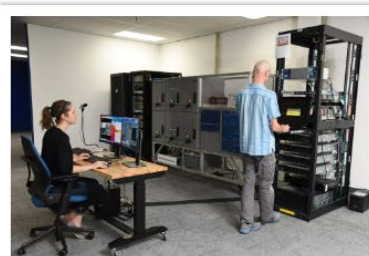
# Industrial Control Systems (ICS) Training

## Instructor Led Training

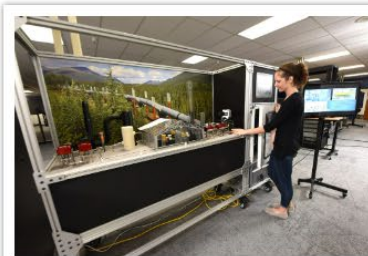
- Introduction to Control Systems Cybersecurity (101) - 4 hrs
- Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ICS Cybersecurity (300) – 12 hrs
- ICS Cybersecurity & RED-BLUE Exercise (301) – **4 days in person**
- ICS Evaluation (401V) – 20 hrs or (401L is **3 days in person**)



Chemical Processing



Electrical Distribution and Transmission



Natural Gas Pipeline



Building Management

Virtual Tour



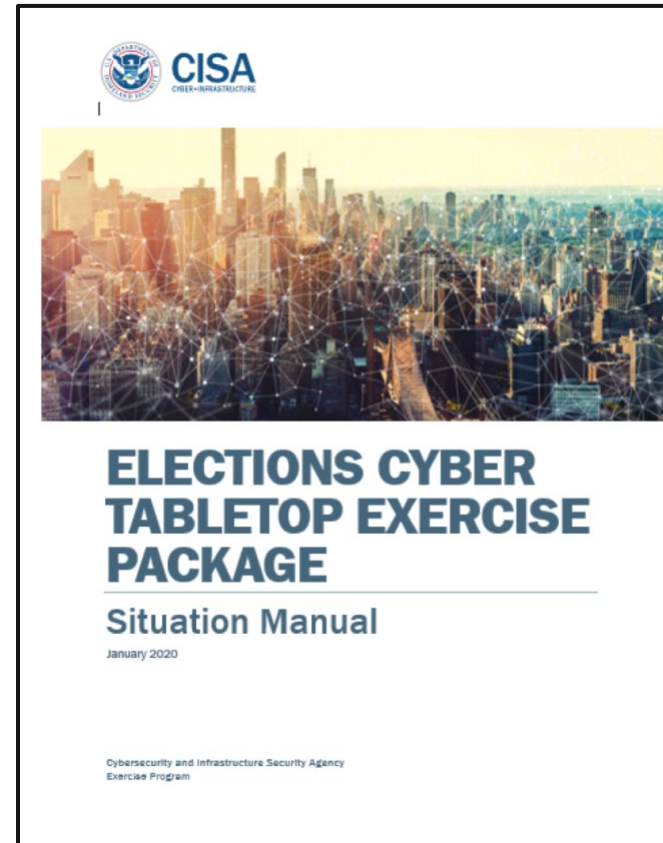
# CISA Tabletop Exercise Package (CTEP)

Designed to assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders.

- **15 cybersecurity scenarios**
- **71 physical security scenarios**
- **2 convergence scenarios**

## Additional Resource Materials

CTEP Fact Sheet  
CTEP Welcome Letter  
CTEP Exercise Planner Handbook  
CTEP Facilitator Evaluator Handbook  
CTEP Invitation Letter Template  
CTEP Exercise Brief Slide Deck Template  
CTEP Participant Feedback Template  
CTEP Planner Feedback Form  
CTEP AAR-IP Template



Joseph Flores  
November 12, 2024

# Resources for Students



# PHYSICAL SECURITY RESOURCES



# Physical Security Assessments/Resources

- Assist Visits
- Security at First Entry (SAFE)
- Infrastructure Survey Tool (IST)
- Infrastructure Visualization Platform (IVP)
- Multi-Asset & Systems Assessment (MASA)
- Regional Resiliency Assessment Program



**CISA**  
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

## SECURITY ASSESSMENT AT FIRST ENTRY

THE SECURITY ASSESSMENT AT FIRST ENTRY (SAFE) PROCESS IS DESIGNED TO EVALUATE A FACILITY'S CURRENT SECURITY POSTURE AND IDENTIFY OPTIONS FOR FACILITY OWNERS AND OPERATORS TO MITIGATE RELEVANT THREATS.

### WHAT IS SAFE?

SAFE may be one of your first steps in implementing an effective security program at your facility. This assessment is intended for owners and operators who would like a review of their existing security measures and feedback on making their facilities more secure. The data collected during the SAFE process is not shared with other entities.

### WHAT DOES A SAFE VISIT ENTAIL?

The SAFE assessment is free, quick, and easy, and involves a brief walk-through of your site by a DHS Protective Security Advisor (PSA). The SAFE visit will be

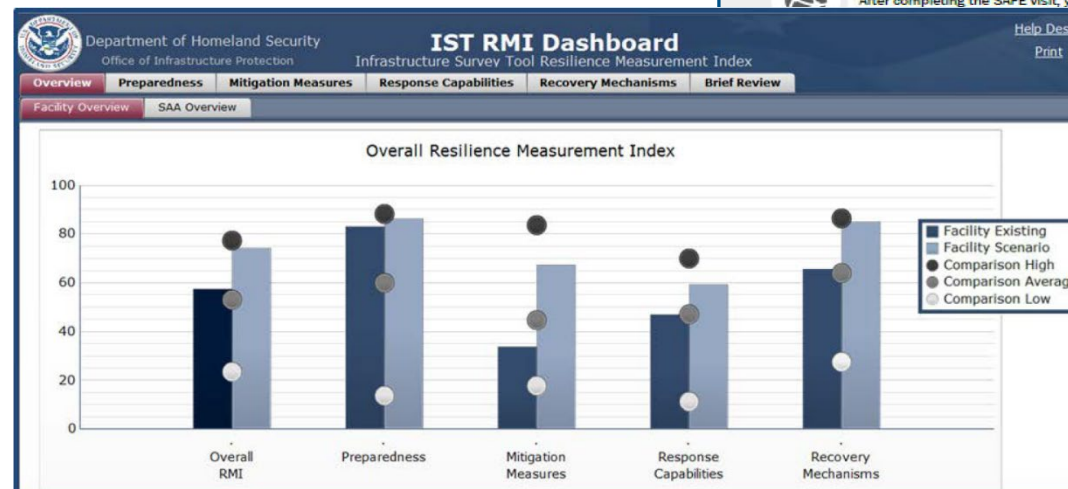
- Focused on physical security;
- Conducted by your local DHS PSA;
- Completed in a few hours; and
- Objective and focused on security measures.

### WHAT DO I GET IN RETURN?

After completing the SAFE visit, your PSA will deliver a printed report about your facility. This report will

ns: During the assessment, the PSA will make note of existing practices t are noteworthy and should continue implementing. options for consideration: The PSA will also make note of any areas at onal attention from a security perspective—areas relating to security perimeter security, and other physical security measures. Each ave one or more options for you to consider to mitigate these issues. untary. Your facility determines what actions to take in light of your sture, anticipated growth or organizational changes, budgetary outlook, s, and organizations: These points of contact may be useful as you ove your facility's security posture. : You can review these resources to learn more about options that the is to implement them.

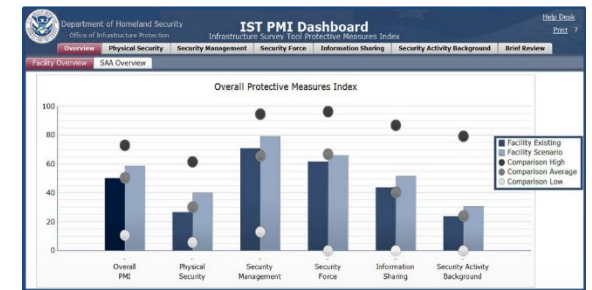
[a.dhs.gov](#)





# IST Data Categories

- Facility Information
- Contacts
- Facility Overview
- **Information Sharing\***
- **Protective Measures Assessment\***
- **Criticality\***
- **Security Management Profile\***
- Security Areas/Assets
- **Physical Security\***
  - Building Envelope
  - Vehicle Access Control
  - Parking
  - Site's Security Force
  - Intrusion Detection System (IDS)/Close Circuit Television (CCTV)
  - Access Control
  - Security Lighting
- Additional DHS Products and Services
- Criticality Appendix
- Images
- **Security Force\***
- Cyber Vulnerability
- **Dependencies\***



**\* Comparative analysis provided**

- Survey and assessment information is shared with owners and operators through interactive dashboards and Dashboards allow users to explore the impacts of potential improvements to their security and resilience status



# EMERGENCY COMMUNICATIONS RESOURCES



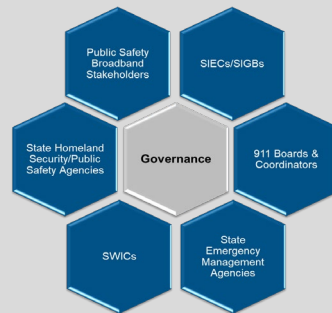
# Emergency Communications Coordinators (ECCs)

## Strategic Planning



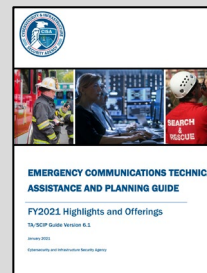
State & Tribal Communications Interoperability Plans

## Governance



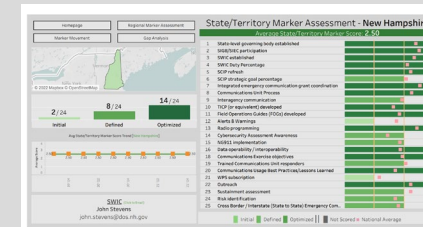
Regional Coordination

## Technical Assistance



Service Offerings Guides

## Assessment



State Markers

*ECCs support emergency communications across government and critical infrastructure*

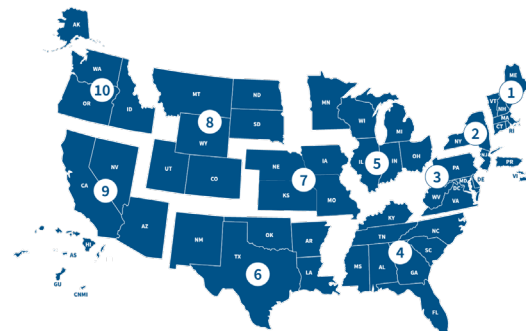
STATEWIDE INTEROPERABILITY COORDINATOR (SWIC)

*ECCs maintain close relationships with SWICs and public safety in their regions*



Special Coordination

ESF-2 | NSSE | SEAR



6,000+ Public Safety Answering Points (911)



50,000+ Radio Systems



300,000+ Cell Towers & Radio Sites

# Emergency Comms Program

Melissa Nazzaro

Emergency Communications Coordinator, Region 1 (CT, MA, RI, VT, NH, ME)

Email: [Melissa.Nazzaro@CISA.DHS.GOV](mailto:Melissa.Nazzaro@CISA.DHS.GOV)

Cell: (202) 322-5263 (FIRSTNET)

## Statewide Communication Interoperability Plans Workshops

Learn how to implement Statewide Communication Interoperability Plans (SCIPs)

RELATED TOPICS: [EMERGENCY COMMUNICATIONS](#)

### Description

Statewide Communication Interoperability Plans (SCIPs) are locally-driven, multi-jurisdictional, and multi-disciplinary statewide plans to enhance emergency communications. The SCIP creates a single resource for all stakeholders and a unified approach for enhancing interoperable communications for public safety and officials at all levels of government. SCIPs define the current and future direction for interoperable and emergency communications within a state or territory.

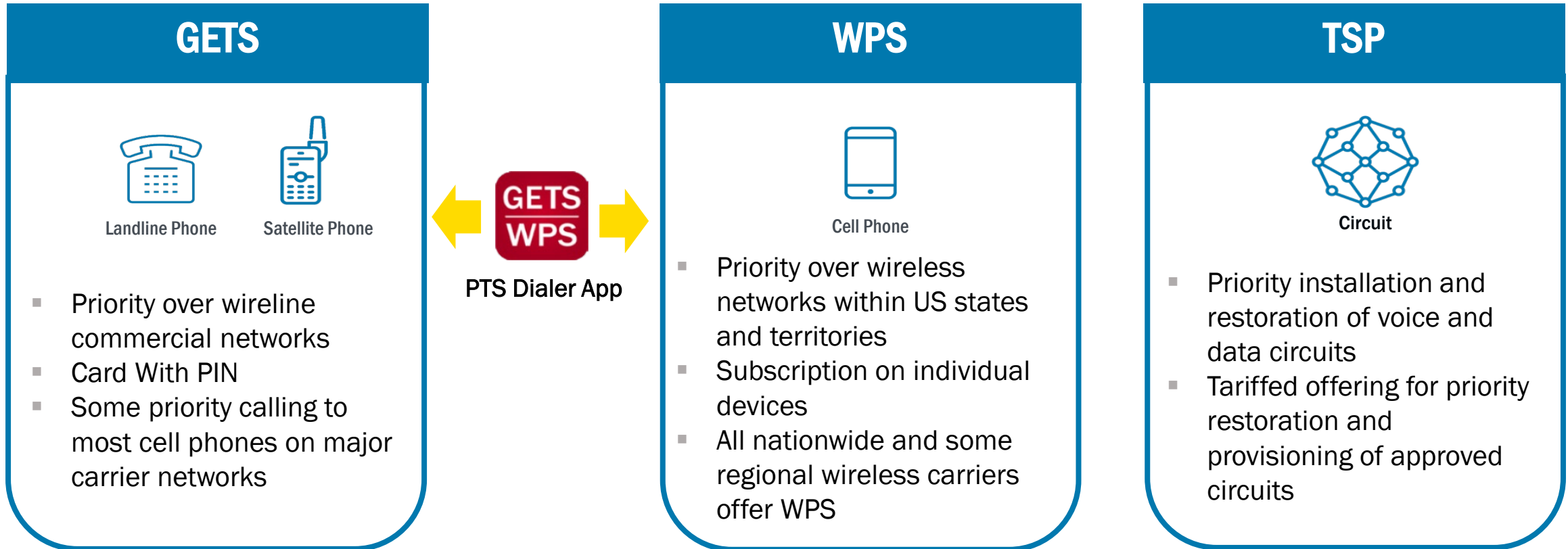
SCIPs are comprehensive plans which outline the:

- Current and future interoperable and emergency communications environment;
- Goals with specific steps for action (including owners and completion timeframes);
- Defined mechanisms to measure achievements; and,
- Process by which the state will record progress and challenges each year.



# Priority Services and Key Features

A suite of services that enable priority telecommunications when networks are degraded or congested



# Next Steps

- **Schedule a Cyber Performance Goals assessment**
- **Schedule a Security at First Entry assessment**
- **Sign up for CISA's CyHy vulnerability scanning**
- **Sign up for CISA's email distribution list**
- **Assess potential use cases for free tools**
- **Utilize training/exercises**





**DEFEND TODAY,  
SECURE TOMORROW**



**CSA for MA**

**Joseph Flores**

**Email: [joseph.flores@cisa.dhs.gov](mailto:joseph.flores@cisa.dhs.gov)**

**Cell: (617) 877-7729**

**PSA for MA**

**John Warren**

**Email: [john.warren@cisa.dhs.gov](mailto:john.warren@cisa.dhs.gov)**

**Cell: (413) 662-9305**

**CSA for MA**

**Monsurat Ottun**

**Email: [monsurat.ottun@cisa.dhs.gov](mailto:monsurat.ottun@cisa.dhs.gov)**

**Cell: (202) 285-6247**

**PSA for MA**

**TJ Swenson**

**Email: [thomas.swenson@cisa.dhs.gov](mailto:thomas.swenson@cisa.dhs.gov)**

**Cell: (202) 880-3143**