CISA Services and Programs

Leslie Ann Kainoa, CISSP
Cybersecurity State Coordinator (CSC), Oregon
Cybersecurity and Infrastructure Security Agency, Region 10

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

CISA

STRATEGIC PLAN 2023–2025

GOAL 1

CYBER DEFENSE:
Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

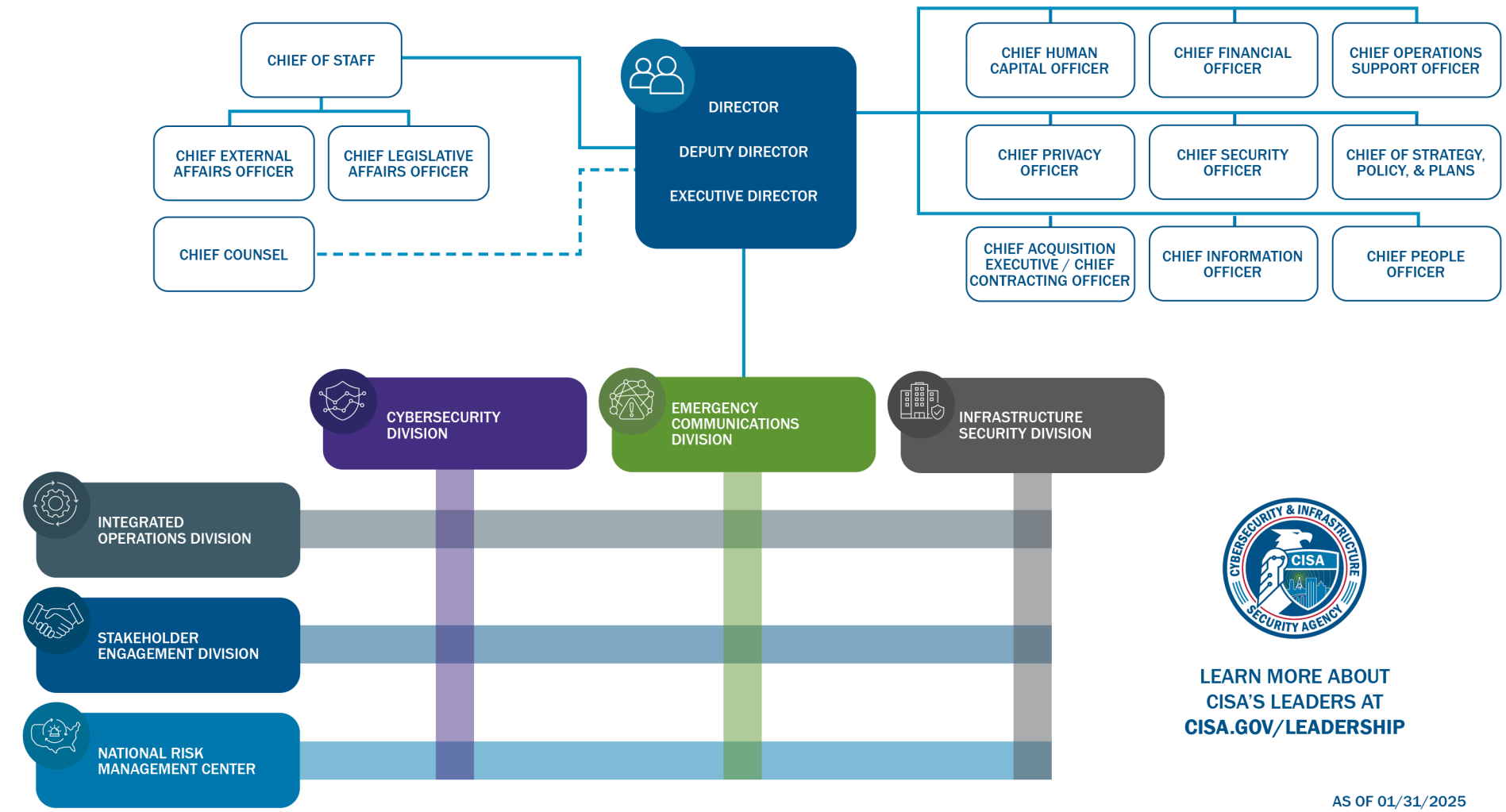
RISK REDUCTION & RESILIENCE:
Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure

GOAL 3

OPERATIONAL COLLABORATION:
Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

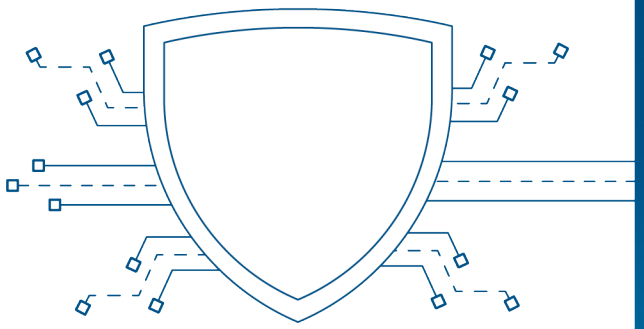
AGENCY UNIFICATION:
Unify as One CISA Through Integrated Functions, Capabilities, and Workforce



LEARN MORE ABOUT
CISA'S LEADERS AT
CISA.GOV/LEADERSHIP

AS OF 01/31/2025

Cybersecurity Mission



CISA's Cybersecurity Division leads the national effort to reduce the prevalence and impact of cyber incidents by providing services, guidance, and capabilities that address immediate risks and advance toward a secure cyber ecosystem.

HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- Catalyze Persistent Collaboration Across Government and the Private Sector
- Expand Operational Visibility into Threats and Vulnerabilities
- Drive Prioritization and Measure Adoption of the Most Effective Security Measures
- Serve as the Operational Lead for Federal Civilian Cybersecurity
- Advance a Technology Product Ecosystem that is Secure by Design

Emergency Communications Mission

CISA's Emergency Communications Division supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient.

HOW CISA IS CARRYING OUT ITS EMERGENCY COMMUNICATIONS MISSION:

- Expand Interoperability
- Coordinate Effective Communications Planning
- Increase Priority Services Adoption with Interoperable Priority

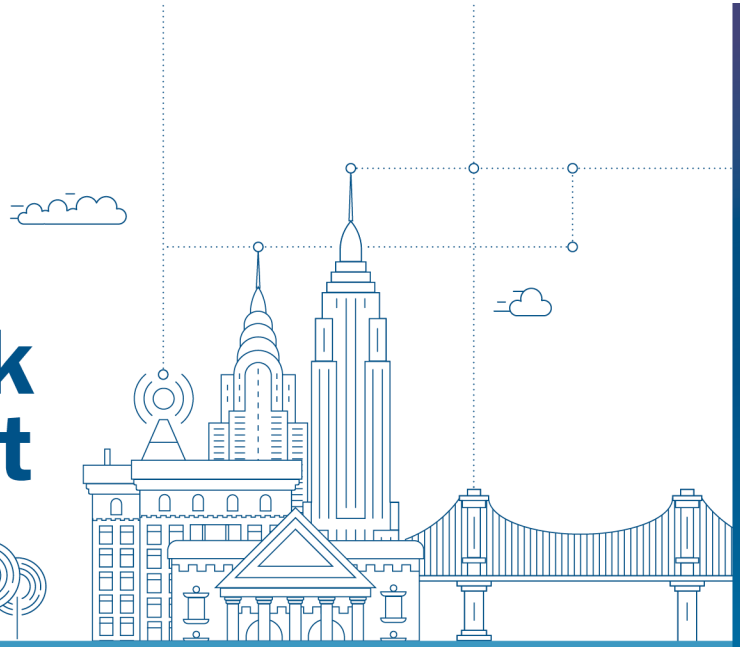
Infrastructure Security Mission

CISA's Infrastructure Security Division leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

HOW CISA IS CARRYING OUT ITS INFRASTRUCTURE SECURITY MISSION:

- Combat Terrorism and Targeted Violence
- Conduct Exercise and Training Programs
- Enhance School Safety with our School Safety Task Force
- Assess and Analyze Critical Infrastructure
- Identify and Prioritize Critical Infrastructure
- Strengthen Chemical Security with ChemLock

National Risk Management Center

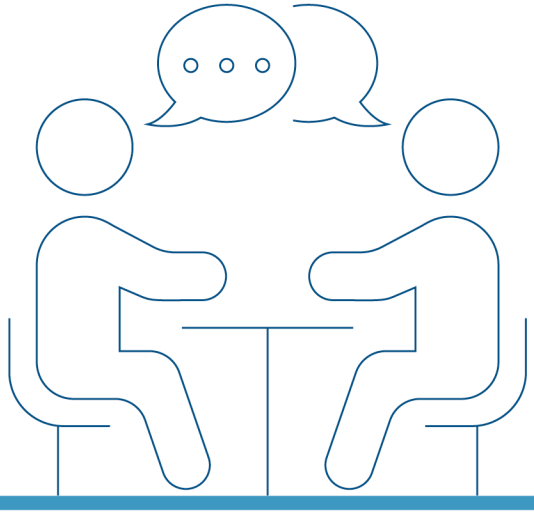


CISA's National Risk Management Center provides planning, analysis, and collaboration to lead strategic risk reduction efforts for the nation.

HOW CISA IS CARRYING OUT ITS RISK MANAGEMENT MISSION:

- Provide Risk Analysis to Customers Throughout the Critical Infrastructure Community
- Drive Shared Understanding and Collaborative Mitigation of Risks
- Drive Action in Focused, Prioritized Risk Areas

Stakeholder Engagement

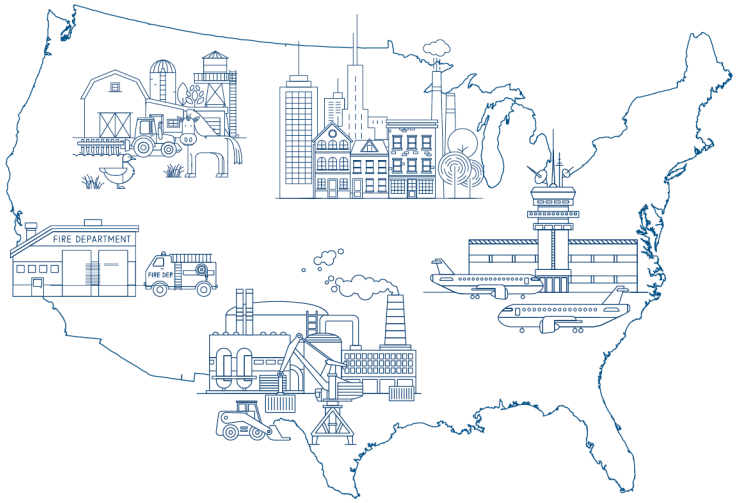


CISA's Stakeholder Engagement Division builds and maintains national and international partnerships and engagements while serving as the hub for the shared stakeholder information that advances unified risk reduction efforts.

HOW CISA IS CARRYING OUT ITS STAKEHOLDER ENGAGEMENT MISSION:

- Plan and Implement Collaboratively Stakeholder Engagements and Partnership Activities to Advance a Unified Mission Delivery
- Use Stakeholder Insights and Feedback to Inform CISA Product Development and Mission Delivery
- Ensure Stakeholders Have Easy Access to CISA Programs, Products, Services, and Information

Integrated Operations



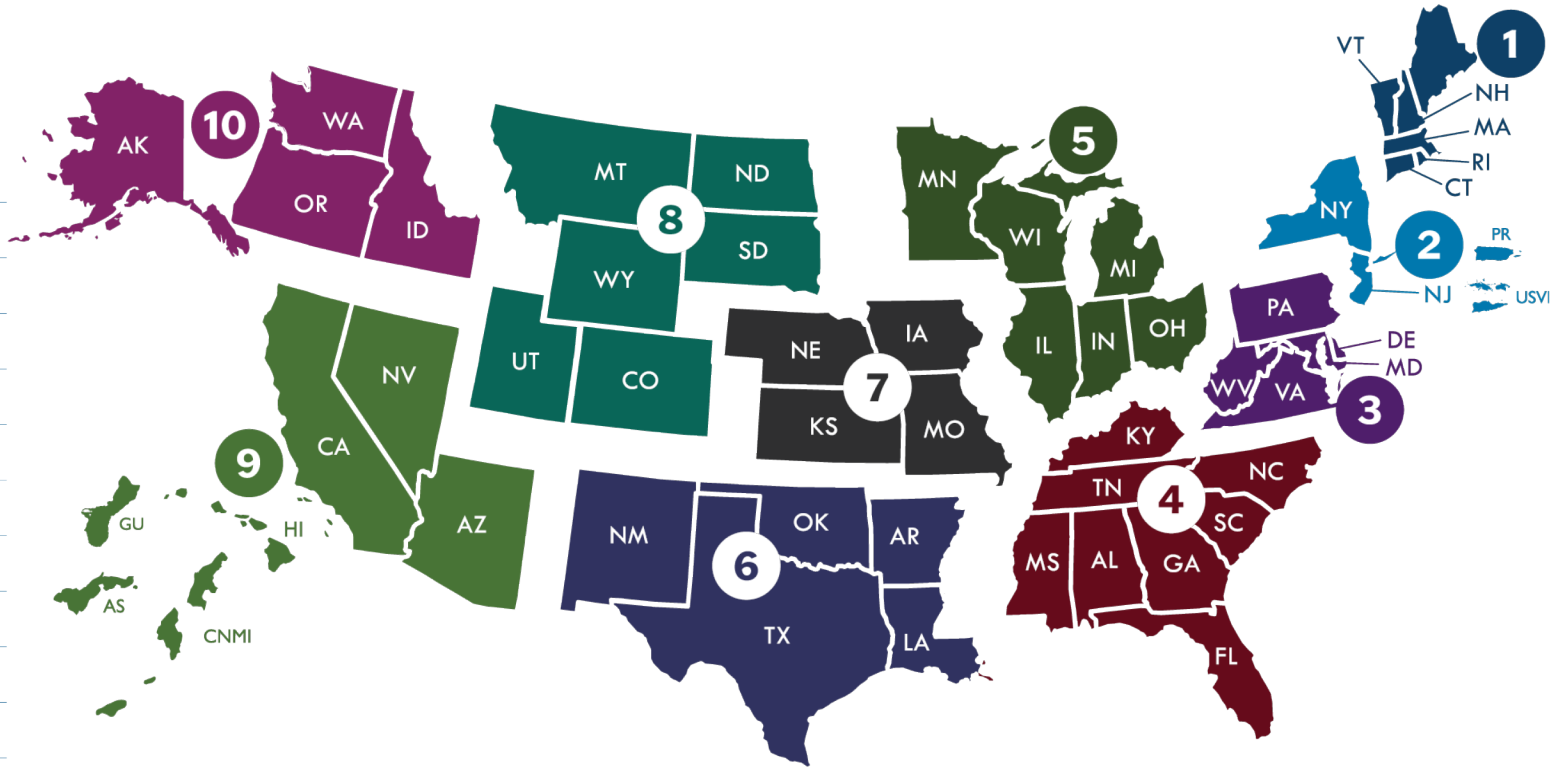
CISA's Integrated Operations Division enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



CISA.GOV/REGIONS

Critical Infrastructure Impact on the Nation

- 16 critical infrastructure sectors create a widely dispersed network, but sectors are interconnected and interdependent
- Critical infrastructure includes:
  - Vital physical and cyber systems, and networks
  - Thousands of essential energy, water and health facilities, transportation networks, agriculture, defense industry, information technology and other systems

CISA Scalable Services

Cyber Hygiene Services

Manage external threat surface with no-cost vulnerability and web application scanning

DotGOV (Public Organizations)

Managed top-level domain, easily identifiable as a government organization to protect against impersonation and hijacking

Priority Telecommunication Services

Government Emergency Telecommunication Service (GETS), Wireless Priority Service (WPS), and Telecommunication Service Priority (TSP)

Cyber Resiliency Toolkits

Evaluate current capabilities, identify improvement to resiliency, develop plans

Vulnerability Scanning (CyHy)

- Continuously monitor and assess Internet accessible network assets
- Identify exposed assets and exploitable vulnerabilities
- Weekly findings report
- Ad-hoc alerts on urgent findings

Web Application Scanning (WAS)

- Vulnerability scanning of publicly accessible web applications
- Identifies risky services, vulnerabilities, and misconfigurations
- Monthly and on-demand reports

Cyber Hygiene Services

Monitor and mitigate attack vectors to reduce organizational exposure to threats

- Typically reduce risk by 40% in the first 12 months
- Identify unmanaged vulnerabilities
- Increase accuracy and effectiveness of response activities
- Better visibility of security boundaries

Getting Started

Email: vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

CISA Field Delivered Services

Cyber Protective Visit (CPV)

Initial visit facilitated by local Security Advisors to assess interest in CISA services

Cyber Security Evaluation Tool (CSET)

Desktop assessment tool. Used to evaluate cybersecurity stance using recognized government and agency standards and recommendations.

Assessments (open enrollment / self service)

Non-technical assessment of the implementation of organizational cybersecurity controls

- Cybersecurity Performance Goals (CPG)
- Cyber Infrastructure Survey (CIS)
- External Dependencies Management (EDM)
- Ransomware Readiness Assessment (RRA)
- Incident Management Review (IMR)
- Cyber Resilience Review (CRR)

Tabletop Exercise

Functional test of organizational incident response plans

Technical Services (Invitation only)

In-depth technical review of cybersecurity control effectiveness

- Remote Penetration Test (RPT)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)

Intended to Be

- Easy to use and complete
  - 38 questions total
- Baseline set of cybersecurity practices
  - Applicable across critical infrastructure
  - Known risk-reduction value
- Benchmark for critical infrastructure operators
  - Measure and improve cybersecurity maturity
- Combination of recommended practices
  - For information and operational technology
  - Prioritized set of security practices
- Unique from other control frameworks
  - Consider not only the practices that address risk to individual entities, but also the aggregate risk to the Nation

Cybersecurity Performance Goals (CPGs)

A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques

CISA Technical Assessments

Remote Penetration Testing (RPT)

- 100% remote penetration test of network controls
- Potential vulnerabilities tested based on the potential level of damage and in coordination with the customer
- Determine susceptibility to an actual attack by infiltrating the target environment, using current, real-world tactics, techniques, and procedures
- Includes network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign

Risk and Vulnerability Assessment (RVA)

- Includes both off-site remote penetration test and on-site, in person assessment
- Identify weaknesses through network, system, and application penetration testing.
- Test stakeholder operational environment, using a standard, repeatable methodology to deliver actionable findings and recommendations.
- Analyze collected data to identify security trends across all RVA stakeholder environments

Validated Architecture Design (VADR)

- Created for Operational Technology (OT) and Industrial Control Systems (ICS)
- Test operational environment, using a standard, repeatable methodology to deliver actionable findings and recommendations
- Analysis and representation of network traffic, data flows, and device relationships
- Identifies anomalous communications flows

CISA Self-Service Products

Malcom

A powerful open-source network traffic analysis tool suite.

- PCAP, Zeek logs, Suricata alerts
- Supports many common protocols

Logging Made Easy

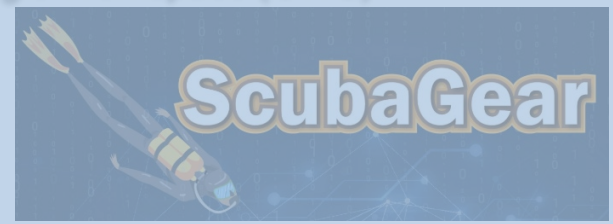
Open-source suite of tools used for centralized log collection for organizations that:

- Have limited resources
- Do not have an existing SOC, event and log management, and monitoring capabilities
- Need a log management and threat detection system

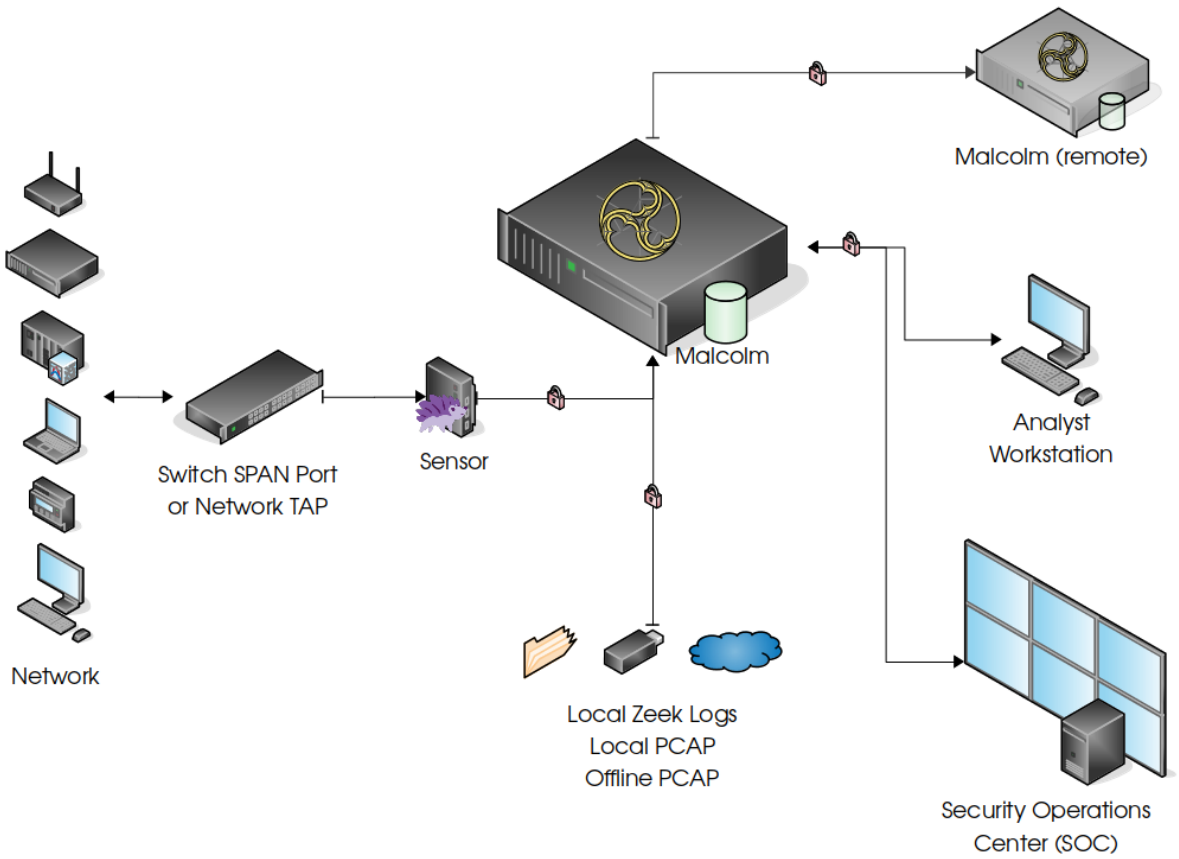
SCUBA

Secure cloud business application environments against CISA secure configuration baseline

- Microsoft tenant environments
- Google Workspace (GWS)



Malcolm

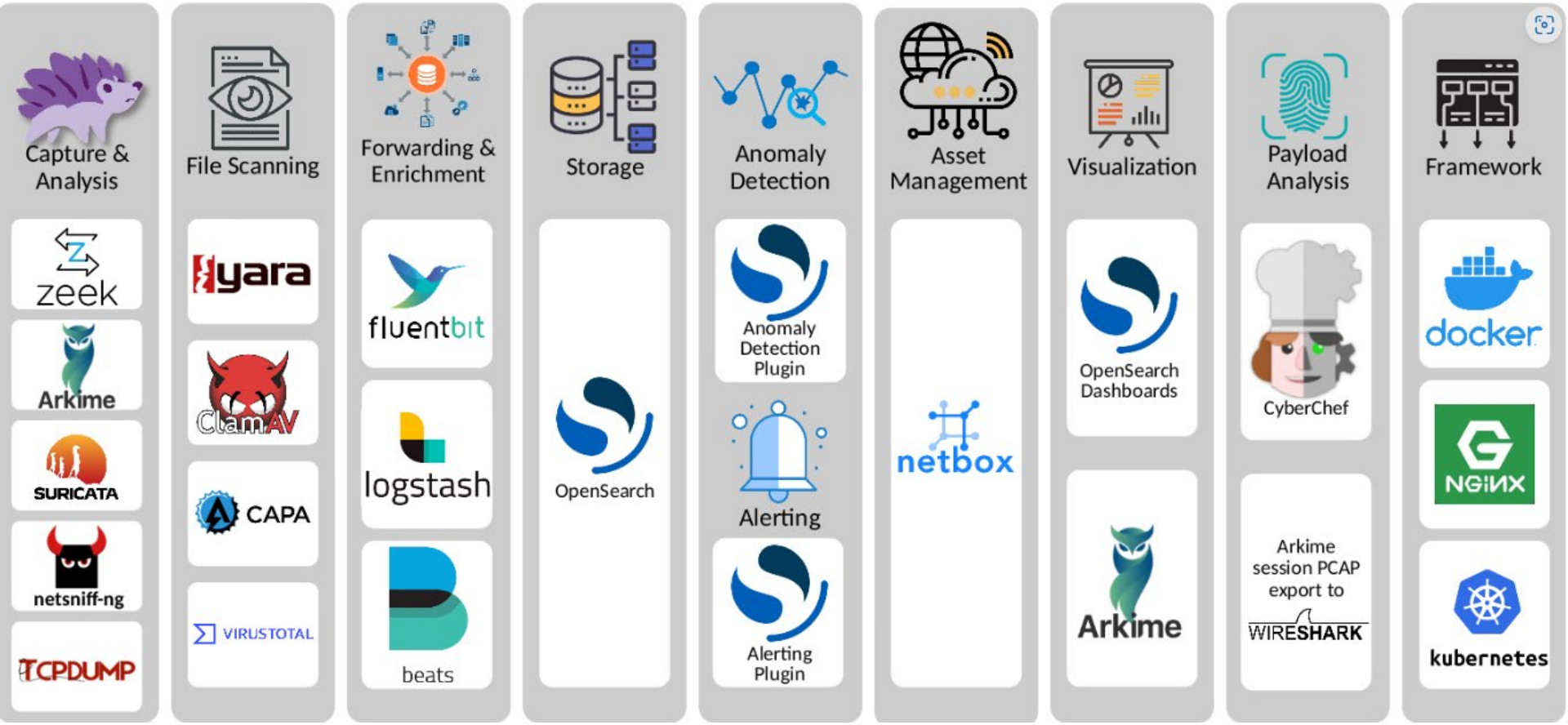


Easily deployable traffic analysis tool suite

- Open source and easy to use
- Full packet capture artifacts (PCAP) and Zeek logs
- Stream-lined deployment
- Secure communications
- Permissive license
- Full download available from CISA GitHub site

https://github.com/cisagov/Malcolm

Malcolm


Capture & Analysis
zeek
Arkime
SURICATA
netsniff-ng
TCPDUMP
File Scanning
yara
ClamAV
CAPA
VIRUSTOTAL
Forwarding & Enrichment
fluentbit
logstash
beats
Storage
OpenSearch
Anomaly Detection
Anomaly Detection Plugin
Alerting
Alerting Plugin
Asset Management
netbox
Visualization
OpenSearch Dashboards
Arkime
Payload Analysis
CyberChef
Arkime session PCAP export to
WIRESHARK
Framework
docker
NGINX
kubernetes

LOGGING MADE EASY

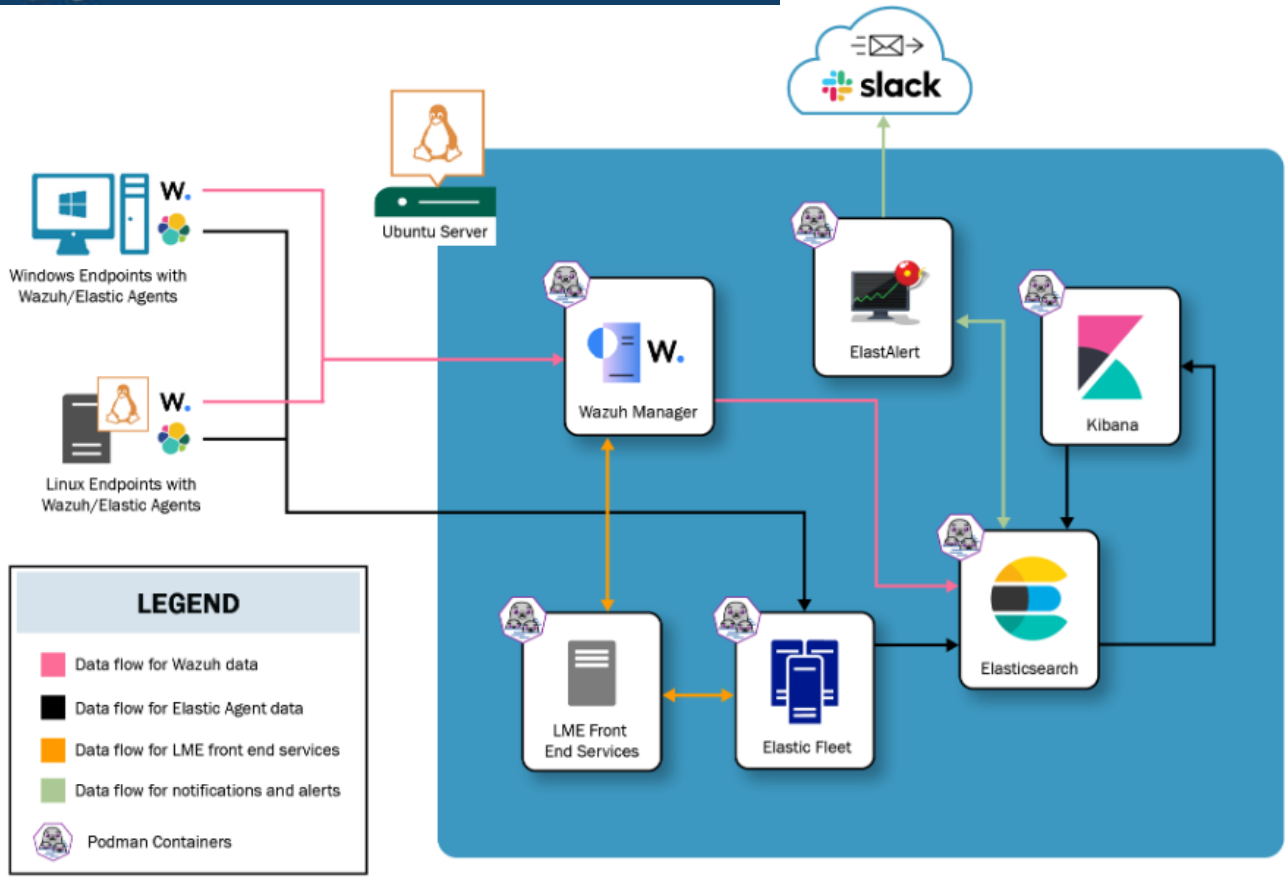
Threat detection solution for small to medium sized organizations that would have little to no functionality to detect attacks

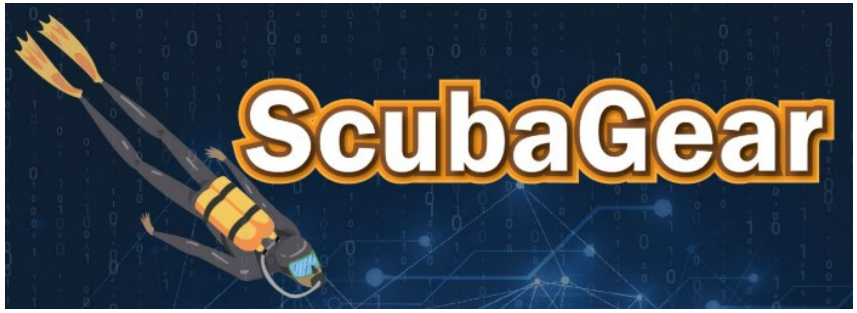
- Monitor networks, identify users, and actively analyze Sysmon data
- Log management and threat detection system
- Adaptable dashboards

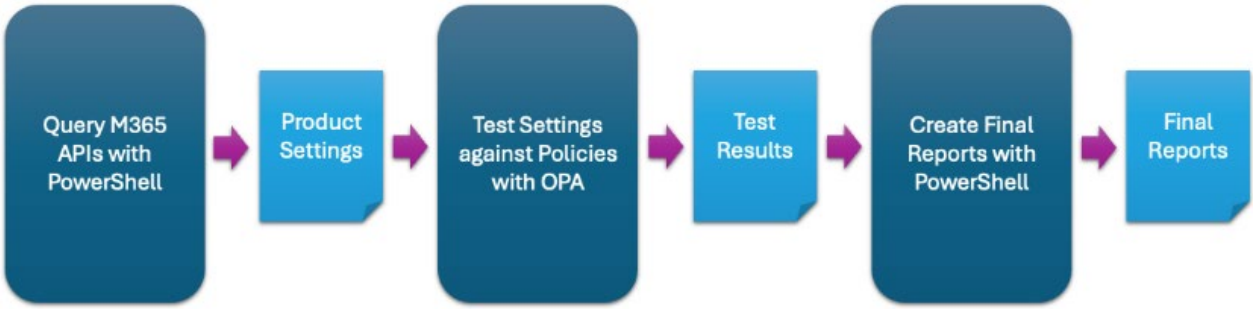
https://github.com/cisagov/LME

LOGGING MADE EASY

COMPONENT	PURPOSE
Elastic Agent	Collects Logs from Clients
Elastic Fleet	Elastic Agent Management
Wazuh Agent	Endpoint Security Monitoring & Response
Wazuh Manager	Wazuh Agent Management
ElastAlert	Framework for Notifications & Alerts
Elasticsearch	Log Storage, Query & Search
Kibana	Build Dashboards & Visualize Data
Podman	Container Management







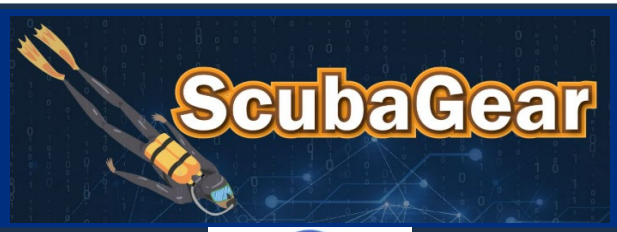
Secure cloud business application environments assessment tool using CISA secure configuration baselines

- SCUBA Gear - M365 tenet environments

https://github.com/cisagov/ScubaGear

- ScubaGoggles - Google Workspace (GWS)

https://github.com/cisagov/Scubagoggles



- Microsoft Entra ID
- Defender
- Exchange Online
- Power BI
- Power Platform
- SharePoint & OneDrive
- Teams

ScubaGoggles

- Common Controls
- Gmail
- Google Calendar
- Google Chat
- Google Classroom
- Google Drive and Docs
- Google Meet
- Google Sites
- Groups for Business

Available Secure Baselines

Vendor and Supplier Risk Awareness

Vendors / Suppliers

- Hold suppliers / manufactures accountable for the security outcomes of their products
- Develop purchasing criteria that emphasize the importance of secure by design
- Establishing policies requiring the security of software
- Prioritize purchases from vendors that practice Secure by Design concepts

Organization

- Accept the risks associated with specific technology products should be formally documented
- Obtain executive management support when enforcing these criteria in purchasing decisions
- Forge strategic relationships with their key IT suppliers
- Provide vehicles to resolve issues
- Expect transparency from their technology suppliers about internal control posture

Resources

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII)
Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is ***protected*** by law from
  - Public release under Freedom of Information Act (FOIA) requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.
- Required: Express and Certification Statement Form
- Find out more: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program

CISA Resources

- Known Exploited Vulnerabilities (KEV) Catalog
  - Current CVE list
  - Subscribe for automated KEV Catalog update bulletin
  - Find out more: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Automated Indicator of Sharing (AIS)
  - Real-time exchange of machine-readable cyber threat indicators and defensive measures
  - Setup STIX and TAXXI Feed for SEIM available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais/how-share-cyber-threat-information-through-ais
- Join the Joint Cyber Defense Collaborative (JCDC)
  - Public and private sector partnerships
  - Unify cyber defenders from organizations worldwide
  - Proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response
  - Find out more: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

Malicious Activity Resources

- StopRansomware.gov – CISA resources and guidance for ransomware information

https://www.cisa.gov/stopransomware

- Ransomware Vulnerability Warning Pilot (RVWP) - Proactive vulnerability notifications for Critical Infrastructure entities

https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) - Nationwide initiative to combat ransomware

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

Getting Ahead of the Ransomware Epidemic:

CISA's Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs

Incident Reporting

- CISA
  - Incident Reporting Center https://www.cisa.gov/forms/report
- FBI
  - Internet Crime Complaint Center (IC3) https://ic3.gov/default
- State of Oregon
  - State of Oregon SOC, ESO.SOC@das.oregon.gov, Phone: 503-378-5930
- MS-ISAC
  - Security Operation Center, soc@cisecurity.org, Phone: 866-787-4722

For more information:
https://www.cisa.gov/cyber-resource-hub

Region 10:
CISARegion10@cisa.dhs.gov

Leslie Ann Kainoa
Cybersecurity State Coordinator
Leslie.kainoa@cisa.gov
503-462-5626

Zeina Boulos
Cybersecurity Advisor
Zeina.boulos@cisa.gov
503-857-9342

Chris Ross
Federal Law Enforcement Liaison-
Cybersecurity Advisor
Christopher.k.ross@cisa.gov
503-979-4368

Chass Jones
Protective Security Coordinator
Chass.jones@cisa.gov
503-507-8822

Jason Salfen
Protective Security Advisor
Jason.salfen@cisa.gov
541-218-3111