



CYBERSECURITY AWARENESS MONTH

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Daniel Brown, CISSP, CISM
Cybersecurity Advisor (CSA)
Inland Northwest
Cybersecurity and Infrastructure Security Agency



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Agenda

- What is CISA?
- Protective Security Advisor (PSA) and Services
- Cybersecurity Advisor (CSA) and Services
- CISA Partnerships/ Initiatives
- Cyber Risk Landscape
- Cyber Tools (used by both sides)
- Security Planning/Incident Response resources



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

We lead the National effort
to understand, manage, and
reduce risk to our cyber and
physical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023



SECURE.
OURWORLD

CYBERSECURITY AWARENESS MONTH

The Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Securing Critical Infrastructure

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



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Region 10

CISA Regions



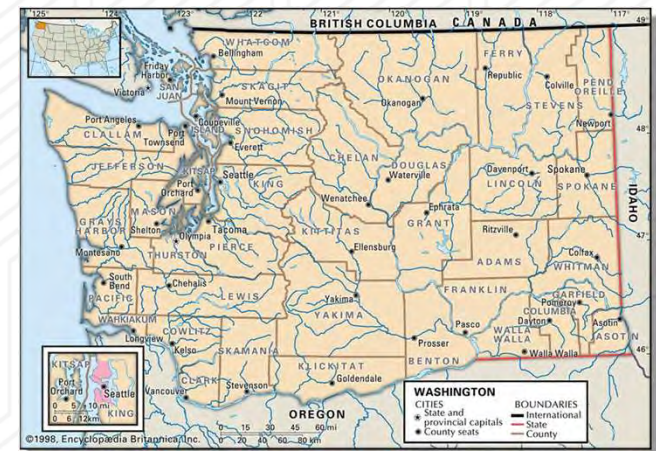
CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

State, Local, and Tribal Governments and Private Industry

As Nations Risk Advisors, support all governments within the United States of America with their cybersecurity.

- **State government and executive agencies**
- **City governments**
- **Tribal governments**
- **County governments**
- **K-12 Education**
- **Higher Education**
- **Private Industry is supported for 16 Critical Infrastructure Sectors.**



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

CISA Protective Security Advisors (PSA)

PSAs are physical security & resiliency subject matter experts who engage with Federal, State, local, tribal, and territorial (FSLTT) government mission partners and members of the private sector stakeholder community to protect the nation's critical infrastructure.

- Plan, coordinate, and conduct security surveys and assessments
- Plan and conduct outreach activities
- Support National Special Security Events (NSSE) and Special Event Activity Rating (SEAR) events
- Respond to significant natural or man-made incidents
- Coordinate and support improvised explosive device awareness and risk mitigation training



CISA Protective Security Advisors (PSA)

PSA's provide access to tools and resources to support physical security and resilience.

- Active Shooter Preparedness
- Bombing Prevention
- Insider Threat Mitigation
- Non-Confrontational Techniques
- Protecting Houses of Worship
- School Safety
- Securing Public Gatherings
- Unmanned Aircraft Systems
- Vehicle Ramming Mitigation



CISA PSA Assessments & Services

Assist Visit -----

Security Assessment at First Entry (SAFE) -----

Infrastructure Survey Tool (IST) -----

Multi-Asset and System Assessment (MASA) -----

Regional Resiliency Assessment Program (RRAP) -----



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

Cybersecurity Advisor (CSA) Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.



CISA Assessments and Services



Cyber Protective Visit (CPV) – discuss stakeholder environment and appropriate CISA services



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

CISA Partnerships



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

CISA Threat Intel Collaboration

Joint Cyber Defense Collaborative (JCDC)

- JCDC is a public-private cybersecurity collaborative that leverages new authorities granted by Congress in the 2021 NDAA.
- JCDC collaborates with over 100 international cyber defense organizations, often known as “CERTs,” to ensure that information about cyber threat is disseminated.
 - PNW Examples:
 - Initial Access Brokers selling credentials/access.
 - Breached data for sale.
 - Pre-Ransomware/Ransomware
 - Known Exploited Vulnerability (KEV) present on a system.



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



MS-ISAC (and other industry-specific ISAC's)



CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).



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

The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.



**Elections
Infrastructure
ISAC®**

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.



CIS is home to the MS-ISAC and the EI-ISAC

- **Multi-State Information Sharing and Analysis Center**
- **The mission of the MS-ISAC is to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication.**



CISA
CYBER+INFRASTRUCTURE

PNNL Test lab for drinking Water and Wastewater treatment



Operational Technology (OT) networks – convergence with IT networks



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

CISA Initiatives



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM)

- Key building block in Software Security.
 - A SBOM is a nested inventory, a list of ingredients that make up software components.

SBOM resources

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



Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.



Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

Secure by Design / Secure by Default

Secure by Design requirements include:

- The security of the customers is a core business requirement
- Security principles should be implemented during the design phase of a product's development lifecycle

Secure by Default features include:

- Products that are secure to use out of the box
- No additional cost for security features (i.e. MFA)
- Gather & log evidence of potential intrusions
- Control access to sensitive information

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



Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

CISA Initiative

Ransomware/Pre-Ransomware Notifications

2023 Pre-Ransomware Notifications

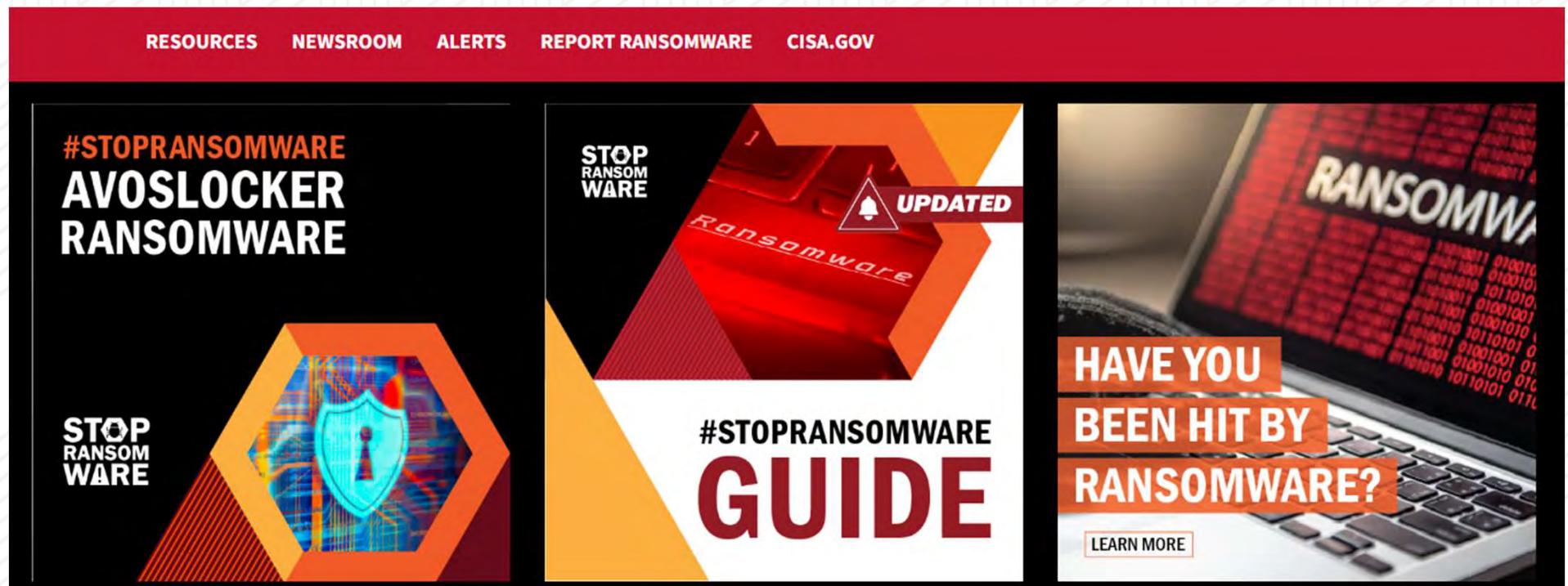
Year to-date, CISA has conducted over 150 pre-ransomware notifications, including over 40 notifications to our international partners. Some quick specifics include: 3 K-12 school districts, 4 institutions of higher education, 9 other state and local organizations, and 10 Healthcare organizations.

Many of these notifications have helped organizations mitigate effects before threat actors have been able to fully compromise systems/networks.



New resources for Ransomware

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



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

CISA and CIRCIA Reporting (coming soon.....)



- In March 2022, President Biden signed into law the **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)**.
- Requires CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA by 2025.
- Details/processes are still being formulated.
- Organizations should report unusual cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.
- Currently voluntary sharing of information about cyber incidents
- More information at www.cisa.gov/CIRCIA



Cyber Risk Landscape



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Cybersecurity statistics from FBI Internet Crime Complaint Center (IC3.gov)

- FBI IC3 2023 Report →
 - 3.26 million total complaints
 - \$27.6 Billion Total Losses
 - Networth of YouTube ~\$25 Billion
 - 870x Ransomware Victims
 1. Healthcare
 2. Critical Manufacturing
 3. Government Facilities
- Washington State was ranked 10th in terms of victim in the US.
- 58% increase in number of published vulnerabilities since 2017.
 - 2022 = ~25k Vulnerabilities.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Additional alerts from www.IC3.gov

Consumer Alerts

- [Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers](#)
Wed, 18 Oct 2023 15:00:00 EDT
- [Cybercriminals are Targeting Plastic Surgery Offices and Patients](#)
Tue, 17 Oct 2023 15:00:00 EDT
- [Situation in Israel](#)
Tue, 10 Oct 2023 18:40:00 EDT
- ["Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings](#)
Fri, 29 Sep 2023 09:00:00 EDT
- [Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material](#)
Tue, 12 Sep 2023 09:00:00 EDT

Industry Alerts

- [#StopRansomware Guide](#)
Thu, 19 Oct 2023
- [Phishing Guidance: Stopping the Attack Cycle at Phase One](#)
Wed, 18 Oct 2023
- [Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default](#)
Mon, 16 Oct 2023
- [Threat Actors Exploit Atlassian Confluence CVE-2023-22515 for Initial Access to Networks](#)
Mon, 16 Oct 2023
- [Improving Security of Open Source Software in Operational Technology and Industrial Control Systems](#)
Wed, 11 Oct 2023



CISA
CYBER+INFRASTRUCTURE

Cyber Insurance Trends

Insurers Have Responded By
Making Insurance Harder To
Qualify For, Pulling Back On Limits
And Available Coverages



Minimum Requirement Insurers Are Looking For

- ☒ MFA--multifactor authentication.
- ☒ Password Hygiene.
- ☒ Encryption/secure communication and payment channels.
- ☒ Data management plan and secure data storage.
- ☒ Screening-employees, vendors, independent contractors, clients, service and IT providers.
- ☒ Training for staff re: phishing, social engineering.
- ☒ Two Person authentication for larger transactions.
- ☒ Annual Cyber Security Audit.
- ☒ Formal Breach Response and Disaster Recovery Plan



CISA
CYBER+INFRASTRUCTURE

An Expanding Attack Surface



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

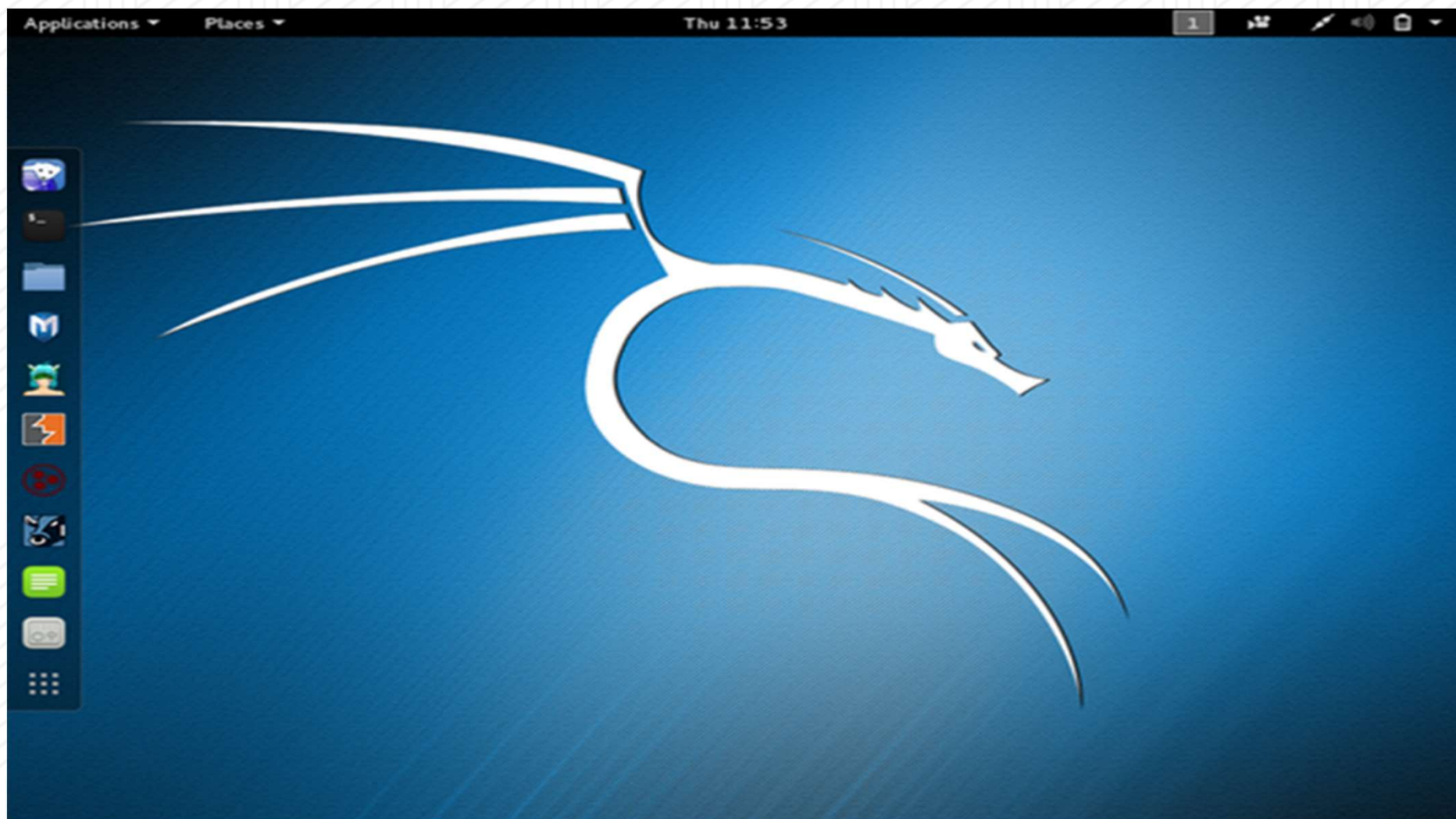
Cyber Tools



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

With Tools Aimed Directly At You



























CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Tools used by adversaries, or to protect from them

Kali Linux tools

From sources across the web

 Wireshark	 Nmap	 Metasploit
 Burp Suite	 Aircrack-ng	 Sqlmap
 Nikto	 John the Ripper	 Ettercap
 Maltego	 Kismet	 ZAP
 Tcpdump	 Nessus	 W3af
 Armitage	 Lynis	 Autopsy
 Hashcat	 Skipfish	 OpenVAS
 Snort	 Netcat	 RouterKeygen



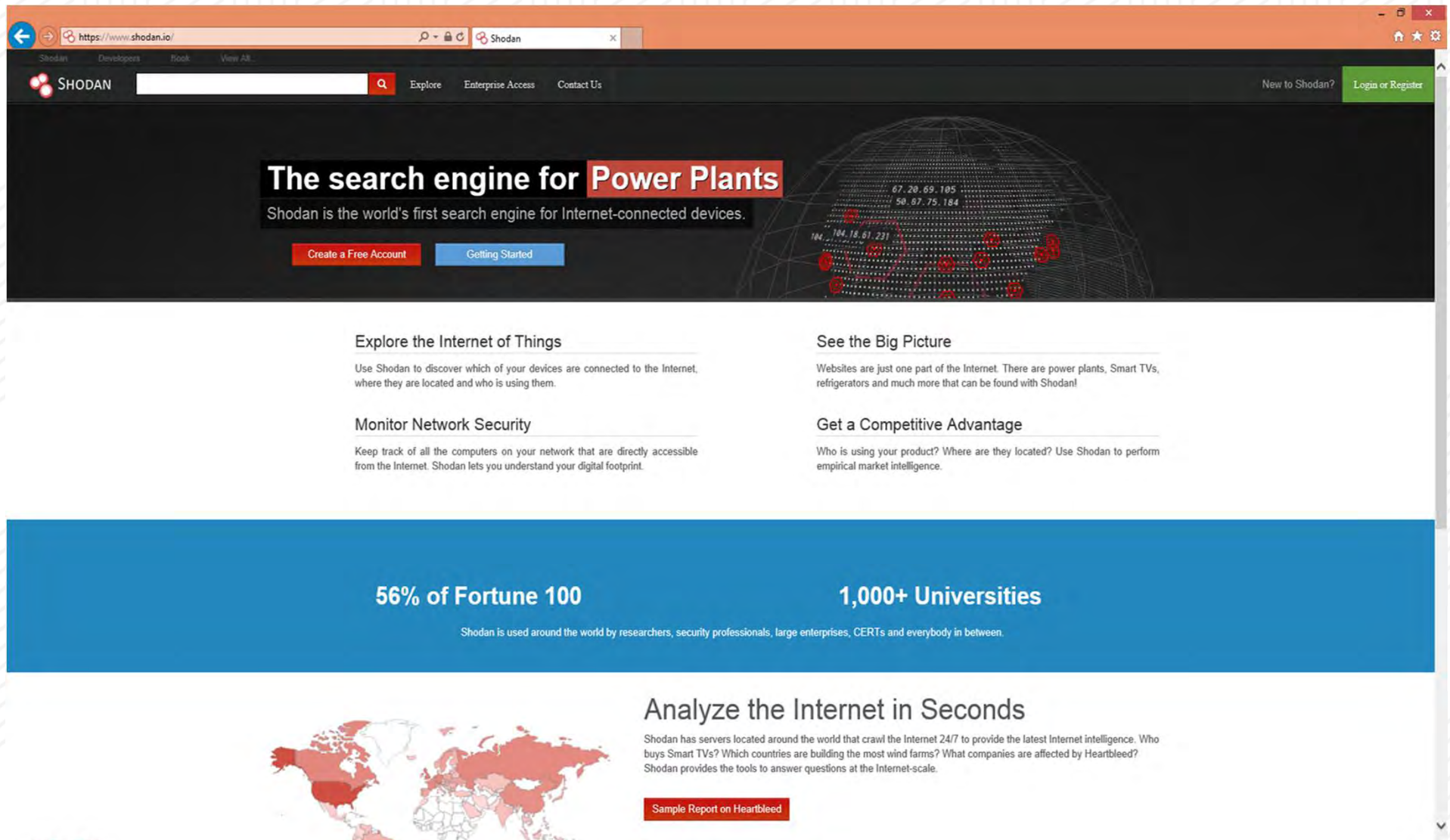
CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

Tools used to identify vulnerabilities

Shodan



The screenshot shows the Shodan website homepage. The browser address bar displays 'https://www.shodan.io/'. The website has a dark header with the Shodan logo, a search bar, and navigation links: 'Explore', 'Enterprise Access', and 'Contact Us'. On the right of the header, there are links for 'New to Shodan?' and 'Login or Register'. The main content area features a large banner with the text 'The search engine for Power Plants' and 'Shodan is the world's first search engine for Internet-connected devices.' Below this banner are four columns of text describing the tool's capabilities: 'Explore the Internet of Things', 'Monitor Network Security', 'See the Big Picture', and 'Get a Competitive Advantage'. A blue section below these columns highlights '56% of Fortune 100' and '1,000+ Universities' using Shodan. At the bottom, there is a world map and a section titled 'Analyze the Internet in Seconds' with a link to a 'Sample Report on Heartbleed'.

<https://www.shodan.io/>

SHODAN

Explore Enterprise Access Contact Us

New to Shodan? Login or Register

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

Shodan – search on device metadata

The screenshot displays the Shodan search engine interface. At the top, a navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More... Below this is a search bar with the query 'http.html:nginx Country:US State:WA City:Pullman' and a search button. The results page shows 83 total results. On the left, there are sections for 'TOP PORTS' and 'TOP ORGANIZATIONS'. The 'TOP PORTS' section lists ports 80, 443, 81, 3000, and 5357 with their respective counts. The 'TOP ORGANIZATIONS' section lists Washington State University, Ziplly Fiber, FIRST STEP INTERNET, LLC, Charter Communications Inc, and Advanced Hardware Architectures. The main content area displays two search results. The first result is for 'Test Page for the Nginx HTTP Server on AlmaLinux' with IP 134.121.22.147, showing HTTP headers and a timestamp of 2023-09-17T02:32:36.599718. The second result is for 'Welcome to nginx!' with IP 50.52.114.95, showing an SSL certificate and a timestamp of 2023-09-16T22:43:53.140810.

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | http.html:nginx Country:US State:WA City:Pullman | Account

TOTAL RESULTS

83

TOP PORTS

Port	Count
80	58
443	20
81	1
3000	1
5357	1

More...

TOP ORGANIZATIONS

Organization	Count
Washington State University	52
Ziplly Fiber	16
FIRST STEP INTERNET, LLC	8
Charter Communications Inc	3
Advanced Hardware Architectures	2

More...

TOP PRODUCTS

View Report | Download Results | Historical Trend | View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Test Page for the Nginx HTTP Server on AlmaLinux [↗](#) 2023-09-17T02:32:36.599718

134.121.22.147
[Washington State University](#)
United States, Pullman

eo-product

HTTP/1.1 200 OK
Server: nginx/1.14.1
Date: Sun, 17 Sep 2023 02:32:36 GMT
Content-Type: text/html
Content-Length: 3854
Last-Modified: Mon, 19 Apr 2021 10:05:11 GMT
Connection: keep-alive
ETag: "607d55d7-f0e"
Accept-Ranges: bytes

Welcome to nginx! [↗](#) 2023-09-16T22:43:53.140810

50.52.114.95
[vanvanmojo.kallisti.us](#)
[Ziplly Fiber](#)
United States, Pullman

eo-product

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
vanvanmojo.kallisti.us

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Sat, 16 Sep 2023 22:43:53 GMT
Content-Type: text/html
Content-Length: 612
Last-Modified: Sun, 21 Mar 2021 19:59:21 GMT
Connection: keep-alive
ETag: "6057a599-264"
Accept-Ranges: bytes



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Shodan

“Savvy searchers can find heating and security control systems for condominium buildings, banks, universities and corporate giants.”

-Forbes, [The Crazy Things A Savvy Shodan Searcher Can Find Exposed On The Internet](#), September 2013

Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023

Chatgpt — “ask precision farm equipment manufacturer how they secure their systems”

1. What measures do you have in place to ensure the security of your precision farming equipment?
2. How do you protect against potential cyber attacks or data breaches?
3. Do you conduct regular security assessments or penetration testing on your systems?
4. How do you manage access to sensitive data and ensure only authorized personnel have access?
5. How do you ensure the security of data transmissions between the equipment and the cloud or other systems?
6. What security protocols are in place to protect against unauthorized modifications to the equipment's firmware or software?
7. How do you keep your software and firmware up to date with security patches and updates?
8. Do you provide security training to your employees and customers?
9. Do you have a system in place for reporting and addressing potential security vulnerabilities or incidents?
10. What certifications or standards do you comply with to ensure the security of your equipment and systems?



SECURITY PLANNING WORKBOOK

Incident Response Resources



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Security Planning Workbook



Objectives

- Provide an overview of topics, resources, products, and practical knowledge to help organizations build a holistic security plan.
- Guide security planners through the risk assessment process to mitigate potential impacts to people and property.



Audience

- Individuals involved in an organization's security planning efforts, including individuals or groups with varying degrees of security expertise, charged with safety and security for people and property.



The **Security Planning Workbook** helps critical infrastructure owners and operators develop a foundational security plan.

Available 9/18/2023:

cisa.gov/resources-tools/resources/security-planning-workbook



CISA
CYBER+INFRASTRUCTURE

Security Planning Workbook Framework

CRITICAL ACTIONS



Identify Planning Team: Develop and implement identified security practices.



Understand Risk: Organizations should identify potential threats and hazards, as well as consider the consequences to determine and prioritize risk.



Mitigate Risk: The decision to accept and mitigate risk is unique to each organization and should be based on its goals, objectives, and available resources.



Develop Plan: Create security and emergency action plans to document steps personnel should take to prepare for, respond to, and recover from an incident.



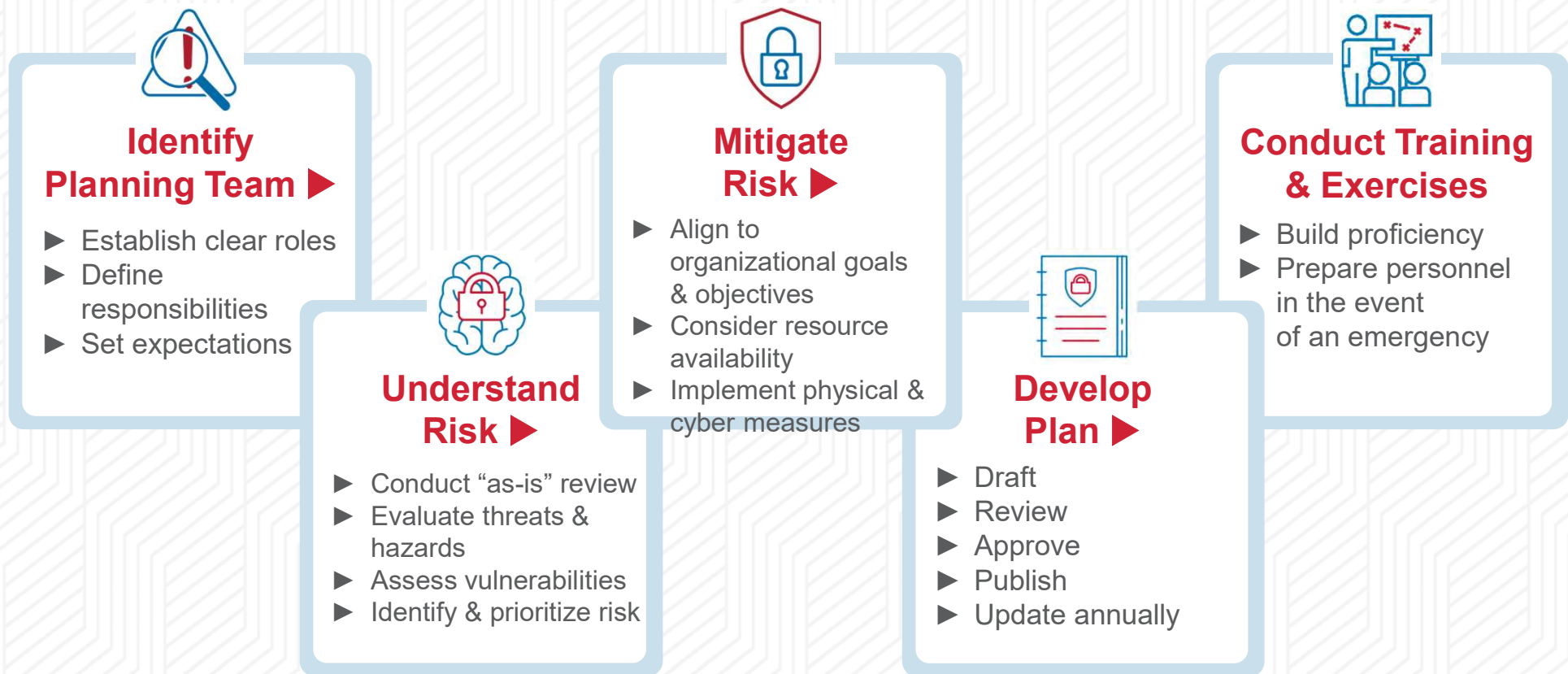
Conduct Training & Exercises: Develop and regularly practice effective training and exercise programs to prepare for emergency situations.



CISA
CYBER+INFRASTRUCTURE

Security Planning Workbook

Critical Actions: Key Steps



CISA
CYBER+INFRASTRUCTURE

Security Planning Workbook

Security Planning Workbook

<https://www.cisa.gov/resources-tools/resources/security-planning-workbook>



CISA
CYBER+INFRASTRUCTURE

Incident Response Resources

- Incident Response Planning
- Incident Response References:
 - CISA.gov - “Incident Response Plan”
 - CISA.gov - “Incident Response Training”
 - <https://www.cisa.gov/resources-tools/programs/Incident-Response-Training>
 - CISA.gov – “Cyber Incident Response”
 - NIST - Computer Security Incident Handling Guide (NIST SP 800-61)
- CISA Assessments and Services.....



Questions?



Daniel Brown
Region 10 (Inland Northwest)
Cybersecurity Advisor
(509) 981-9920
daniel.brown@cisa.dhs.gov



Steve Neal
Region 10 (Eastern WA)
Protective Security Advisor
(509) 216-2534
steven.neal@cisa.dhs.gov

CISA Resources

For inquiries or further information,
contact central@cisa.dhs.gov



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 24, 2023