SECURE OUR WORLD

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

SECURE OUR WORLD

CYBERSECURITY AWARENESS MONTH

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

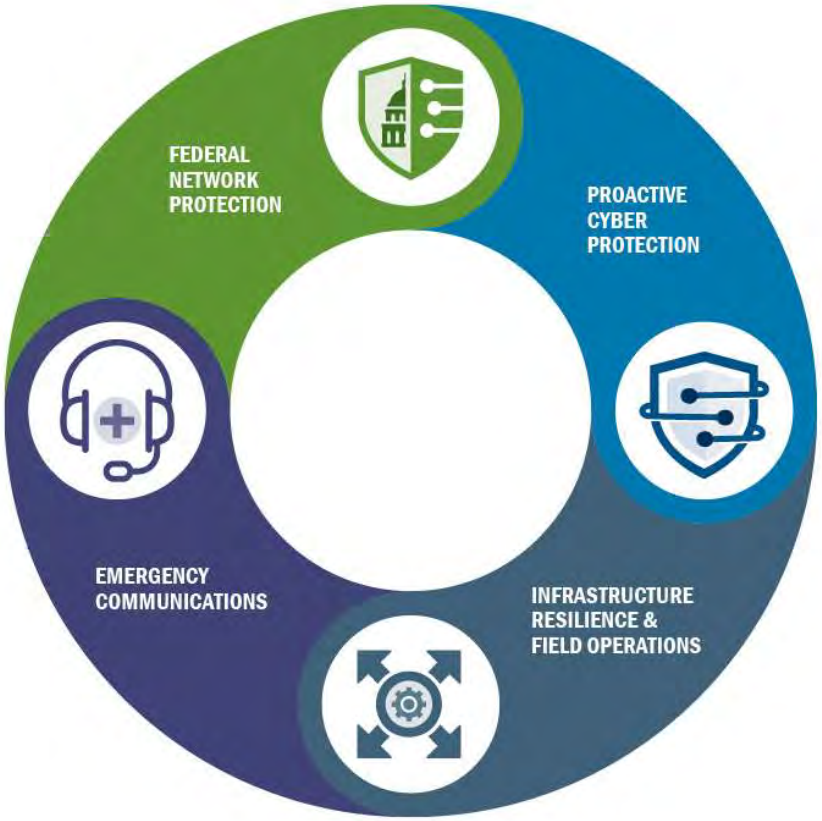
Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

SECURE OUR WORLD

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

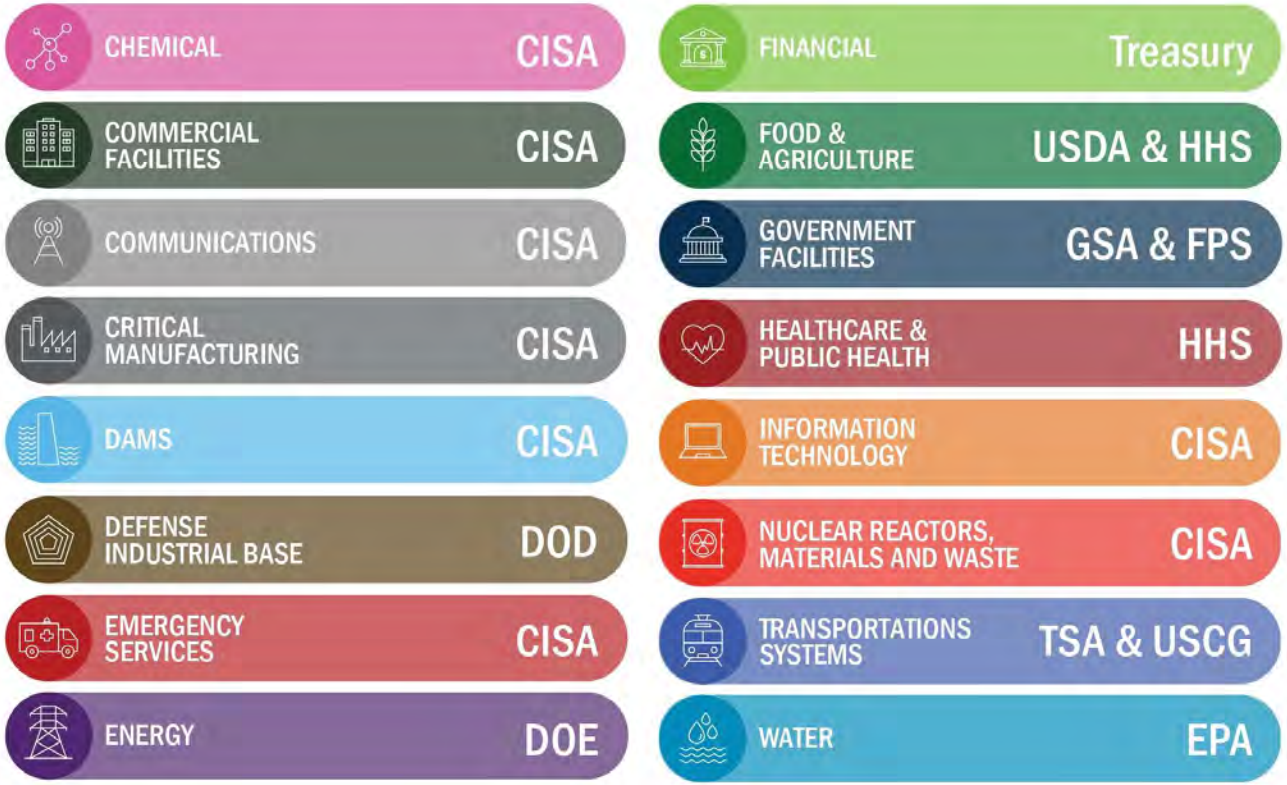


CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 24, 2023

Securing Critical Infrastructure

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

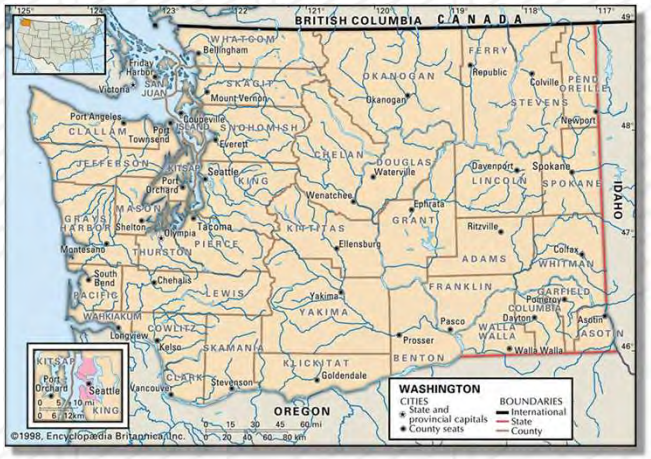


Region 10

CISA Regions

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 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) ----------

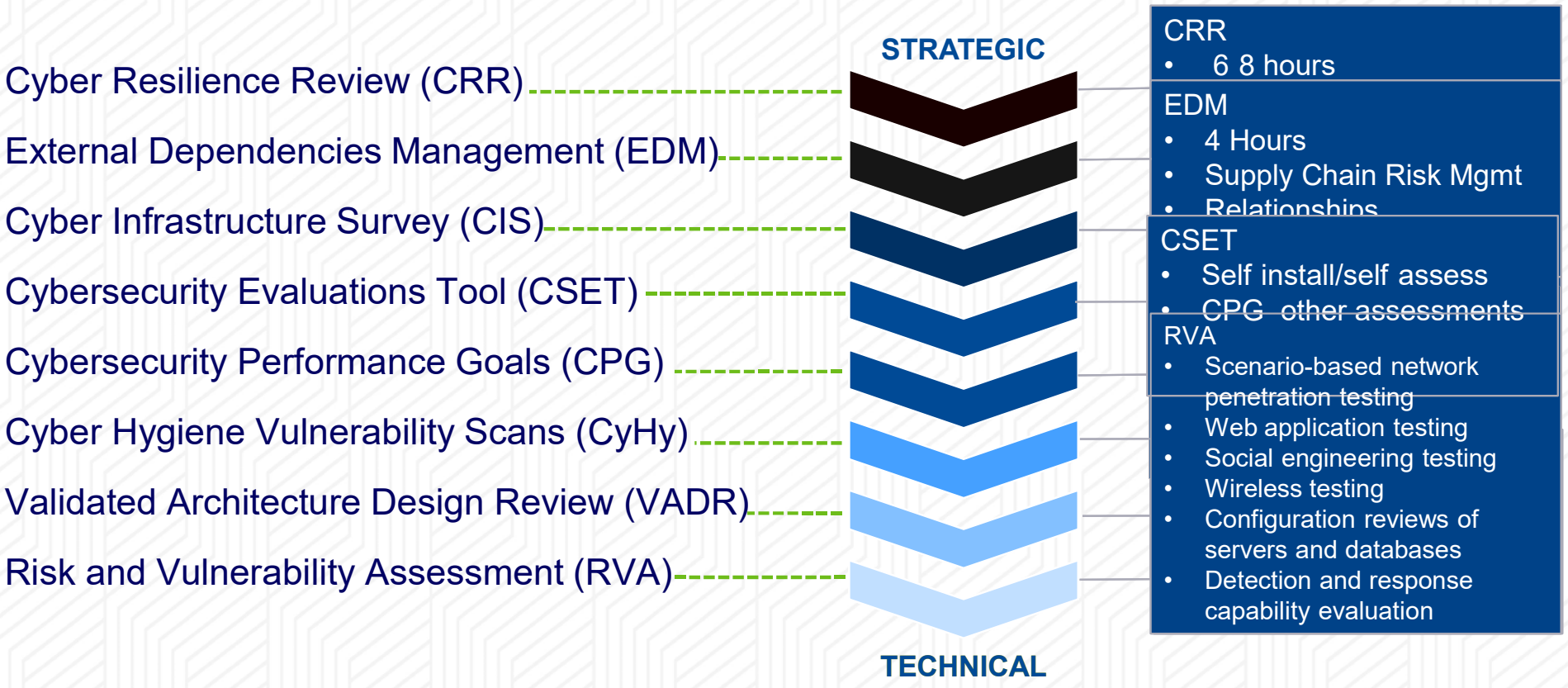
Cybersecurity Advisor (CSA) Program

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 Partnerships

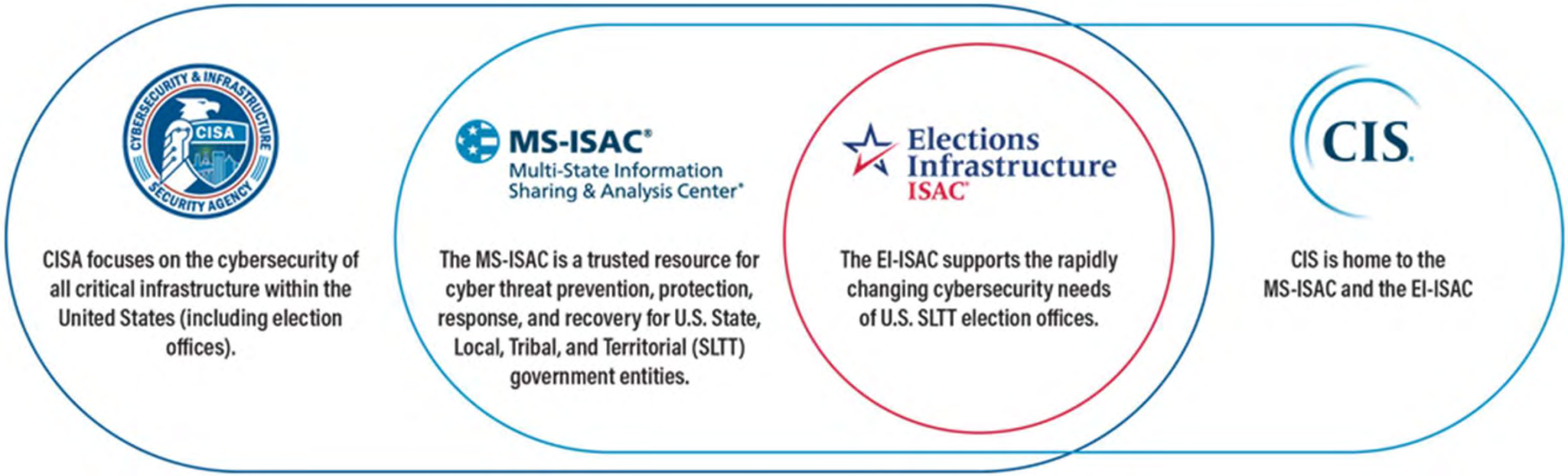
CISA Threat Intel Collaboration

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.

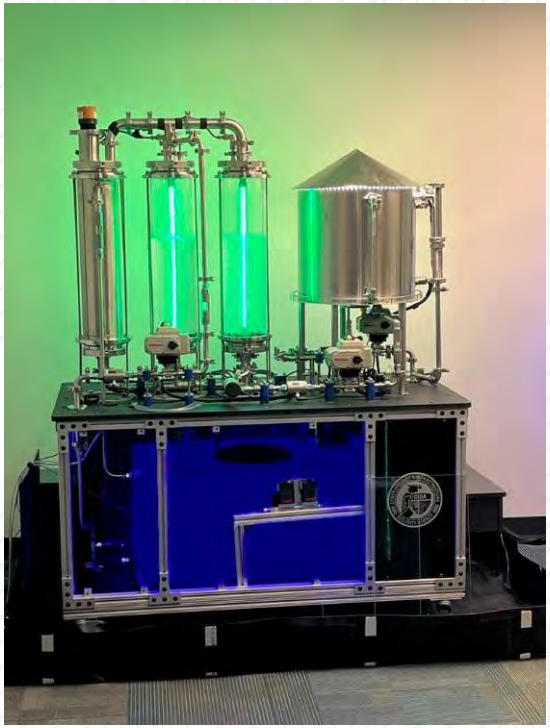
https://www.cisa.gov/jcdc

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



- **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.**

PNNL Test lab for drinking Water and Wastewater treatment



Operational Technology (OT) networks – convergence with IT networks

CISA
CYBER+INFRASTRUCTURE

CISA Initiatives

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.

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 ydesign

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 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

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.

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

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

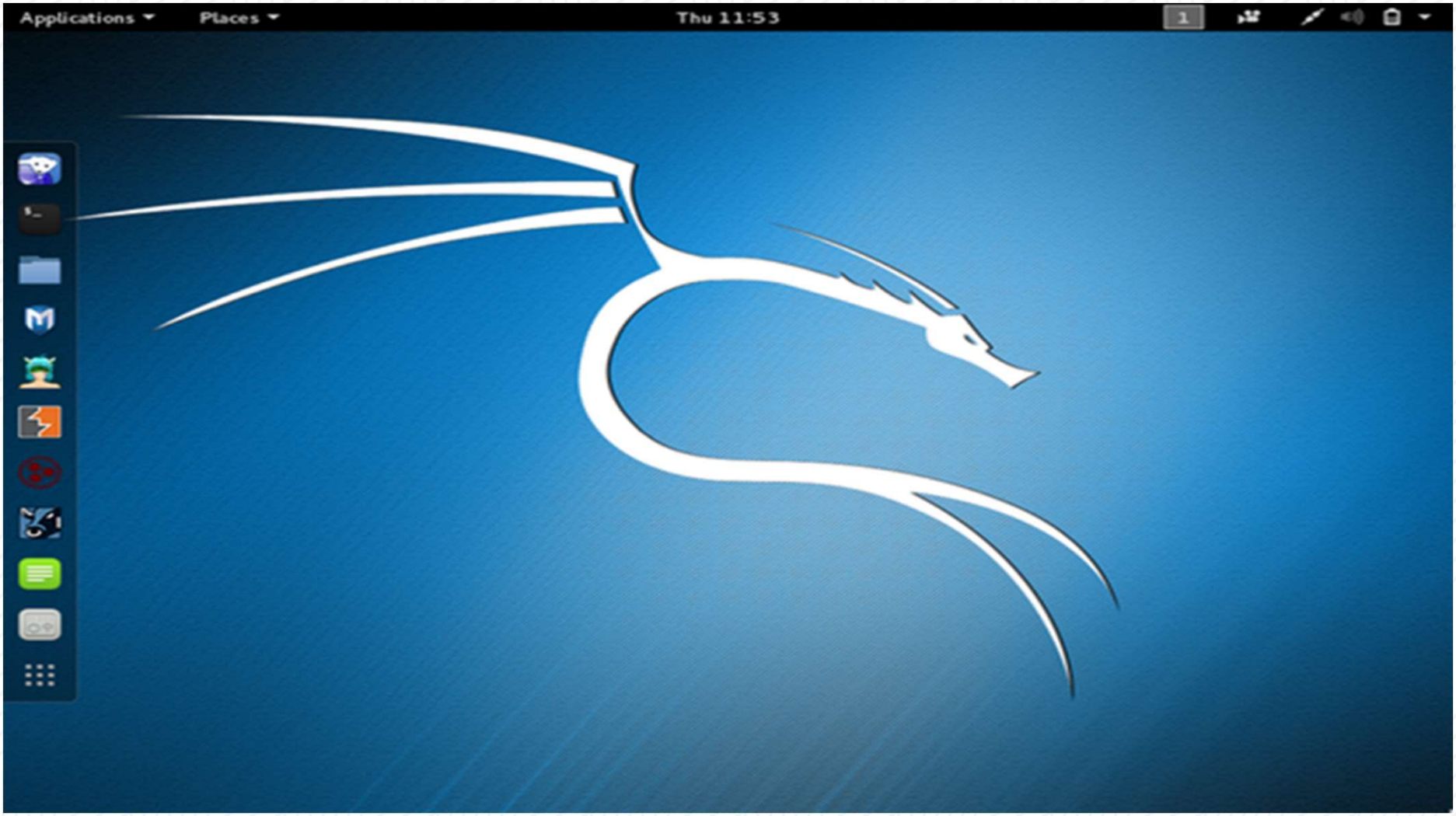
CISA CYBER+INFRASTRUCTURE

An Expanding Attack Surface

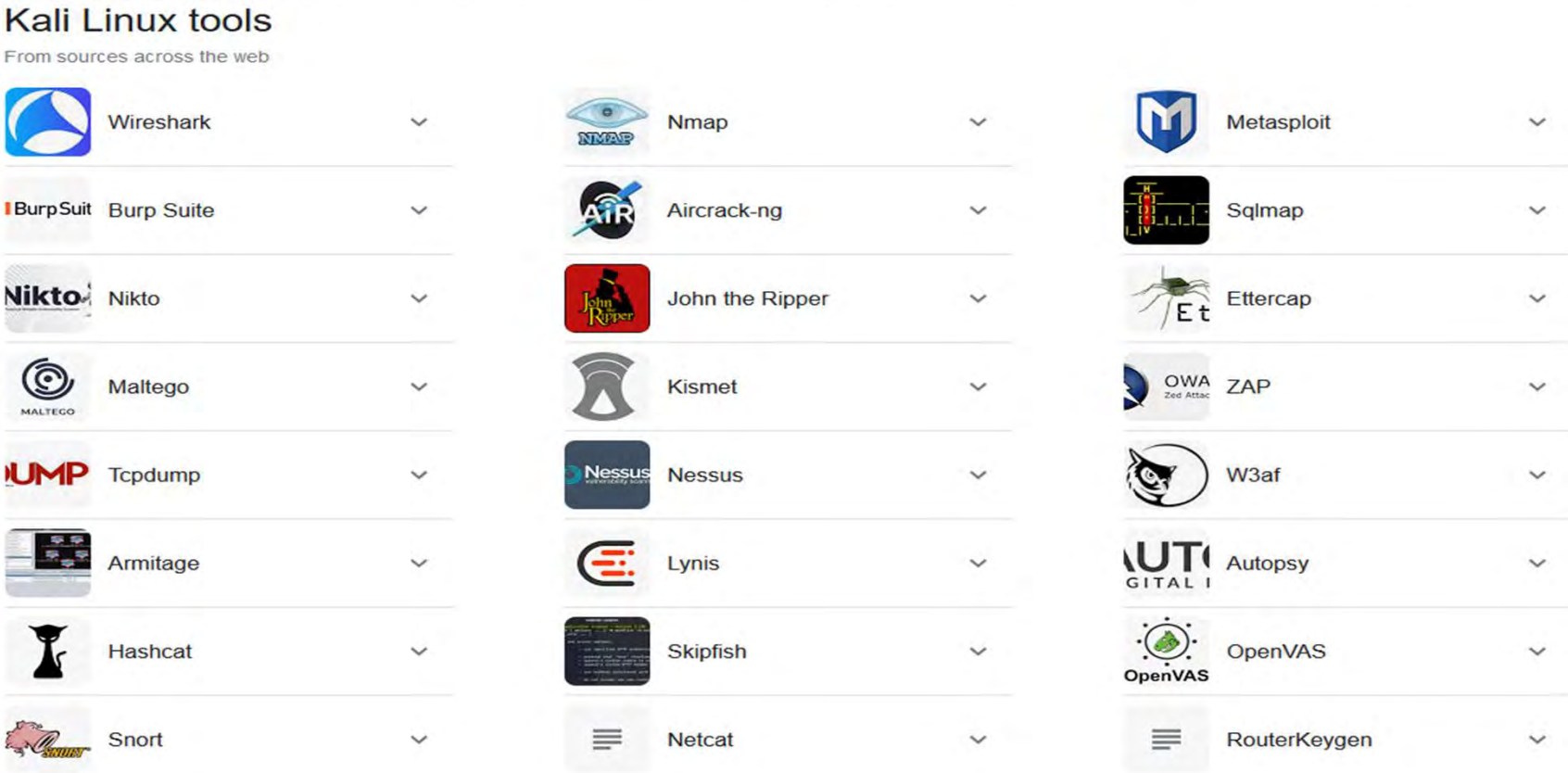
CISA
CYBER+INFRASTRUCTURE

Cyber Tools

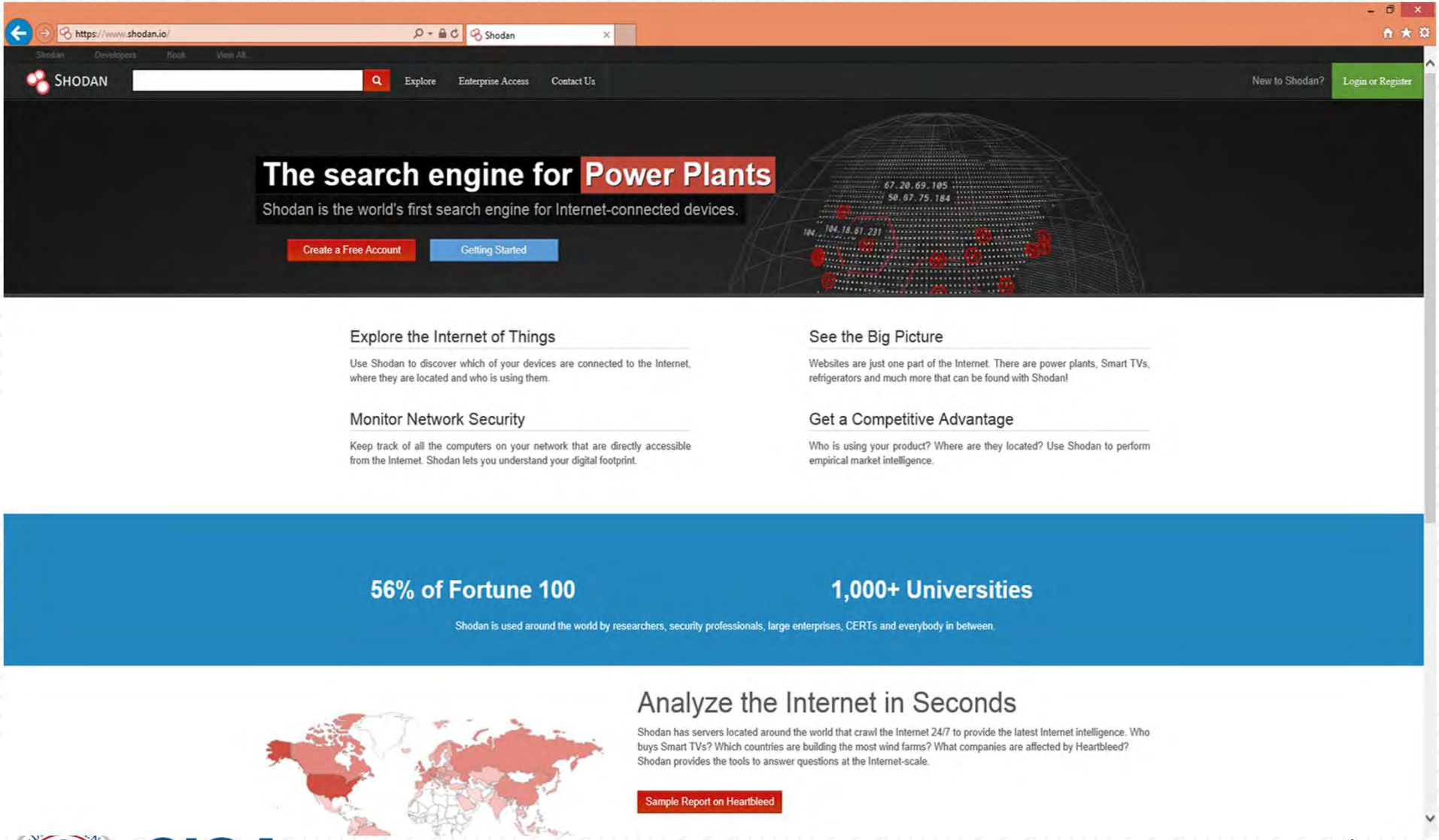
With Tools Aimed Directly At You



Tools used by adversaries, or to protect from them

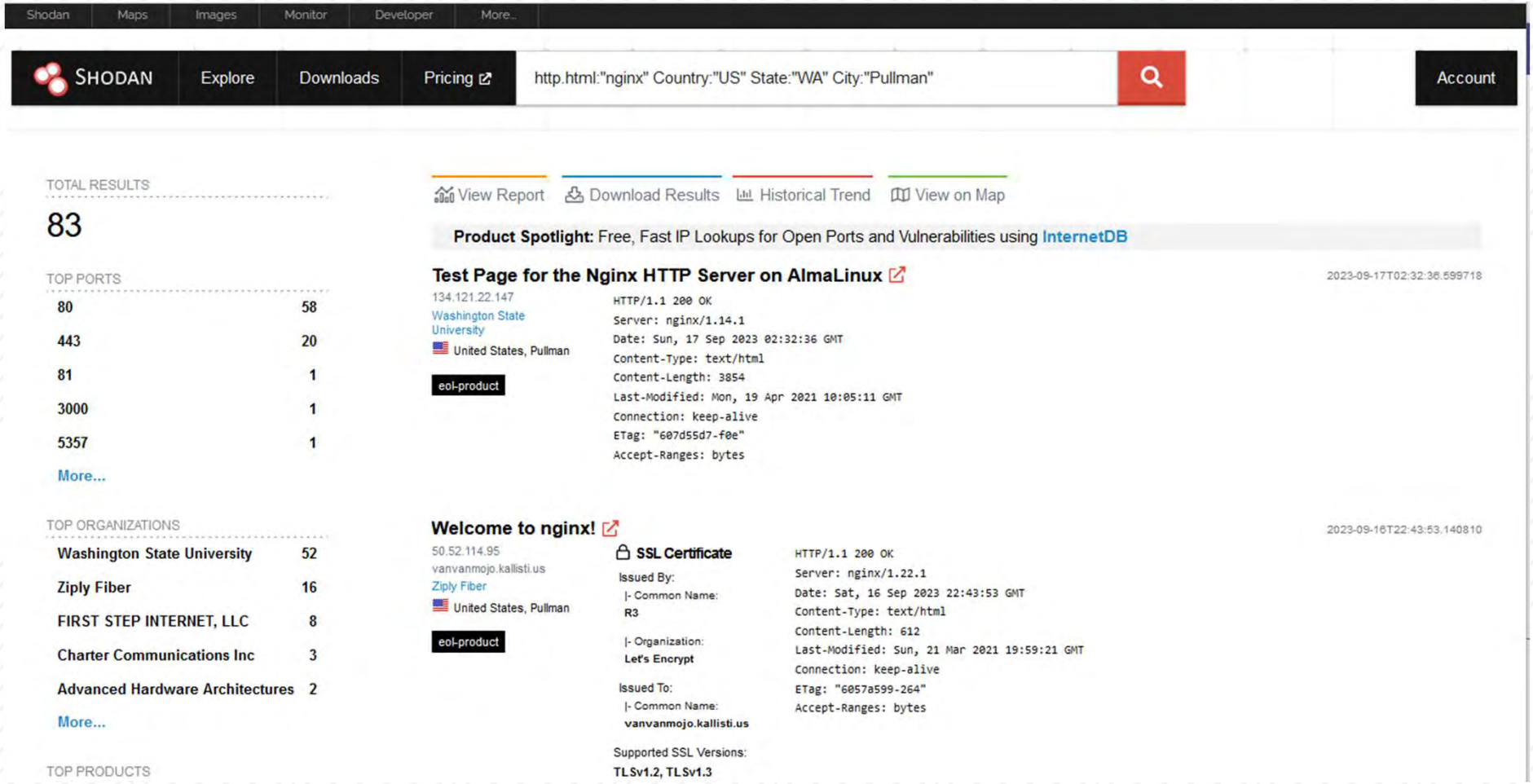


Tools used to identify vulnerabilities
Shodan



CISA
CYBER+INFRASTRUCTURE

Shodan – search on device metadata



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

CISA
CYBER+INFRASTRUCTURE

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

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.

Security Planning Workbook
Critical Actions: Key Steps

Identify Planning Team ▶

- Establish clear roles
- Define responsibilities
- Set expectations

Understand Risk ▶

- Conduct “as-is” review
- Evaluate threats & hazards
- Assess vulnerabilities
- Identify & prioritize risk

Mitigate Risk ▶

- Align to organizational goals & objectives
- Consider resource availability
- Implement physical & cyber measures

Develop Plan ▶

- Draft
- Review
- Approve
- Publish
- Update annually

Conduct Training & Exercises

- Build proficiency
- Prepare personnel in the event of an emergency

Security Planning Workbook

Security Planning Workbook
https://www.cisa.gov/resources-tools/resources/security-planning-workbook

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

CISA Resources

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

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