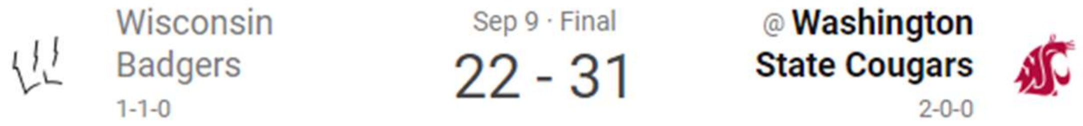
U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

WSU CYSER Fall 2023

Dan Brown, CISSP
Cybersecurity Advisor, Region 10

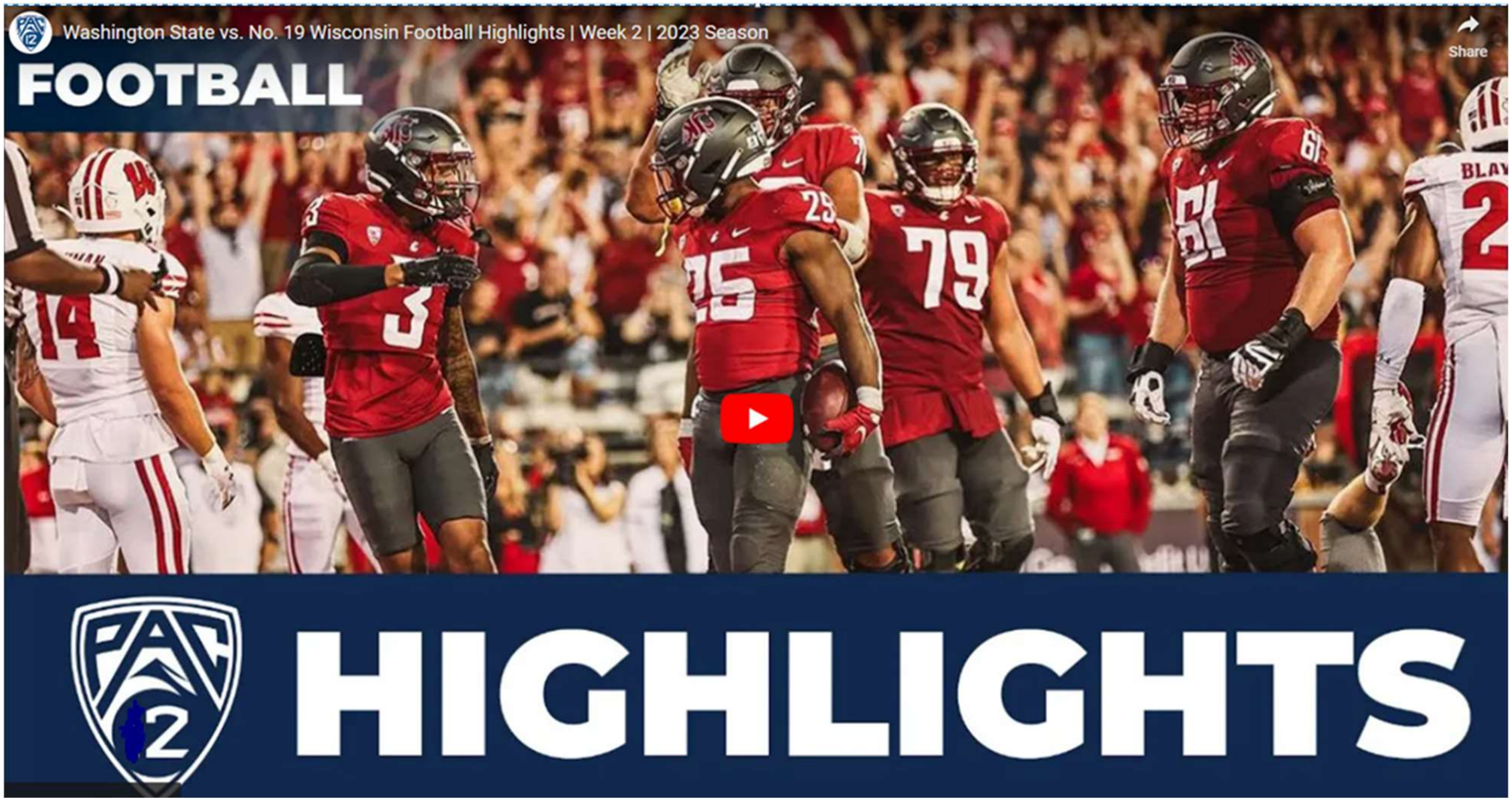


Wisconsin Badgers 1-1-0

Sep 9 · Final

22 - 31

@ **Washington State Cougars** 2-0-0



Washington State vs. No. 19 Wisconsin Football Highlights | Week 2 | 2023 Season

Agenda

- What is CISA?
- Cyber Threat Intelligence (CTI)
- Tools
- Shodan demo
- Partnerships/Initiatives
- CISA Career information

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

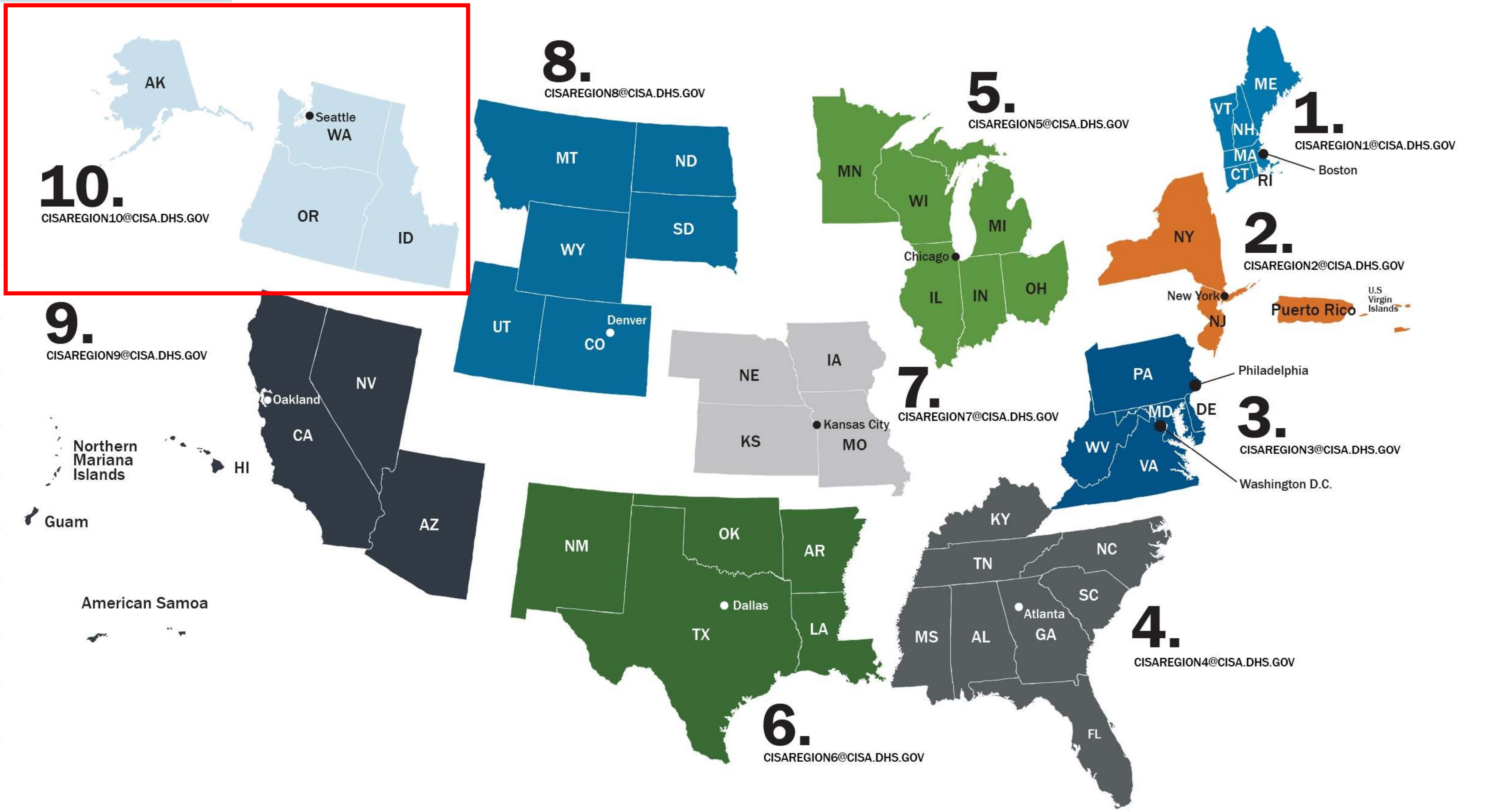
SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CISA Regions

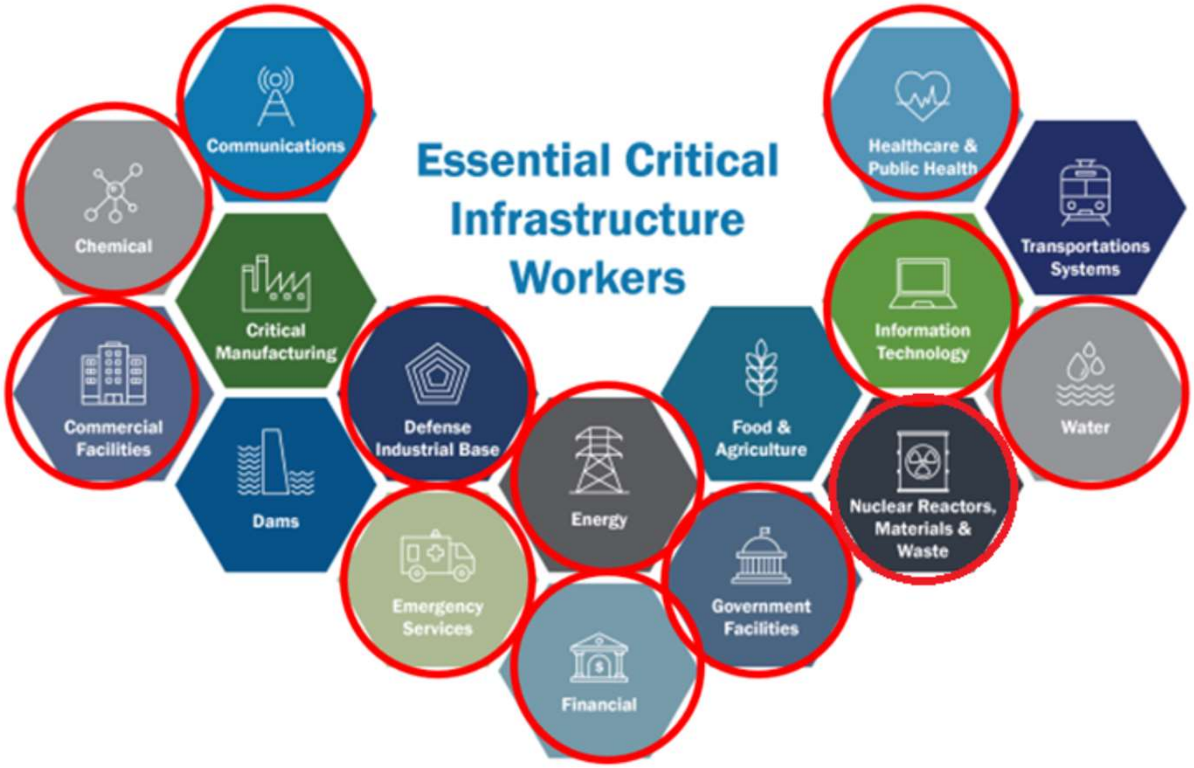
1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

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

Is WSU a Target?



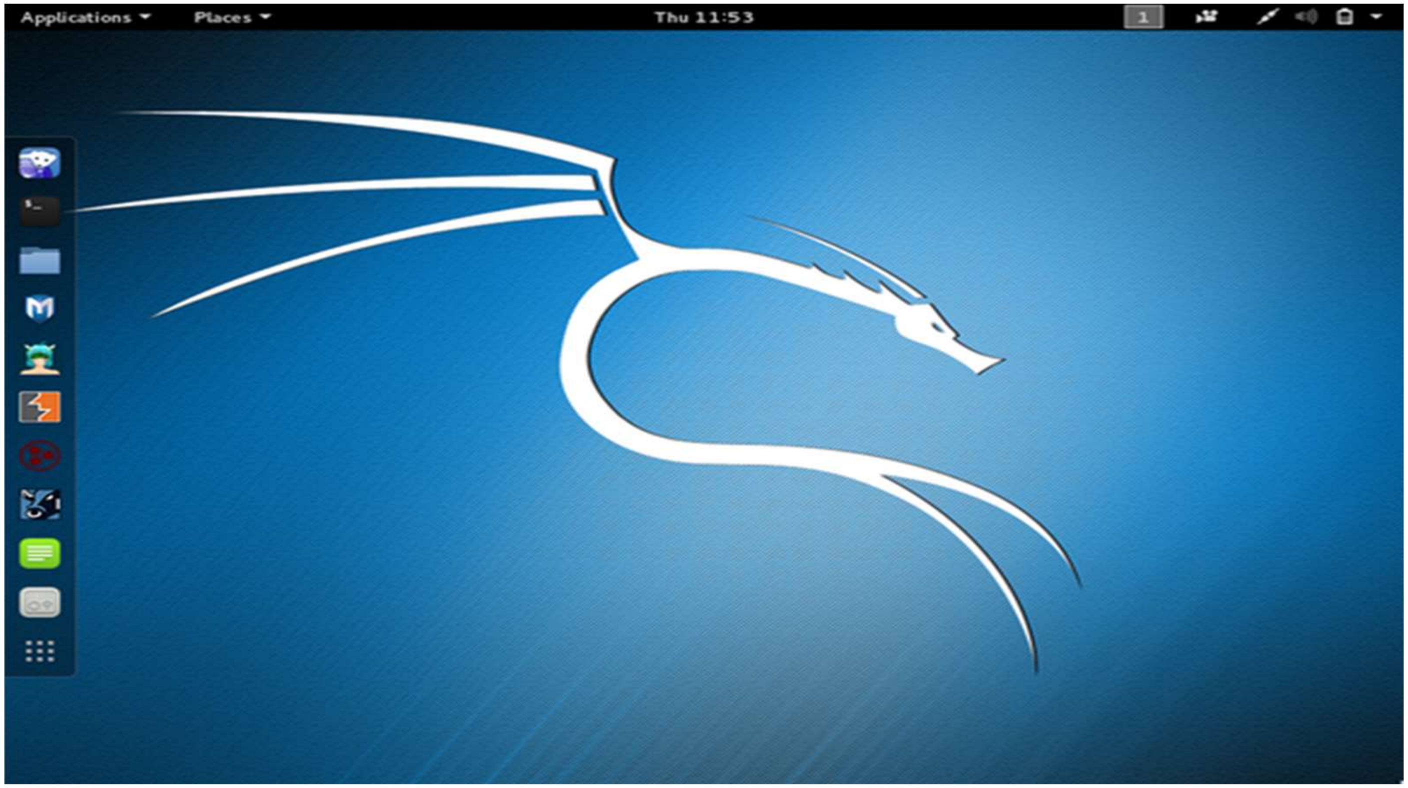
What is Cyber Threat Intelligence?

- Center for Internet (CIS) Security Definition:
  - “Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information. Like all intelligence, cyber threat intelligence provides a value-add to cyber threat information, which reduces uncertainty for the consumer, while aiding the consumer in identifying threats and opportunities. It requires that analysts identify similarities and differences in vast quantities of information and detect deceptions to produce accurate, timely, and relevant intelligence.”

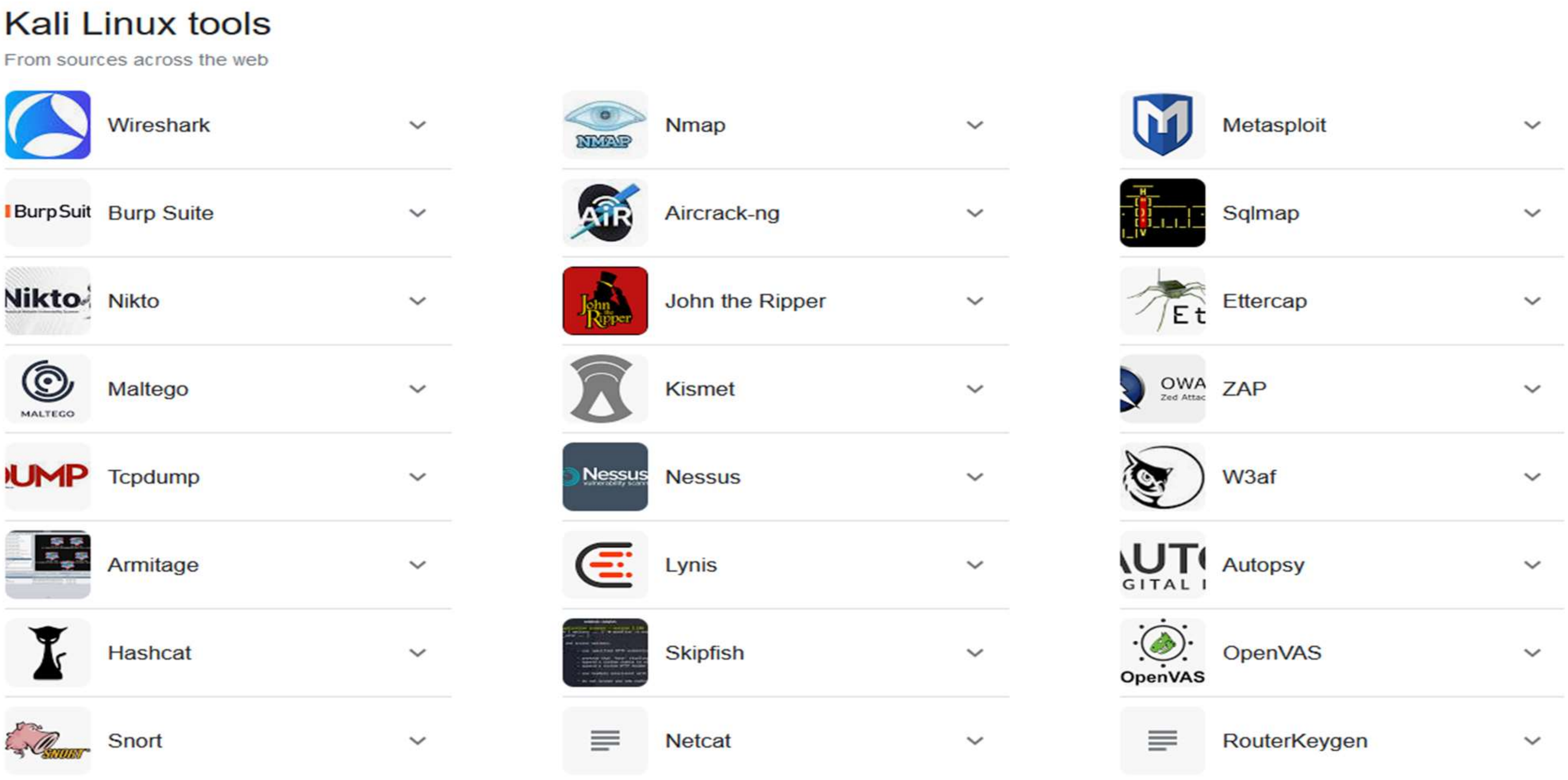
- TL/DR: **Provide analysis on cyber related topics**.

- NIST: Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Kali



Tools used by adversaries, or to protect from them

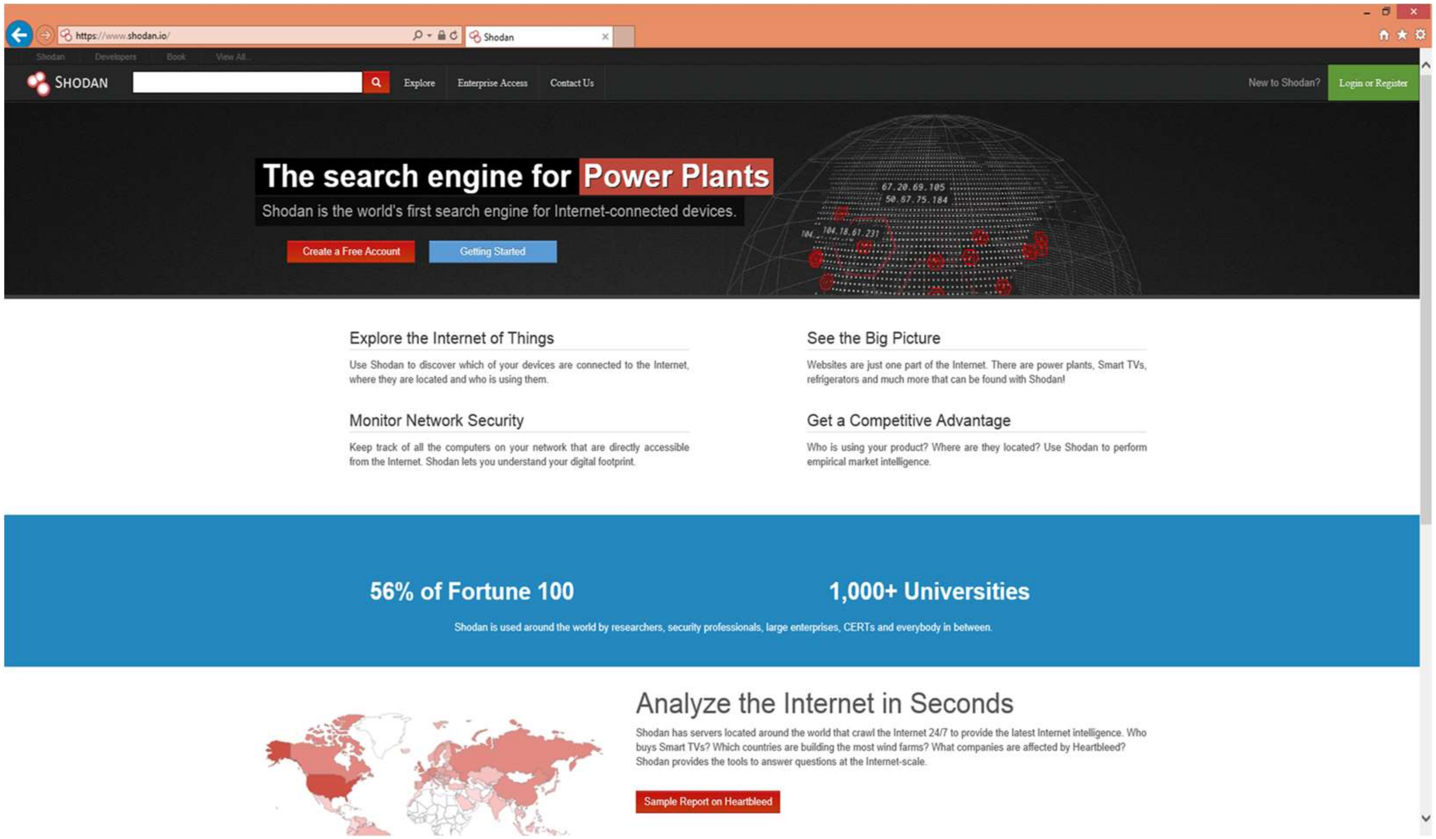


Kali Linux tools

From sources across the web

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

Shodan – search on metadata



The search engine for Power Plants

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

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.

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!

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.

Get a Competitive Advantage

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

56% of Fortune 100

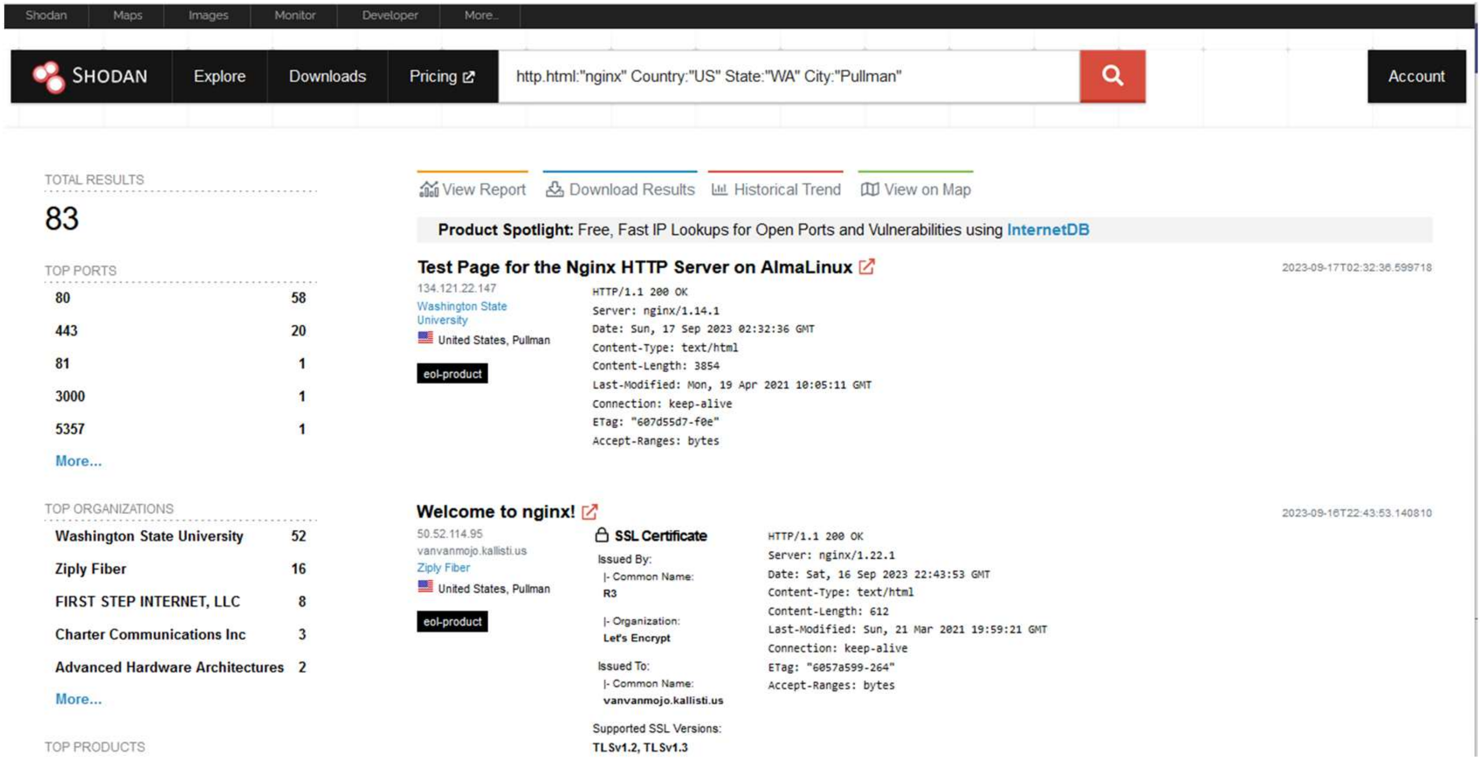
1,000+ Universities

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.

Shodan – search on metadata



http.html:"nginx" Country:"US" State:"WA" City:"Pullman"

TOTAL RESULTS

83

TOP PORTS

80	58
443	20
81	1
3000	1
5357	1

More...

TOP ORGANIZATIONS

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

More...

TOP PRODUCTS

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

eol-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
Ziply Fiber
United States, Pullman

eol-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
```

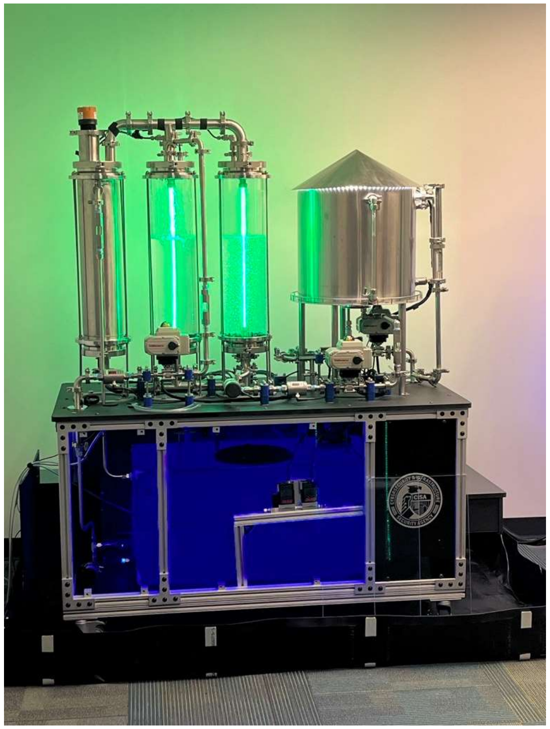
CISA Threat Intel Collaboration

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.

JCDC
CROWDSTRIKE
paloalto NETWORKS
FIREEYE
Microsoft
Google
aws
AT&T
verizon
LUMEN

PNNL Test lab for drinking Water and Wastewater treatment



Operational Technology (OT) networks – convergence with IT networks

CISA Initiative Example

Software Bill of Materials (SBOM)

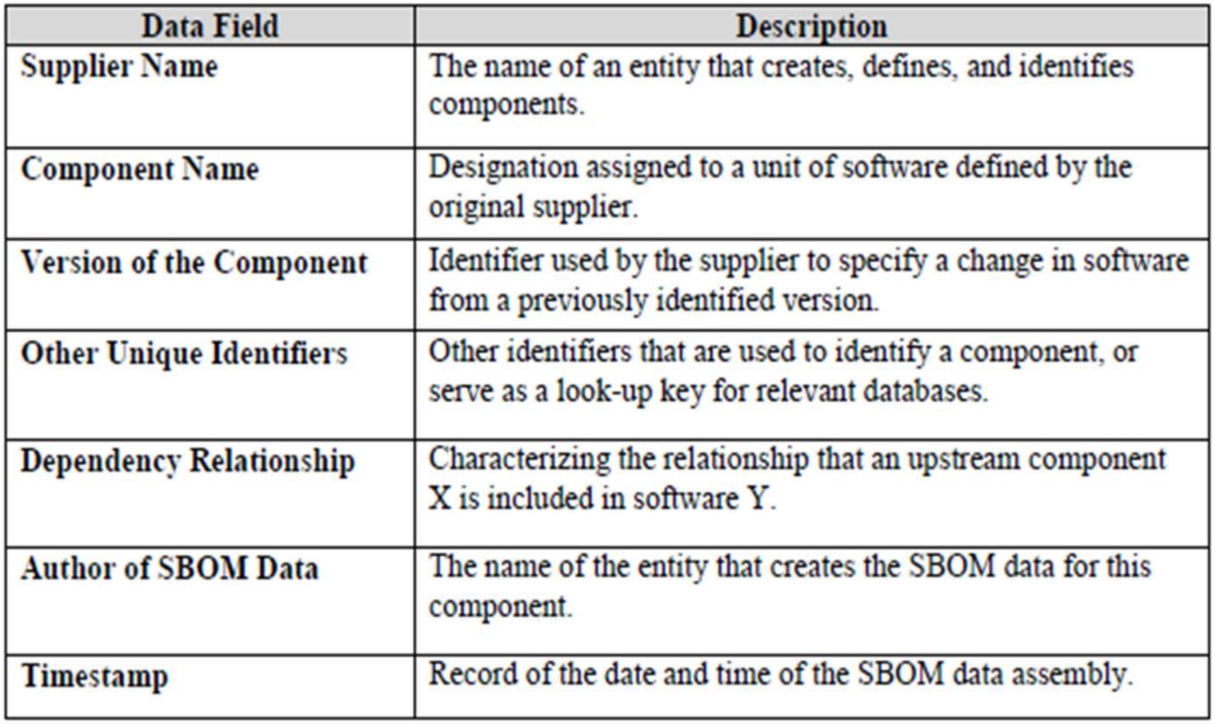
- Key building block in Software Security.
  - A SBOM is a nested inventory, a list of ingredients that make up software components.

SBOM resources

https://www.cisa.gov/sbom

SBOM

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

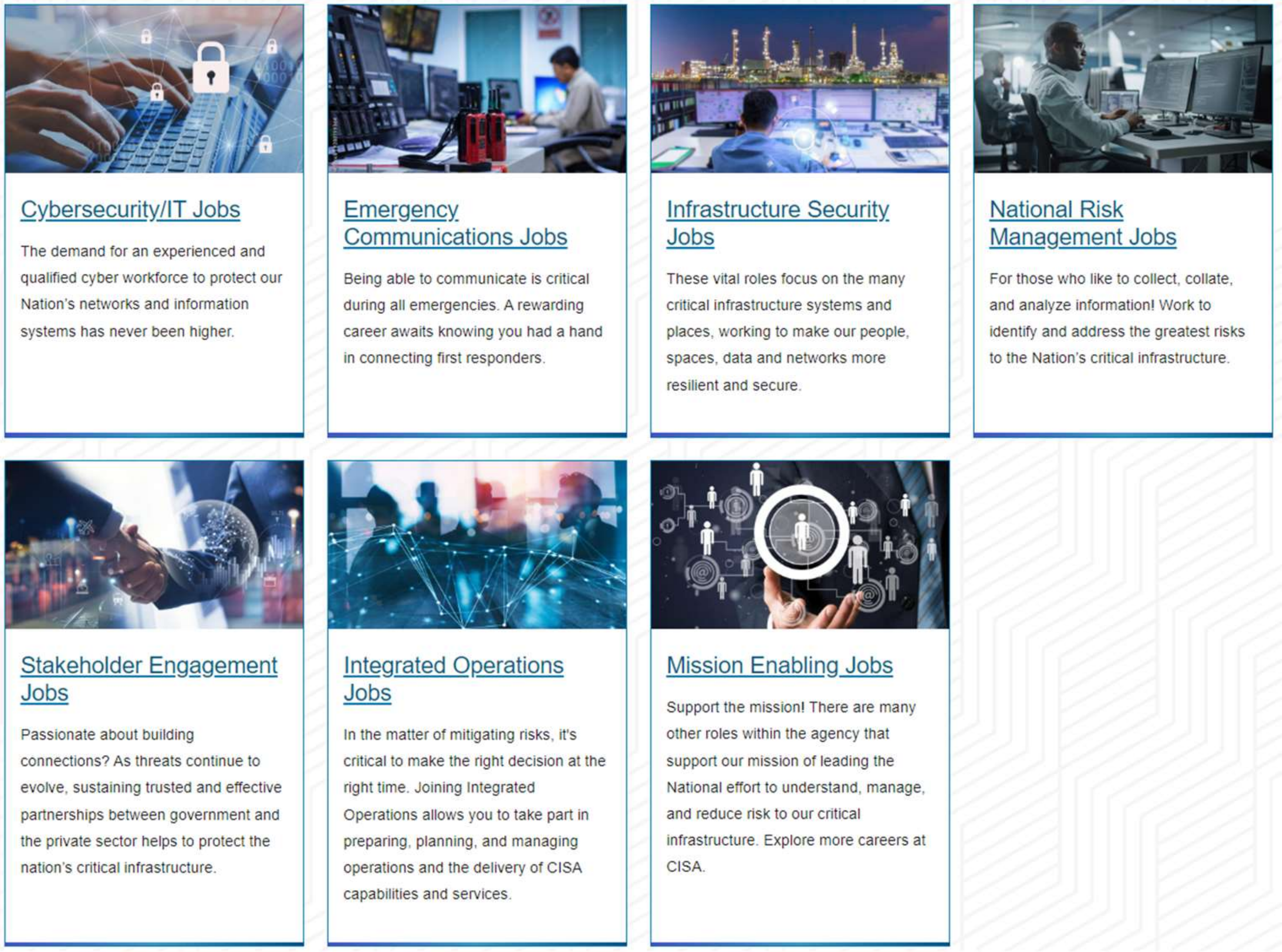
"Consumer safety must be front and center in all phases of the technology product lifecycle—with security designed in from the beginning."

DIRECTOR JEN EASTERLY

https://www.cisa.gov/securebydesign

Joining CISA

- CISA.gov/careers
  - www.usajobs.gov
  - dhscs.usajobs.gov
  - StudentCareers@cisa.dhs.gov
- Resume Help
  - www.cisa.gov/careers/resume-application-tips
- Hiring Timeline
  - Depending on Job, 3-8 Months.



Cybersecurity/IT Jobs

The demand for an experienced and qualified cyber workforce to protect our Nation's networks and information systems has never been higher.

Emergency Communications Jobs

Being able to communicate is critical during all emergencies. A rewarding career awaits knowing you had a hand in connecting first responders.

Infrastructure Security Jobs

These vital roles focus on the many critical infrastructure systems and places, working to make our people, spaces, data and networks more resilient and secure.

National Risk Management Jobs

For those who like to collect, collate, and analyze information! Work to identify and address the greatest risks to the Nation's critical infrastructure.

Stakeholder Engagement Jobs

Passionate about building connections? As threats continue to evolve, sustaining trusted and effective partnerships between government and the private sector helps to protect the nation's critical infrastructure.

Integrated Operations Jobs

In the matter of mitigating risks, it's critical to make the right decision at the right time. Joining Integrated Operations allows you to take part in preparing, planning, and managing operations and the delivery of CISA capabilities and services.

Mission Enabling Jobs

Support the mission! There are many other roles within the agency that support our mission of leading the National effort to understand, manage, and reduce risk to our critical infrastructure. Explore more careers at CISA.

Contacts and Questions?

Daniel Brown
Region 10 (WA, Eastern WA, Northern ID)
Cybersecurity Advisor
(509) 981-9920
Daniel.Brown@cisa.dhs.gov

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