Agenda

- What is CISA?
- Cyber Threat Intelligence (CTI)
- Tools
- Shodan demo
- Partnerships/Initiatives
- CISA Career information
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
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
- TRANSPORTATION 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
- Tcddump
- Armitage
- Hashcat
- Snort
- Nmap
- Aircrack-ng
- John the Ripper
- Kismet
- Nessus
- Lynis
- Skipfish
- Smbcheck
- Metasploit
- Sqimap
- Ettercap
- OWASP ZAP
- W3af
- Autopsy
- OpenVAS
- RouterKeygen
Shodan – search on metadata
# Shodan – search on metadata

**TOTAL RESULTS**

<table>
<thead>
<tr>
<th>PORT</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>58</td>
</tr>
<tr>
<td>443</td>
<td>20</td>
</tr>
<tr>
<td>81</td>
<td>1</td>
</tr>
<tr>
<td>3000</td>
<td>1</td>
</tr>
<tr>
<td>5357</td>
<td>1</td>
</tr>
</tbody>
</table>

**TOP ORGANIZATIONS**

<table>
<thead>
<tr>
<th>Organization</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Washington State Unv</td>
<td>57</td>
</tr>
<tr>
<td>Zippy Fiber</td>
<td>16</td>
</tr>
<tr>
<td>FIRST STEP INTERNET, LLC</td>
<td>8</td>
</tr>
<tr>
<td>Charter Communications Inc</td>
<td>3</td>
</tr>
<tr>
<td>Advanced Hardware Architectures</td>
<td>2</td>
</tr>
</tbody>
</table>

**TOP PRODUCTS**

<table>
<thead>
<tr>
<th>Product</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx</td>
<td>56/52, 114/95</td>
</tr>
<tr>
<td>SSL cipher</td>
<td>43</td>
</tr>
</tbody>
</table>

**Product Spotlight:** Free, Fast IP Lookups for Open Ports and Vulnerabilities using **InternetDB**

### Test Page for the nginx HTTP Server on AlmaLinux

| Server: | nginx/1.22.1 |
| Date:   | Sat, 16 Sep 2023 22:42:53 GMT |
| Content-Type: | text/html |
| Content-Length: | 412 |
| Last-Modified: | Sat, 16 Sep 2023 22:42:53 GMT |
| Connection: | keep-alive |
| ETag:     | "36875657-a9" |
| Accept-Ranges: | bytes |

### Welcome to nginx!

| Version: | 1.23.8 |
| Supported SSL Ciphers: | TLSv1.2, TLSv1.3 |

**SSL Certificate**

- Issuing Authority: 43
- Common Name: varname:kelli
- Issued To: varname:kelli
- Valid From: 16 Sep 2023 22:42:53 GMT
- Valid To: 16 Sep 2023 22:42:53 GMT
- Serial Number: 412
- Certificate Authority: 43
- Issuer: 43
- Subject: varname:kelli

**HTTP/1.1 200 OK**

| Server: | nginx/1.22.1 |
| Date:   | Sat, 16 Sep 2023 22:42:53 GMT |
| Content-Type: | text/html |
| Content-Length: | 412 |
| Last-Modified: | Sat, 16 Sep 2023 22:42:53 GMT |
| Connection: | keep-alive |
| ETag:     | "36875657-a9" |
| Accept-Ranges: | bytes |
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.
PNNL Test lab for drinking Water and Wastewater treatment

Operational Technology (OT) networks – convergence with IT networks
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
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/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.
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