



DIGITAL OBSERVATORY FOR JOINT ASSET ANALYSIS
A unified observatory for an organization's internet-facing systems – one coherent, queryable view.



THE DOJAA TEAM

Dubem Okoye
TEAM MANAGER · FRONTEND

Om Savaliya
PROJECT MANAGER · BACKEND

Akhil Binumon
SECRETARY · BACKEND

Jon Tu
CHIEF TECHNOLOGY OFFICER · FRONTEND

Alex Williams
CHIEF INFORMATION SECURITY OFFICER · BACKEND



WITH GRATITUDE TO
Professor David Comroe

For keeping us on track

FACULTY ADVISOR · COLLEGE OF COMPUTING & INFORMATICS

01 THE PROBLEM

WHY DOJAA EXISTS

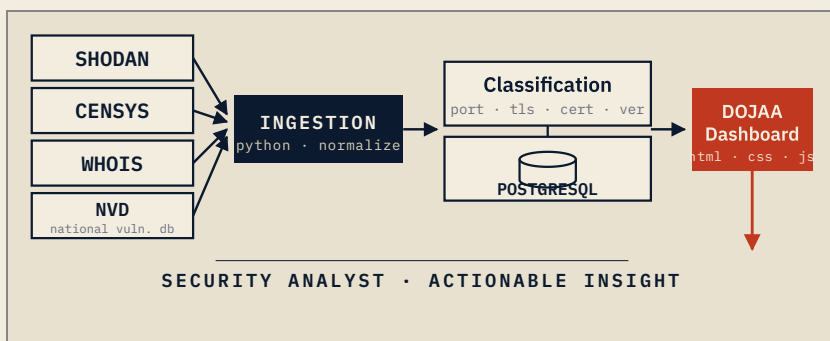
The view of an organization's public footprint is fragmented across *dashboards, raw JSON, and one-off queries* – even though every record is already publicly available.

02 OUR APPROACH PASSIVE · STRUCTURED · CONTEXTUAL

- ◆ **Aggregate, don't pivot.** Four public sources → one normalized inventory.
- ◆ **Passive by design.** Every observation from public datasets – zero packets sent to any target.
- ◆ **Asset classification.** A weighted engine groups hosts using port, TLS, certificate, and version signals.

03 ARCHITECTURE

HOW THE DATA FLOWS



04 IN NUMBERS

REPRESENTATIVE SCAN

HOSTS DISCOVERED 851 Shodan 802 · Censys 49	SERVICE PORTS 5 unique TCP services
CVE FINDINGS 19 reconciled with NVD	CERTIFICATES 50 TLS expiry tracked



05 THE STACK

TOOLS WE BUILT ON

SHODAN ASSET DISCOVERY	censys ASSET DISCOVERY	PostgreSQL RELATIONAL DATABASE
python	postgresql	html · css · javascript
nvd · national vuln. db	whois	

SCREEN 01 · THE DASHBOARD

OVERVIEW · 851 ASSETS · REFRESHED CONTINUOUSLY

Overview

Where to look first. Each tile and widget links to its detail tab.
Data refreshed just now

HOSTS DISCOVERED
424
802 via Shodan · 49 via Censys

HIGH-RISK ASSETS
588
15 medium · 248 low

CVE FINDINGS
19
6 critical / high severity

CERTIFICATES
50
2 expiring within 30 days

Exposure by protocol

Risk distribution

Top risky hosts

IP	SERVICE	RISK
129.25.131.190	HTTP	76.0
129.25.131.190	HTTPS	76.0
35.168.172.251	HTTP	76.0
34.196.243.228	HTTP	76.0
54.84.32.71	HTTP	76.0

Expiring certificates

IP	SUBJECT	DAYS LEFT
129.25.11.79	filemaker.lcc.drexel.edu	Expired
129.25.139.41	print.westphal.drexel.edu	30d

Latest CVEs

CVE	SERVICE	SEVERITY
CVE-2009-0941	HP Printer Embedded Web Server	UNKNOWN
CVE-2024-8901	AWS ELB	HIGH
CVE-1999-0236	Apache httpd	HIGH
CVE-1999-0071	Apache httpd	UNKNOWN
CVE-2002-1850	Apache httpd	HIGH

SCREEN 02 · EXTERNAL ASSET GRAPH

NODE COLOR = CLASSIFICATION TIER

Attack surface graph

The external attack surface fans out through service hubs (SSH / WEB / OTHER) into individual assets. Node colour is the risk score.

Surface 851 rows

● Risk < 30 ● Risk 30-69 ● Risk ≥ 70

Hosts

Combined inventory from Shodan and Censys - CSV unique IP's. Click any row for the full asset detail. Data refreshed just now.

IP	SERVICE	SEVERITY	PORT	STATUS	RISK	WEIGHT
129.25.131.190	SSH	88	22	OPEN	76.0	1000
129.25.131.190	HTTPS	80	443	OPEN	76.0	1000
35.168.172.251	HTTP	80	80	OPEN	76.0	1000
34.196.243.228	HTTP	80	80	OPEN	76.0	1000
54.84.32.71	HTTP	80	80	OPEN	76.0	1000

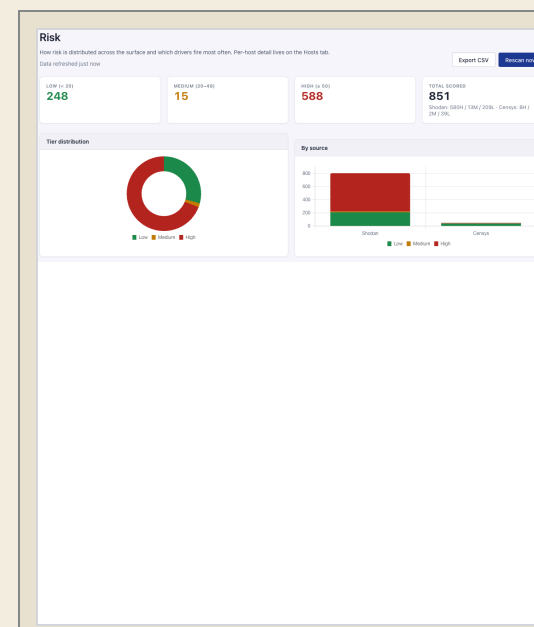
HOSTS 851

Open ports

Port and service discovery across the attack surface. Click a port to see the hosts behind it. Data refreshed just now.

PORT	ADDRESS	HOSTS	WEIGHT
80	HTTP	315	37%
443	HTTPS	347	41%
22	SSH	193	23%
3306	MySQL	10	1%
3307	MySQL	9	1%
3308	MySQL	9	1%

PORTS 5



DISTRIBUTION 851

CVE findings

Unauthorized keyword-matched from the National Vulnerability Database against discovered services. Trust each match as a hypothesis until confirmed on the host.

CVE	SERVICE	SEVERITY	CVSS	PUBLISHED	CWE	REFERENCES	DESCRIPTION
CVE-2009-0941	HP Printer Embedded Web Server	UNKNOWN	14	2009-01-18	CWE-204	https://www.hackerone.com/reports/10144	The HP Embedded Web Server (EWS) on HP printers is vulnerable to a Denial of Service (DoS) attack. An attacker can cause a DoS by sending a specially crafted request to the EWS. The request must contain a specific header value and a specific body value. The request must also be sent to a specific IP address and port.
CVE-2024-8901	AWS ELB	HIGH	9.8	2024-08-22	CWE-280	https://aws.amazon.com/advisories/aws-2024-08-22-aws-elb-cve-2024-8901/	A critical vulnerability in Amazon Elastic Load Balancing (ELB) allows an attacker to cause a Denial of Service (DoS) by sending a specially crafted request to the ELB. The request must contain a specific header value and a specific body value. The request must also be sent to a specific IP address and port.
CVE-1999-0236	Apache httpd	HIGH	10	1999-01-01	N/A	https://nvd.nist.gov/vuln/detail/CVE-1999-0236	A Denial of Service (DoS) vulnerability in the httpd daemon. A specially crafted request can cause the daemon to crash or to consume all available memory.
CVE-1999-0071	Apache httpd	UNKNOWN	10	1999-01-01	N/A	https://nvd.nist.gov/vuln/detail/CVE-1999-0071	A Denial of Service (DoS) vulnerability in the httpd daemon. A specially crafted request can cause the daemon to crash or to consume all available memory.
CVE-2002-1850	Apache httpd	HIGH	10	2002-08-01	N/A	https://nvd.nist.gov/vuln/detail/CVE-2002-1850	A Denial of Service (DoS) vulnerability in the httpd daemon. A specially crafted request can cause the daemon to crash or to consume all available memory.

CVE FINDINGS 19

SSL/TLS certificates

Certificates installed for every HTTP endpoint the pipeline could reach. Click an IP to open the host detail.

IP	RISK	ISSUER	SUBJECT	NAME	EXPIRY	DATE LEFT	TIER
129.25.131.190	76.0	Amazon.com	filemaker.lcc.drexel.edu	filemaker.lcc.drexel.edu	2024-10-29	2024-10-29	High
35.168.172.251	76.0	Amazon.com	print.westphal.drexel.edu	print.westphal.drexel.edu	2024-10-29	2024-10-29	High
34.196.243.228	76.0	Amazon.com	print.westphal.drexel.edu	print.westphal.drexel.edu	2024-10-29	2024-10-29	High
54.84.32.71	76.0	Amazon.com	print.westphal.drexel.edu	print.westphal.drexel.edu	2024-10-29	2024-10-29	High

CERTIFICATES 50