

Final Presentation

Group Two

Kenneth, Hashim, Jeffery, Mohamed, Madison



Intro & Objectives

A full-stack application that provides real-time threat analysis



User Authentication	Secure registration and login using hashed passwords (bcrypt)
Secure Data Storage	PostgreSQL with parameterized queries to prevent SQL injection
Secure Log In	CSRF Protected; session-based authentication with token storage
User Activity	Actively logged within the system via backend logging
Input Validation	All form fields sanitized; inputs checked server-side
Session Management	Secure server-side sessions with logout/timeout enforcement

System Architecture & Tech Used

OSINT Specialist

Shodan (scanning IPs & retrieving data based on parameters), VirusTotal

Risk Analyst

Python, OpenAI GPT-4 API, Node.js, Flask, NIST CSF/RMF frameworks, risk threshold modeling, alerting frameworks, cost-benefit analysis tools, OWASP Risk Assessment Framework

Main Developer

Flask, PostgreSQL, JSX, Node.js, Express.js, psycopg2-binary, Axios, Hugging Face AI, httpx, dotenv, flask-cors, cryptography, and SendGrid, EPSS, OSV APIs

Git Admin

PostgreSQL, Node.js, Flask, yaml, OpenAI GPT-4 API

[illegible]

Shop Smart Solutions

Real Time Threat Intelligence SIEM

Login

Don't have an account? [Register here](#)

The screenshot displays the ShopSmart Solutions SIEM interface. At the top, there's a navigation bar with the company name and a 'Logout' button. The main content area is divided into several sections:

- API Scans:** A section showing a 'VirusTotal IP' scan for '192.168.1.1'. It includes a 'Scan' button and a 'Details' button. Below this, there's a 'Shodan IP' section with a 'Scan' button and a 'Details' button. A 'Shodan Search Query' section is also present with a 'Scan' button and a 'Details' button. A 'Hostname to Resolve' section is visible with a 'Scan' button and a 'Details' button.
- Recent Alerts:** A section showing a list of alerts with columns for Severity, Source, and Threat Type. The alerts are categorized by severity: Critical (Red), High (Orange), Medium (Yellow), and Low (Green).
- Alert Details:** A detailed view of a 'VirusTotal IP' scan for '192.168.1.1'. It shows the scan results, including the IP address, the scan date, and the scan status. The results are categorized by severity: Critical (Red), High (Orange), Medium (Yellow), and Low (Green).

Dependency Risk Intelligence									
Proj.	Ver.	OS	Product Risk Score	OS Support EOL	Date	Summary	Risk	Severity	
proj-1	1.0.0.0.0.0.0	100	0.0%	2024-06-30	2024-06-30	Server software is secure	Low	Low	
proj-1	1.0.1.0.0.0.0	175	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.2.0.0.0.0	220	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.3.0.0.0.0	300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.4.0.0.0.0	350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.5.0.0.0.0	400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.6.0.0.0.0	450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.7.0.0.0.0	500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.8.0.0.0.0	550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.9.0.0.0.0	600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.10.0.0.0	650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.11.0.0.0	700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.12.0.0.0	750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.13.0.0.0	800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.14.0.0.0	850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.15.0.0.0	900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.16.0.0.0	950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.17.0.0.0	1000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.18.0.0.0	1050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.19.0.0.0	1100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.20.0.0.0	1150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.21.0.0.0	1200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.22.0.0.0	1250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.23.0.0.0	1300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.24.0.0.0	1350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.25.0.0.0	1400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.26.0.0.0	1450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.27.0.0.0	1500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.28.0.0.0	1550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.29.0.0.0	1600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.30.0.0.0	1650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.31.0.0.0	1700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.32.0.0.0	1750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.33.0.0.0	1800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.34.0.0.0	1850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.35.0.0.0	1900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.36.0.0.0	1950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.37.0.0.0	2000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.38.0.0.0	2050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.39.0.0.0	2100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.40.0.0.0	2150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.41.0.0.0	2200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.42.0.0.0	2250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.43.0.0.0	2300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.44.0.0.0	2350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.45.0.0.0	2400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.46.0.0.0	2450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.47.0.0.0	2500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.48.0.0.0	2550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.49.0.0.0	2600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.50.0.0.0	2650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.51.0.0.0	2700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.52.0.0.0	2750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.53.0.0.0	2800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.54.0.0.0	2850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.55.0.0.0	2900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.56.0.0.0	2950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.57.0.0.0	3000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.58.0.0.0	3050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.59.0.0.0	3100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.60.0.0.0	3150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.61.0.0.0	3200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.62.0.0.0	3250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.63.0.0.0	3300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.64.0.0.0	3350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.65.0.0.0	3400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.66.0.0.0	3450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.67.0.0.0	3500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.68.0.0.0	3550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.69.0.0.0	3600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.70.0.0.0	3650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.71.0.0.0	3700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.72.0.0.0	3750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.73.0.0.0	3800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.74.0.0.0	3850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.75.0.0.0	3900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.76.0.0.0	3950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.77.0.0.0	4000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.78.0.0.0	4050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.79.0.0.0	4100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.80.0.0.0	4150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.81.0.0.0	4200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.82.0.0.0	4250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.83.0.0.0	4300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.84.0.0.0	4350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.85.0.0.0	4400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.86.0.0.0	4450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.87.0.0.0	4500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.88.0.0.0	4550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.89.0.0.0	4600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.90.0.0.0	4650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.91.0.0.0	4700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.92.0.0.0	4750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.93.0.0.0	4800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.94.0.0.0	4850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.95.0.0.0	4900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.96.0.0.0	4950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.97.0.0.0	5000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.98.0.0.0	5050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.99.0.0.0	5100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.100.0.0.0	5150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.101.0.0.0	5200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.102.0.0.0	5250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.103.0.0.0	5300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.104.0.0.0	5350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.105.0.0.0	5400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.106.0.0.0	5450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.107.0.0.0	5500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.108.0.0.0	5550	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.109.0.0.0	5600	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.110.0.0.0	5650	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.111.0.0.0	5700	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.112.0.0.0	5750	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.113.0.0.0	5800	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.114.0.0.0	5850	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.115.0.0.0	5900	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.116.0.0.0	5950	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.117.0.0.0	6000	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.118.0.0.0	6050	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.119.0.0.0	6100	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.120.0.0.0	6150	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.121.0.0.0	6200	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.122.0.0.0	6250	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.123.0.0.0	6300	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.124.0.0.0	6350	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.125.0.0.0	6400	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.126.0.0.0	6450	0.0%	2024-06-30	2024-06-30	Minor security updates	Low	Low	
proj-1	1.0.127.0.0.0	6500	0.0%	2024-06-30	2024-06-30	Minor security updates	Low		

VirusTotal IP:

Scan

Example: 8.8.8.8

Shodan IP:

Scan

Example: 8.8.8.8

Shodan Search Query:

Search

Example: ip:8.8.8.8 country:us

Hostname to Resolve:

Resolve DNS

Example: google.com or
site1.com,site2.net

Enter IP:

Example: 8.8.8.8

Enter a search query

Example: ip:8.8.8.8 country:us

google.com

Example: google.com or
site1.com,site2.net

▲ VirusTotal Results

Owner: GOOGLE (AS15169)

Location: US (NA)

Network: 8.8.8.0/24

Reputation: 549

Malicious: 0

Suspicious: 0

[View Full Report](#)

▲ Shodan DNS Resolve Results

{ "google.com": "72.17.147.8" }

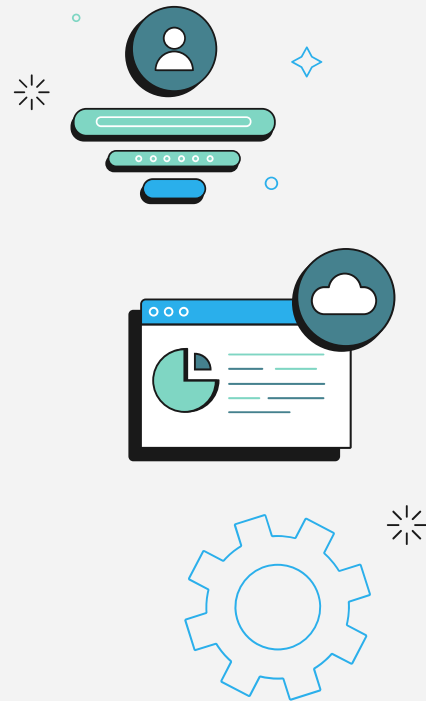
Security Features & Risk Management

Measures

- CSRF Tokens
- Input Validation
- API Key Protection
- Rate Limiting
- Session Management
- Environment Variables
- Access Control
- Secure Headers
- Output Encoding
- CORS Handling
- Secure Cookies

Risk Management

- Dependency Audits
- Active CVE Scanning



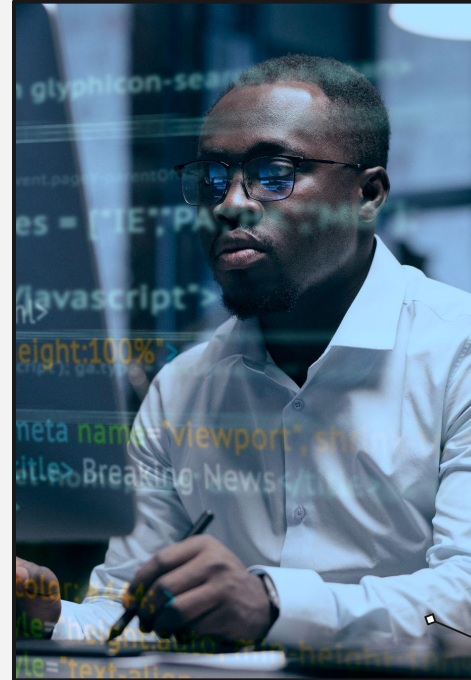
Testing & Evaluation

Key Tests Conducted

- Shodan API Integration:
 - Validates the structure of the data returned for an IP (checks for dictionary format, ports key, and list type for ports).
- VirusTotal API Integration:
 - Verifies that the data returned for a domain includes the malicious key and ensures it is an integer.

Evaluation Metrics

- Test Coverage: Ensures the APIs return correctly structured and essential data.
- Data Integrity: Confirms the response matches expected formats and values



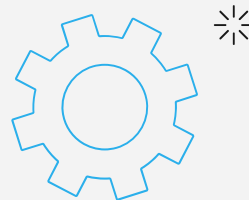
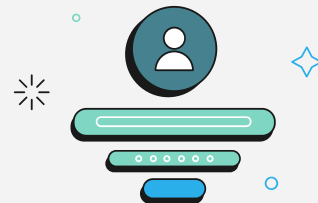
Challenges → Solutions

Challenges

1. Maintaining secure communication between frontend and backend.
2. Combining scan data with live CVE and EPSS feeds in real time.

Solutions

1. Implemented **CSRF protection**, session-based authentication, and used **parameterized queries** to defend against SQL injection.
2. Created an **asynchronous enrichment pipeline** using OSV + EPSS APIs, integrated with **Hugging Face** to score risks and display them in the dashboard.



Future Improvements

**Enhancements
in RBACs**

**Broader API
Integrations for richer
and more diverse
data sources**



**User
Customization**

**Contextual Help
("What's this?")**