Final Presentation

Group Two

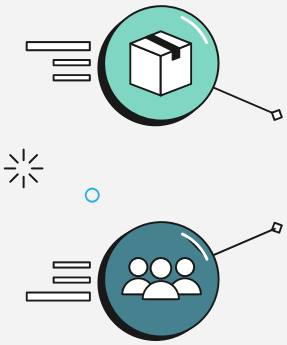
Kenneth, Hashim, Jeffery, Mohamed, Madison

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

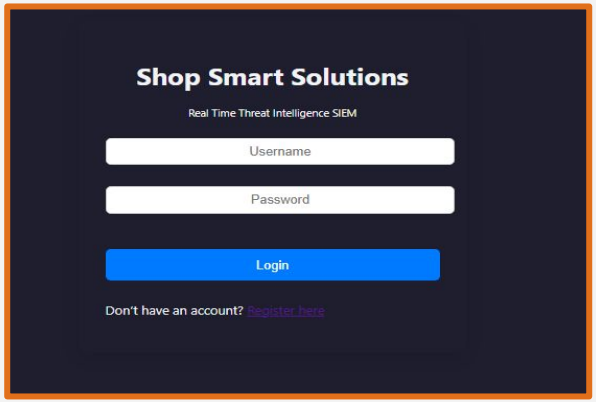
Main Developer

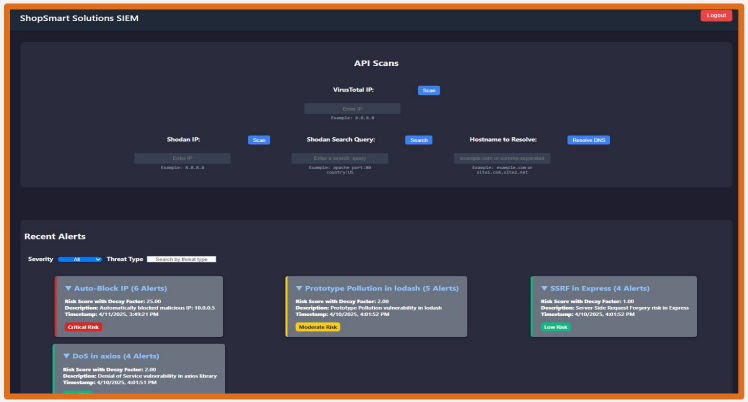
Flask, PostgreSQL, JSX, Node.js, Express.js, psycopg2-binary, Axios, Hugging Face AI, httpx, dotenv, flask-cors, cryptography, and SendGrid, EPSS, OSV APIs

Git Admin

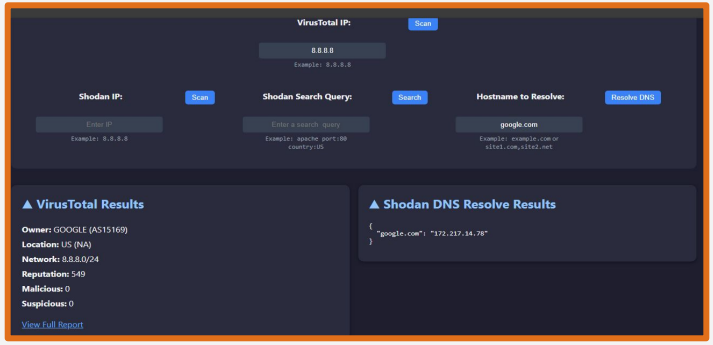
PostgreSQL, Node.js, Flask, yaml, OpenAI GPT-4 API

System Demo


Shop Smart Solutions
Real Time Threat Intelligence SIEM
Username
Password
Login
Don't have an account? Register here


ShopSmart Solutions SIEM
Logout
API Scans
VirusTotal IP:
Scan
Shodan IP:
Shodan Search Query:
Search
Hostname to Resolve:
Resolve DNS
Recent Alerts
Severity
Threat Type
Auto-Block IP (6 Alerts)
Prototype Pollution in lodash (5 Alerts)
SSRF in Express (4 Alerts)
DoS in axios (4 Alerts)


Dependency Risk Intelligence


VirusTotal IP:
Scan
8.8.8.8
Example: 8.8.8.8
Shodan IP:
Scan
Shodan Search Query:
Search
Hostname to Resolve:
Resolve DNS
google.com
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": "172.217.14.78"

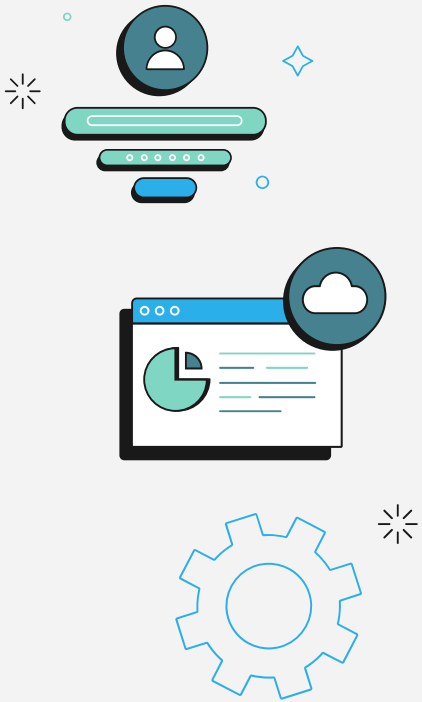
Security Features & Risk Management

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



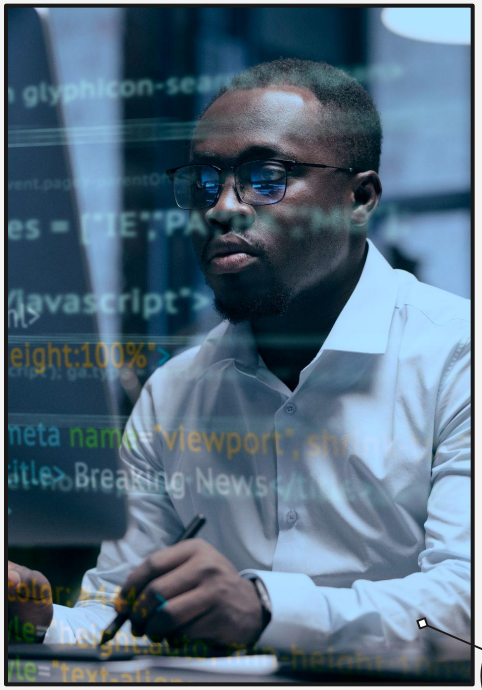
Testing & Evaluation

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



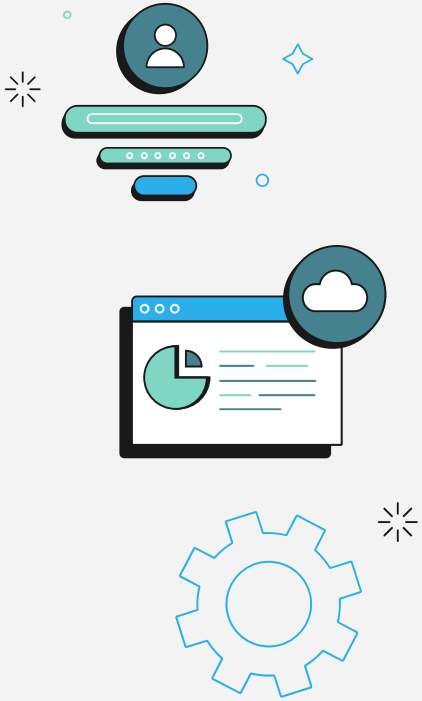
Challenges → Solutions

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 Customerization

Contectional Help (“What’s this?”)