Lokeshwar V

Tamil Nadu, India
+91 8098239802 — lokeshwar.v06@gmail.com
LinkedIn: https://www.linkedin.com/in/lokeshwar-v-011b20289
GitHub: https://github.com/Loke31033

Professional Summary

Cybersecurity student with hands-on experience in SOC monitoring, incident response, vulnerability assessment, and web application security testing. Skilled in Splunk SIEM, Windows and Sysmon log analysis, IOC identification, forensic timelines, and OWASP Top 10 vulnerabilities including SQL injection and XSS. Strong ability in alert triage, threat detection, and security reporting. Seeking SOC Analyst, Security Analyst, or VAPT roles.

Education

B.Tech – Computer Science Engineering (Cybersecurity)
SRM Institute of Science and Technology, Trichy
Expected Graduation: 2027

Internship Experience

Cyber Security Intern (Virtual SOC) Sep 2024 – Nov 2024
Elevate Labs (Skill India / MSME)

- Monitored alerts involving authentication anomalies and suspicious processes
- Investigated Windows Security and Sysmon logs
- Performed alert triage, IOC extraction, and incident escalation
- Documented investigations following SOC workflows

Ethical Hacking Intern (Virtual) Sep 2024 – Dec 2024
InLighnX Global Pvt. Ltd.

- Conducted vulnerability assessments on web applications
- Tested OWASP Top 10 including SQL Injection and Cross-Site Scripting
- Validated exploits in controlled labs
- Assisted in writing remediation guidance

Projects

CYBER-SOC v2.0 – Incident Response and Forensic Dashboard
GitHub: https://github.com/Loke31033/CyberSOC-Intrusion-Sim-v2

- Built a SOC platform for real-time threat monitoring and case management
- Implemented severity classification and SLA-based auto escalation
- Created automated forensic timeline logging of analyst and system activity
- Enabled attachment of investigation notes and digital evidence
- Generated management-ready incident reports
- Performed log correlation and IP tracking using Python and SQLite

SOC Threat Detection using Splunk
GitHub: https://github.com/Loke31033/SOC-Threat-Detection-Project-Splunk

- Developed SPL searches for brute-force and suspicious executions
- Analyzed Event IDs such as 4624, 4625 and Sysmon process creation
- Detected lateral movement patterns
- Extracted indicators of compromise and built timelines

Web Application Security and Ethical Hacking Projects

- Bruteforce Attack Simulation – https://github.com/Loke31033/Bruteforce-Attack-Project
- Broken Authentication Testing – https://github.com/Loke31033/Broken-Authentication
- Command Injection Exploitation – https://github.com/Loke31033/Command-Injection-Project
- Information Gathering and Reconnaissance – https://github.com/Loke31033/Information-Gathering-report
- Phishing Simulation and Email Analysis – https://github.com/Loke31033/Phishing-Simulation-Project

Technical Skills

SIEM: Splunk, alert investigation

Operating Systems: Windows, Linux

Logs: Windows Event Logs, Sysmon

Security Concepts: Incident response, MITRE ATT&CK, IOC analysis

VAPT: OWASP Top 10, SQL Injection, XSS, command injection, brute force

Tools: Nmap, Wireshark, Zeek, Burp Suite, VirusTotal

Programming: Python, Bash

Networking: TCP/IP, DNS, HTTP/HTTPS

Certifications

ISC2 Certified in Cybersecurity (CC)
Google Cybersecurity Professional Certificate

Languages

English, Tamil, Telugu