

Lokeshwar V

Tamil Nadu, India

lokeshwar.v06@gmail.com — +91 80982 39802 — LinkedIn — GitHub

Professional Summary

Entry-level SOC Analyst (L1) with strong hands-on experience in Splunk SIEM, SPL query development, Windows Security and Sysmon log analysis, and SOC incident response workflows. Skilled in alert triage, IOC extraction, timeline reconstruction, and evidence-based incident escalation through multiple real-world SOC simulation projects. ISC2 Certified in Cybersecurity (CC) and actively seeking full-time SOC Analyst opportunities.

Education

B.Tech – Computer Science Engineering (Cybersecurity)

SRM Institute of Science and Technology, Trichy

Expected Graduation: 2027

Available for Full-Time SOC Roles

Internship Experience

Cyber Security Intern (Virtual / Simulated SOC)

Sep 2024 – Nov 2024

Elevate Labs (Skill India / MSME)

- Monitored and investigated simulated SOC alerts related to authentication failures and suspicious process activity.
- Analyzed Windows Security and Sysmon logs using structured SOC investigation workflows.
- Performed alert triage, IOC extraction, timeline creation, and incident documentation.
- Escalated validated security incidents with supporting log evidence and IOC context following SOC escalation procedures.
- Worked within simulated 24/7 SOC workflows handling concurrent alerts and prioritizing incidents based on severity.
- Awarded **Best Performer** for investigation accuracy and reporting quality.

Ethical Hacking Intern (Virtual)

Sep 2024 – Dec 2024

InLighnX Global Pvt. Ltd.

- Conducted vulnerability assessments and basic web application testing (SQL Injection, XSS).
- Validated vulnerabilities in controlled lab environments and documented findings.
- Prepared remediation recommendations aligned with security best practices.

Projects

SOC Threat Detection Project — Splunk SIEM

GitHub Repository

- Built an end-to-end SOC L1 detection workflow using Splunk with Windows Security and Sysmon logs.
- Developed 15+ SPL queries to detect brute-force attacks (4625/4624), suspicious process creation (Sysmon Event ID 1), persistence mechanisms (4698, 4657), lateral movement (PsExec, WMIC), and network connections (Sysmon Event ID 3).

- Created forensic timelines (CSV), extracted IOCs, and produced SOC investigation reports suitable for escalation.

CyberSOC Intrusion Detection Simulator — Full Stack SOC Project

GitHub Repository

- Developed a full-stack SOC simulation platform for detecting SSH brute-force attacks.
- Implemented a Python-based log correlation engine with Flask REST APIs and a React dashboard.
- Performed IP-based session tracking, IOC generation, and automated SOC reporting (CSV/JSON).

PhishGuard — Email Phishing Detection Tool

GitHub Repository

- Built an automated SOC email triage tool to analyze phishing indicators from .eml files.
- Performed header analysis, URL inspection, attachment checks, and threat validation.
- Implemented SPF, DKIM, and DMARC validation with VirusTotal integration.

Technical Skills

SIEM & Detection: Splunk (SPL), Windows Event Logs (4624, 4625, 4688, 4698, 4657), Sysmon, MITRE ATT&CK

Threat Investigation: Alert triage, IOC extraction, incident escalation, brute-force analysis, persistence and lateral movement detection

Tools: Wireshark, Zeek, Nmap, VirusTotal, ServiceNow

Scripting: Python, Bash

Networking & OS: TCP/IP, DNS, HTTP/HTTPS, Linux CLI

Certifications

- ISC2 Certified in Cybersecurity (CC) — Passed
- Google Cybersecurity Professional Certificate

Languages

English — Tamil — Telugu