

Muthu Kumar S

Security Operations Analyst | SOC | Cybersecurity Operations

Bengaluru, Karnataka / Chennai (Open to Relocation) | +91 7548822001 | muthukumars1720@gmail.com

LinkedIn: <https://l1nk.dev/5e727> | GitHub: <https://muthu1720.github.io/>

Executive Summary

Security operations-focused cybersecurity professional with hands-on experience in SIEM monitoring, alert triage, log analysis, and incident investigation gained through internships and practical security environments. Experienced in analyzing authentication anomalies, suspicious endpoint activity, phishing threats, and abnormal network behavior using tools such as Splunk and IBM QRadar. Practical exposure to incident response workflows including alert validation, investigation, and documentation. Strong foundation in networking, Windows and Linux systems, and basic scripting, with a focus on proactive threat detection and continuous security monitoring within SOC environments.

Core Skills

- Security Operations & Incident Response** - SIEM Monitoring, Alert Analysis, Incident Triage, Log Analysis, Event Correlation, IOC Identification, Threat Investigation, Incident Documentation, Security Monitoring, Threat Detection.
- Security Tools & Technologies** - Splunk, IBM QRadar, Snort IDS, Wireshark, Nmap, Burp Suite, Vulnerability Scanning Tools, ZAP.
- Endpoint & Threat Analysis** - Process Analysis, Suspicious Activity Investigation, Phishing Analysis, Malware Indicator Identification, Basic Threat Hunting, False Positive Analysis.
- Networking & Systems** - TCP/IP, DNS, HTTP/HTTPS, VPN, Packet Analysis, Windows Security Logs, Linux Administration (Ubuntu/Kali), Active Directory.
- Scripting & Technical Skills** - Python, Bash, PowerShell.

Experience

Cybersecurity Analyst Intern — The Coding Cult Mar 2025 – Jun 2025

- Supported SOC monitoring operations through SIEM dashboards and security alert analysis using Splunk.
- Performed log analysis to investigate authentication anomalies and suspicious system behavior.
- Assisted in incident investigation by correlating endpoint, authentication, and network activity.
- Conducted alert triage and supported incident documentation aligned with SOC procedures.
- Participated in threat analysis discussions and security monitoring activities.

Cybersecurity Professional Intern — Cartel Software Pvt Ltd Feb 2024 – Sep 2024

- Conducted vulnerability assessments and participated in simulated security monitoring exercises.
- Reviewed IDS alerts and investigated suspicious binaries, phishing artifacts, and abnormal network traffic.
- Supported firewall rule review and assisted with detection tuning exercises.
- Automated repetitive analysis tasks using Python and Bash scripts.
- Participated in security incident simulations to understand threat detection workflows.

Technical Support Engineer Trainee — Accura FMS Nov 2025

- Performed application troubleshooting and operational testing activities.
- Supported onboarding workflows and maintained structured technical documentation.
- Followed SOP-driven operational procedures and strengthened incident communication practices.

Projects

ReconnaissPro — Network Vulnerability Scanner

- Developed a Python-based automated scanner for service discovery and vulnerability identification.
- Performed CVE mapping and generated structured reports with remediation guidance.

Security Labs & Threat Simulation Practice

- Investigated simulated brute-force login attempts, phishing scenarios, and suspicious DNS activity.
- Conducted endpoint process analysis and observed malware behavior in controlled lab environments.
- Practiced incident analysis workflows aligned with SOC monitoring activities.

Education

B.Tech — Computer Science and Business Systems

Dhanalakshmi Srinivasan College of Engineering (2020 - 2024)

Certifications

Certified Ethical Hacker (CEH) — EC-Council

HSCCSP — Hacker School Certified Cyber Security Professional

Advanced Diploma in Cyber Security

Practical Security Experience

| - TryHackMe | VulnHub CTF Machines

| - PortSwigger Labs | OWASP Juice Shop