

Muthu Kumar S

SOC Analyst | Certified Ethical Hacker | SIEM | Threat Detection

Executive Summary

Cybersecurity graduate with hands-on experience in security monitoring, vulnerability management, and incident analysis within structured SOC environments. Skilled in log analysis, threat detection, and risk identification using SIEM platforms such as Splunk and IBM QRadar. Familiar with security frameworks including MITRE ATT&CK and OWASP Top 10, with strong technical foundations in networking, Linux, and scripting. Demonstrates strong documentation, reporting, and analytical skills suitable for enterprise security operations and risk-focused environments.

Professional Experience

Cybersecurity Analyst Intern – The Coding Cult

Mar 2025 – Jun 2025

- Monitored security events and performed continuous log analysis using Splunk in a SOC environment
- Triaged alerts and identified anomalies including suspicious logins and phishing attempts
- Assisted in incident investigations, evidence collection, and remediation tracking
- Documented incidents and created security reports for senior analysts

Cybersecurity Professional Intern – Cartel Software

Feb 2024 – Sep 2024

- Conducted network and web application vulnerability assessments aligned with OWASP Top 10
- Investigated phishing indicators, malware activity, and suspicious traffic patterns
- Automated routine SOC and enumeration tasks using Python and Bash
- Reviewed firewall rules, analyzed IDS alerts, and supported threat mitigation planning

Technical Support Engineer – Training – Accura FMS

Nov 2025

- Supported platform troubleshooting and performed application sanity testing
- Assisted onboarding processes and operational support tasks

Education

Bachelor of Technology in Computer Science and Business Systems

Dhanalakshmi Srinivasan College of Engineering, 2024 | CGPA: 8.1

Certifications

- Hacker School Certified Cyber Security Professional (Hacker School)
- Certified Ethical Hacker (EC- Council)
- Advance Dip. in Cyber Security (Win in Life Academy)
- Python (Udemy)

Contact

Phone: +91 7548822001

Email: muthukumars1720@gmail.com

LinkedIn: Muthu Kumar S

GitHub: Muthu1720

Portfolio: <https://muthu1720.github.io>

Core Skills

Security Operations

Splunk, IBM QRadar, Log Analysis, Alert Triage, Incident Response, EDR/XDR Threat Detection, Phishing Analysis, Wireshark, Nmap, IDS/IPS Concepts

Vulnerability & Offensive Security

OWASP Top 10, Web Application Testing, Nessus, Metasploit, Msfvenom, Hydra Network VAPT, CVSS, Burp Suite, ZAP

Systems & Scripting

Linux, Windows, AWS, Azure, Java Script, Bash, Python, HTML, CSS, Git/GitHub TCP/IP, DNS, HTTP/HTTPS, Firewall

Projects

ReconnaissPro – Automated Network Vulnerability Scanner

- Developed Python-based scanner for port scanning and service enumeration
- Integrated CVE mapping with CVSS scoring
- Generated well-structured vulnerability reports with remediation guidance

Network & Service Penetration Testing

- Performed reconnaissance, exploitation, and privilege escalation testing
- Identified service misconfigurations and insecure permissions
- Documented the core risks and mitigation strategies

Web Application Security Testing

- Conducted testing for directory traversal and file inclusion vulnerabilities
- Simulated controlled remote access scenarios
- Provided secure coding and patch remediation recommendations

Practical Security Training

TryHackMe | VulnHub | PortSwigger Labs | OWASP Juice Shop

Languages

- English (Fluent)
- Tamil (Native)
- Kannada (Conversational)