VIGNESHWARAN MURUGESAN

Bengaluru, India | Mail | LinkedIn | GitHub | Portfolio | Medium

SUMMARY

Entry-level Cybersecurity Engineer / SOC Analyst with hands-on experience in SIEM operations, log analysis, incident response, threat detection, and vulnerability assessment. Skilled in Splunk, QRadar, Wireshark, Nmap, Burp Suite, Linux, Windows, and basic scripting. Completed SOC & Incident Response training at Hackerschool Bengaluru. Passionate about threat hunting, MITRE ATT&CK mapping, and adversary detection.

PROFESSIONAL EXPERIENCE

L1 Security Admin Associate Intern | Infotact Solutions, Bengaluru | Sep 2025 – December 2025

- Conducted vulnerability assessments, secure code reviews, and assisted in security hardening.
- Monitored logs, system alerts, and user activity to identify suspicious behavior & policy violations.
- Prepared IR documentation, security policies, system hardening guides, and compliance reports.
- Supported patch management workflows and coordinated remediation with IT teams.
- Assisted during security incidents by collecting evidence, triaging events, and escalating high-severity alerts to senior analysts.

Junior SOC Analyst Trainee | HackerSchool, Bengaluru | Jul–Aug 2025

- Performed log analysis, correlation, and triage using Splunk and QRadar for real-time monitoring.
- Investigated phishing attacks, brute-force attempts, port scans, malicious IP connections, and suspicious user behavior.
- Assisted in SIEM rule creation & tuning, reducing false positives in daily alert queues.
- Contributed to incident response playbooks and threat intelligence sharing across the SOC team.
- Documented incidents, mapped attacks to MITRE ATT&CK, and improved escalation workflows.

CORE SKILLS

- **SOC Operations:** Log Analysis, Alert Triage, Threat Hunting, Escalation, Playbook Execution
- **Security Tools:** Splunk, IBM QRadar, Wireshark, Nmap, Burp Suite, Kali Linux
- **Security Domains:** Incident Response, Vulnerability Management, Phishing Analysis
- **Operating Systems:** Linux, Windows
- **Networking:** TCP/IP, DNS, DHCP, Firewalls, IDS/IPS
- **Scripting & Programming:** Basic Python, Java
- **Database:** SQL

PROJECTS

- NIDS Rule Creation & Testing Lab
- Web Server Log Analysis & Attack Detection (Splunk/QRadar)
- Phishing URL Scanner (Python)
- Network Traffic Analysis (Wireshark)

CERTIFICATIONS

- Certified SOC Analyst (CSA) - EC Council.
- Java Programming – IIT Bombay | Wipro PRP in J2EE.

EDUCATION

B.E. Electronics & Communication Engineering **Nov 2021 - Apr 2025**
Velalar College of Engineering and Technology | CGPA: 8.04