

HARIHARAN A

+919344136854 hariharanvj24@gmail.com linkedin.com/in/hariharan

SUMMARY

Proactive and Detail-oriented Cybersecurity Analyst with expertise in threat detection, incident response, and log analysis using SIEM tools like Splunk, QRadar, and Microsoft Sentinel. Skilled in real-time monitoring, threat hunting, and leveraging the MITRE ATTCK framework to enhance detection and response. Proficient in network analysis, alert triage, and vulnerability management, with a strong focus on improving SOC workflows and ensuring compliance with cybersecurity standards.

EXPERIENCE

L&T TECHNOLOGY SERVICES - CYBERSECURITY ANALYST INTERN Oct 2024 - Jan 2025

- Monitored and analyzed network traffic, security events, and logs to detect and respond to potential threats using SIEM platforms such as Splunk, QRadar, and Microsoft Sentinel.
- Investigated and triaged security incidents, correlating data from multiple sources to identify and mitigate cybersecurity threats.
- Configured and maintained SIEM systems, fine-tuning detection rules and alerts to improve threat visibility and response time.
- Provided detailed incident reports and post-incident analysis, offering actionable recommendations to strengthen security controls and prevent future incidents.

THREAT DETECTION AND ANALYSIS USING SPLUNK (PROJECT) Oct 2024 - Jan 2025

- Implemented a Splunk Enterprise SIEM environment to detect and respond to cybersecurity threats, monitoring for suspicious activities and vulnerabilities. Simulated real-world attacks using Atomic Red Teaming and mapped adversary behaviors with the MITRE ATT&CK framework to enhance threat detection and defense strategies. Conducted security assessments, improved alerting mechanisms, and recommended risk mitigation measures. Utilized tools such as Mimikatz, Metasploit, PowerShell, MITRE ATT&CK, and Atomic Red Teaming to emulate advanced persistent threats (APT) and strengthen security posture and incident response capabilities.

EDUCATION

RAJALAKSHMI ENGINEERING COLLEGE Aug 2023 - April 2025

- Master's in Computer Science Engineering

PANIMALAR ENGINEERING COLLEGE Aug 2018 - May 2022

- Bachelor's in Electronics & Communication Engineering

SKILLS

- | | | | |
|------------------------|----------------------------|---------------------|-----------------------------|
| ○ Networking Protocols | ○ SIEM | ○ Incident Response | ○ Cyber Threat Intelligence |
| ○ Python | ○ Vulnerability Management | ○ Log Analysis | ○ EDR |
| ○ Operating Systems | ○ Malware Analysis | ○ Network Security | ○ Phishing Analysis |

TOOLS

- | | | | |
|---------------|----------------|----------------------|-------------|
| ○ Splunk | ○ MITRE ATT&CK | ○ Virus Total | ○ Wireshark |
| ○ Q Radar | ○ Open VAS | ○ Suricata | ○ Nessus |
| ○ MS Sentinel | ○ YARA | ○ Microsoft Defender | |

CERTIFICATION

CERTIFIED ETHICAL HACKER - CEH March 2024 - March 2027

EC COUNCIL - ECC6492351087