

Surineella Sunitha

Contact No: +91 7893923635

Email Id: sunithasurineella@gmail.com

Career Objective

Looking for the opportunity with dynamic work environment that will allow me to utilize my skills, experience, and willingness to learn and work in making an organization's objective.

Professional Summary

- 6 months of internship experience in Network and Security concepts.
- Good knowledge of architecture and operations of SIEM platform (IBM QRadar) from an Analyst's point of view.
- Strong knowledge in malware analysis and the ability to conduct a detailed analysis of various security-related events like Phishing, Malware, login failures, Ransomware. etc.
- Working on assign tickets queue and understanding and exceeding expectations on all tasked SLA commitments.
- Hands on experience on the Incident Management (IM) support.
- Underwent training on SOC functions and Incident life cycle management.
- Knowledge networking concepts & understanding of networking models.

Technical Skills

- SIEM: IBM QRadar
- EDR: CrowdStrike Falcon
- Email Security: Proofpoint
- Vulnerability Management: Spotlight
- Malware Analysis: Static Analysis Techniques
- Threat Intelligence Tools: VirusTotal, Cisco Talos, IPVoid, MXToolbox
- Ticketing & Incident Management: ServiceNow Ticketing Tool
- Networking & Security: TCP/IP, Cryptography, OSI Model, Cyber Kill Chain

Project:

SIEM, DLP, EMAIL SECURITY , EDR , VULNERABIITY MANAGEMENT

Duration: May 2025 – Oct2025

Key Responsibilities:

- Monitored real-time security events using QRadar SIEM and analyzed incidents to mitigate potential threats.
- Conducted malware analysis and detailed investigations of alerts, escalating to Level-2/Level-3 when necessary.

- Ensured SLA compliance by tracking, resolving, and reporting tickets, along with fine-tuning alerts to improve accuracy.
- Performed regular log analysis, QRadar operational tasks, and optimization for enhanced security operations.
- Aggregated, correlated, and analyzed log data from network and security devices to identify potential vulnerabilities.
- Monitored and analyzed 2nd-level offenses from security devices, providing timely incident response and escalation.
- Analyzed spam email trends and false positives, reporting insights to leadership and optimizing detection mechanisms.
- Gained proficiency in TCP/IP, WAN/LAN concepts, routing protocols.

Education

- B. Tech (AI&DS) in Malineni Lakshmaiah Women's Engineering College — 2025
- Intermediate (MPC) in Sri Chaitanya Junior College — 2021
- NSZP High School — 2019

Declaration

I hereby declare that all the details mentioned above are my own and are true to the best of my knowledge.

Surineella Sunitha