POORNA SUJAMPATHI RATHNAYAKA

SOC ANALYST

Hemel Hempstead, HP24JL, UK | +44 7362 304258 | poornasujampathi@gmail.com
sujampathirathnayaka.com | linkedin.com/in/sujampathi-rathnayaka-304a752a9

PROFESSIONAL SUMMARY

SOC Analyst with 2.5+ years of experience in Security Operations Centers across banking, aviation, and telecommunications environments. Experienced in SIEM monitoring, incident investigation, threat detection, and network traffic analysis using tools such as IBM QRadar, McAfee SIEM, Azure Sentinel, and CrowdStrike. Skilled in log analysis, DDoS detection, and security incident response to support effective threat mitigation.

TECHNICAL SKILLS

SIEM: IBM QRadar, McAfee SIEM, Azure Sentinel
EDR: CrowdStrike, Cortex XDR, Microsoft Defender
Security Tools: Forcepoint DLP, SOCRadar, NetScout Arbor, Darktrace
Security Operations: Incident Response, Alert Triage, Threat Hunting, IOC Analysis, Log Analysis
Technical: Python, Bash, Linux Fundamentals, Network Security, MITRE ATT&CK

PROFESSIONAL EXPERIENCE

Associate Infrastructure Analyst – Air Arabia | Jun 2023 – Sep 2024 (24 hour Shift)

- Monitored and triaged **1000+ daily security alerts** across servers, network devices, firewalls, and endpoints.
- Investigated suspicious activities through **SIEM log analysis, event correlation, and alert validation**.
- Analyzed **network and firewall logs** to detect abnormal traffic patterns and potential DDoS activity.
- Conducted **incident investigation and escalation** following SOC procedures.
- Prepared monthly security reports and presented incident findings.
- **Best Performance Award – 2023**

Information Security Analyst – Nations Trust Bank | Jan 2023 – May 2023 (12 hour Shift)

- Performed **SIEM monitoring and threat detection** using McAfee SIEM, CrowdStrike, and SOCRadar.
- Investigated **security alerts and supported incident response activities** following SOC procedures.
- Mitigated a **5-hour DDoS attack** by identifying malicious IP ranges and updating firewall rules.
- Worked in environments with basic awareness of GDPR and PCI-DSS compliance.
- Prepared monthly security reports and presented incident findings.

Information Security Analyst (Intern) – SLT-Mobitel | Jan 2022 – Dec 2022 (6 hour Shift)

- Performed log correlation and anomaly detection using IBM QRadar and Cortex XDR.
- Analyzed **network traffic and DDoS activity** using NetScout Arbor to detect abnormal traffic patterns.
- Monitored **WAF logs and privileged access activity** using CyberArk to support SOC monitoring.
- Assisted in **developing and optimizing SOC playbooks for new security tools**
- Supported **L2 analysts with incident reporting, documentation, and security report presentations**.

EDUCATION

MSc Cyber Security – University of Hertfordshire (2025)
BSc (Hons) IT – Cyber Security – SLIIT (2020-2024)

CERTIFICATIONS

IBM Cybersecurity Analyst – Coursera | Red Hat - Enterprise Linux Fundamentals