Poorna Sujampathi Rathnayaka

Security Operations Centre (SOC) Analyst

Hatfield, United Kingdom | +44-7768875587 | poornasujampathi@gmail.com| sujampathirathnayaka.com | linkedin.com/in/sujampathi-rathnayaka-304a752a9

Summary

SOC Analyst with 2.5+ years of hands-on experience in Tier 1/2 Security Operations Centre (SOC) environments across banking, aviation, and telecommunications. Experienced in 24/7 security monitoring, high-volume alert triage, incident detection and response, threat hunting, log analysis, and IOC investigation across SIEM, EDR, and XDR platforms. Hands-on experience with Microsoft Defender, CrowdStrike, IBM QRadar, McAfee SIEM, and Microsoft Sentinel, with expertise in MITRE ATT&CK, detection engineering, correlation rule tuning, SOC automation, and Python/KQL scripting. Proven ability to investigate and escalate security incidents within SLA requirements while developing automation and detection capabilities to improve SOC efficiency.

Experience

SOC Analyst (Tier 2) — Air Arabia, UAE *Jun 2023 – Sep 2024*

- **Alert Triage & Incident Response:** Monitored and triaged 1,000+ daily security alerts across enterprise network and endpoint environments, investigating high-severity threats within target SLA timelines
- **SOC Automation & Optimization:** Engineered custom automation tools to streamline incident workflows and improve overall SOC operational efficiency
- **Threat Detection & Rule Tuning:** Executed threat detection using Microsoft Defender and tuned alert correlation rules to reduce false positive rates
- **Cross-Functional Incident Escalation:** Collaborated closely with NOC teams to investigate, contain, and escalate critical incidents efficiently
- **Key Achievement:** Awarded Best Performance Award (2023) for outstanding contributions to SOC monitoring and incident handling

Information Security Analyst (SOC) — Nations Trust Bank, Sri Lanka *Feb 2023 – May 2023*

- **SIEM & EDR Operations:** Performed real-time security event analysis, monitoring, and threat correlation using McAfee SIEM and CrowdStrike EDR
- **Live Attack Mitigation:** Detected and successfully mitigated a live targeted DDoS attack, protecting critical banking operations from disruption
- **Incident Investigation & Reporting:** Executed end-to-end incident investigations, analyzed Indicators of Compromise (IOCs), and authored comprehensive post-incident reports
- **DLP Monitoring & Playbook Development:** Monitored data exfiltration attempts using Forcepoint DLP and updated standard SOC playbooks to enhance team response procedures

Information Security Analyst Intern (SOC) — SLT-Mobitel, Sri Lanka *Feb 2022 – Feb 2023*

- **Log Analysis & Threat Identification:** Monitored security logs using IBM QRadar SIEM to identify anomalous behaviour and potential security breaches
- **Tier 1 SOC Workflows:** Supported daily SOC operations, including initial alert triage, IOC verification, and threat escalation
- **Perimeter & Access Defence:** Assisted in detecting DDoS attacks and monitored web traffic and privileged access via WAF and CyberArk PAM

SOC Projects

Threat Intelligence & Detection Engineering Platform (2025 – Present)

- Built a threat intelligence platform ingesting 100+ RSS feeds, applying TF-IDF and cosine similarity to significantly cut analyst noise
- Enriched and scored IOCs in real time using VirusTotal, AbuseIPDB, EPSS, and CISA KEV threat intelligence feeds
- Mapped detected threats to 14 MITRE ATT&CK tactics and 52+ techniques via interactive heat-map visualizations
- Auto-generated detection rules in Splunk SPL, Microsoft Sentinel KQL, and Sigma YAML directly from IOCs
- Delivered multi-channel SOC alerting and AI-generated executive threat briefings via Slack, Teams, and Email

Phishing Incident Response Tool

- Built a triage tool to parse email headers, extract malicious URLs/attachments, and automatically check IOC reputation scores

Education

MSc Cyber Security — University of Hertfordshire, UK (2024 – 2025)

BSc (Hons) IT, Specialized in Cyber Security — SLIIT, Sri Lanka (2020 – 2024)

Certifications

- IBM Cyber Security Analyst
- Microsoft SC-200: Security Operations Analyst — Scheduled: Nov 2026

Key Skills

Security Operations Centre (SOC) Monitoring, 24/7 Security Event Monitoring, Alert Triage, Incident Detection & Response (IDR), Log Analysis, IOC Investigation & Enrichment, Threat Hunting, Threat Intelligence, DDoS Detection & Mitigation, MITRE ATT&CK Framework, Correlation Rule Tuning, SOC Playbook Development, SOC Automation & Scripting, Data Loss Prevention (DLP), SLA-Driven Incident Escalation

Tools & Technologies

SIEM Platforms: IBM QRadar, Azure Sentinel, McAfee SIEM, FortiAnalyzer

EDR / XDR: CrowdStrike, Microsoft Defender, Cortex XDR

Security & Network: CyberArk PAM, Forcepoint DLP, NetScout Arbor, Darktrace, WAF

Scripting & Analytics: Python, KQL