

POORNA SUJAMPATHI RATHNAYAKA

SOC ANALYST

poornasujampathi@gmail.com | <https://sujampathirathnayaka.com/>

linkedin.com/in/sujampathi-rathnayaka-304a752a9/

Hemel Hempstead, Hertfordshire, HP2 4JL, GB | +44-7362-304258

SOC Analyst with 2.5+ years of hands-on experience supporting enterprise-scale Tier 1 / Tier 2 24/7 Security Operations Center (SOC) environments across banking, aviation, and telecommunications sectors. Skilled in SIEM monitoring, alert triage, incident response, threat intelligence, DDoS mitigation, and endpoint detection & response (EDR). Experienced working within GDPR and PCI-DSS regulated infrastructures supporting 24/7 continuous operations. Possesses strong analytical and problem-solving capabilities with a focus on reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Seeking SOC Analyst opportunities to contribute to safeguarding critical systems and ensuring continuous operations.

WORK EXPERIENCE

Associate Infrastructure Analyst Jun 2023 - Sep 2024

Air Arabia | Hemel Hempstead

- Monitored and analyzed 1,000+ daily security events across servers, APIs, firewalls, and endpoints within a PCI-DSS regulated airline environment, contributing to effective information security and vulnerability management.
- Conducted real-time SIEM monitoring and alert triage, reducing manual log investigation workload by 30% through automation scripting and enhancing continuous operations.
- Utilized Microsoft Defender and Stella Cyber for forensic investigations and endpoint security threat detection, supporting threat hunting efforts.
- Enhanced SOC-NOC coordination to reduce MTTR and improve high-severity alert response across multi-system enterprise infrastructure.
- Awarded Best Performance Award (2023).

Information Security Analyst Jan 2023 - May 2023

Nations Trust Bank | Hemel Hempstead

- Performed continuous SIEM monitoring using McAfee SIEM, CrowdStrike, and SOCRadar in a regulated banking environment, supporting robust cybersecurity measures and access control.
- Mitigated a live 5-hour DDoS attack by identifying malicious IP ranges and updating firewall/IPS rules, ensuring zero data loss and maintaining operational continuity.
- Documented root cause analysis and incident timelines to strengthen SOC playbooks and future response strategies, contributing to continuous improvement and effective communication.
- Maintained security posture during recovery using Forcepoint DLP operations, demonstrating effective access control.

Information Security Analyst (Intern) Jan 2022 - Dec 2022

SLT-Mobitel | Hemel Hempstead

- Performed log correlation and anomaly detection using IBM QRadar and Cortex XDR to identify potential security incidents, supporting threat hunting efforts.
- Contributed to SOC playbook development and standardized incident response protocols, enhancing incident management capabilities and documentation.
- Conducted volumetric traffic analysis and DDoS detection using NetScout Arbor in telecom-scale environments.
- Monitored web traffic via WAF and managed privileged access monitoring using CyberArk, contributing to overall cybersecurity and vulnerability management.

PROJECTS

SOC Intelligence Platform

Developed a real-time SOC dashboard aggregating cybersecurity intelligence from 100+ RSS feeds. Engineered automated threat severity classification using keyword-based analysis and implemented a SQLite backend for historical threat tracking. Built interactive visualizations, automated critical alert email reporting, and a responsive UI using React and TypeScript.

Advanced BYOD Security Framework (MSc Project)

Developed a secure BYOD solution using AES-128 encryption, UUID-based device authentication, and machine learning (Isolation Forest, CNN) for anomaly detection.

BYOD Data Protection System (BSc Project)

Built a DLP-integrated file access control mechanism linked to Active Directory to prevent unauthorized access after employee offboarding.

SIEM Log Processing Automation

Automated log parsing and alert analysis using Python to improve SOC efficiency and reduce manual triage time.

Phishing Email Detection Tool

Developed a Python-based email threat detection system to identify and quarantine phishing attempts.

CORE SKILLS

Security Operations: SIEM, IBM QRadar, McAfee SIEM, Azure Sentinel, EDR, CrowdStrike, Cortex XDR, Microsoft Defender, SOC Playbooks, Intrusion Detection, Access Control, Physical Security Monitoring, Vulnerability Management, Security Operations.

Threat Detection & Mitigation: Real-time monitoring, Threat Hunting, DDoS Mitigation, IOC Analysis, MITRE ATT&CK framework, Threat Intelligence, Vulnerability Scanning.

Technical Tools: Darktrace, FortiAnalyzer, Zabbix, Grafana, SOCRadar, NetScout Arbor.

Technical Proficiencies: Automation Scripting, Python, Log Correlation, Network Security, Data Encryption, Incident Documentation, SIEM, Incident Management, Resolving Issues, Investigations, Analytical, Written and Verbal Communication.

Stella Cyber, Microsoft Defender, McAfee SIEM, CrowdStrike, SOCRadar, Forcepoint DLP, IBM QRadar, Cortex XDR, NetScout Arbor, WAF, CyberArk, AES-128 encryption, UUID-based device authentication, Isolation Forest, CNN, Active Directory, Python, React, TypeScript

EDUCATION

- **University of Hertfordshire** 2025
MSc Cyber Security

- **SLIIT** 2024
BSc (Hons) IT (Specialization in Cyber Security)

AWARDS

- **Best Performance Award** 2023
Air Arabia (ISA)
- **President Scouts Award** 2019
Sri Lanka Scout Association

CERTIFICATES

- **Certified Information Security Manager (CISM)**
Cybrary
- **IBM Cybersecurity Analyst**
Coursera
- **Fundamentals of Red Hat Enterprise Linux**
Coursera