

POORNA SUJAMPATHI RATHNAYAKA

Hemel Hempstead, HP2 4JL | +44-7362-304258 | poornasujampathi@gmail.com

LinkedIn: [linkedin.com/in/sujampathi-rathnayaka-304a752a9/](https://www.linkedin.com/in/sujampathi-rathnayaka-304a752a9/)

Work Eligibility: Eligible to work Full time in the UK

PROFESSIONAL SUMMARY

Junior SOC Analyst with hands-on experience in 24x7 security monitoring, SIEM alert triage, incident response, and threat detection across banking, aviation, and enterprise IT environments. Skilled in L1/L2 SOC operations, log analysis, endpoint security, and DDoS mitigation using industry-standard tools including IBM QRadar, CrowdStrike, Microsoft Defender, Darktrace, and McAfee SIEM. I am currently completing an MSc in Cyber Security and seeking Junior / Graduate SOC Analyst roles in the UK.

CORE SKILLS

- **SOC Operations:** L1/L2 SOC Monitoring (24x7 environments), Alert Triage & Escalation, Incident Response & Investigation, SIEM Use Case Analysis, SOC Playbooks & Runbooks, Incident Documentation & Reporting, Threat classification aligned with MITRE ATT&CK framework, Incident tracking and escalation using ticket based workflows
- **Threat Detection & Security:** Log Analysis (Network, Endpoint, API), DDoS Detection & Mitigation, Endpoint Detection & Response (EDR), Vulnerability Monitoring, Data Loss Prevention (DLP), GDPR & PCI DSS Awareness
- **SOC Tools & Technologies:**
 - SIEM: IBM QRadar, McAfee SIEM, Azure Logs
 - EDR/XDR: CrowdStrike, Cortex XDR, Microsoft Defender
 - Security: Darktrace, NetScout Arbor, FortiAnalyzer
 - Monitoring & Logging: Zabbix, Grafana, Site24x7
 - Data Protection: Forcepoint DLP
 - Cloud & Infrastructure: Microsoft Azure

PROFESSIONAL EXPERIENCE

IT Security Intern

London Property & Letting Management, UK

Nov 2024 – Present

- Performed continuous monitoring of system and security events, escalating suspicious activity in line with SOC procedures.
- Supported access control and user account security for internal systems, ensuring data confidentiality and integrity.
- Assisted in incident documentation and internal security reporting.
- Delivered IT troubleshooting and network support, supporting secure day-to-day operations.

SOC Analyst (Infrastructure & Monitoring)

Air Arabia (ISA)

Jun 2023 – Sep 2024

- Monitored SIEM alerts across servers, APIs, and network infrastructure, supporting L1/L2 incident triage.
- Investigated security events using Microsoft Defender and Stella Cyber, contributing to endpoint threat containment.
- Developed automation scripts for log processing, improving alert visibility and SOC efficiency.
- Produced security performance dashboards using Zabbix and Grafana.
- Coordinated SOC and NOC workflows to reduce incident resolution time.

Information Security Analyst

Nations Trust Bank

Jan 2023 – May 2023

- Conducted real-time monitoring of network traffic and SIEM alerts using McAfee SIEM, CrowdStrike, and SOCRadar.
- Played a key role in mitigating a live DDoS attack, identifying malicious IP ranges and supporting firewall/IPS rule updates.
- Documented incident timelines, root causes, and response actions to enhance SOC playbooks.
- Supported Forcepoint DLP operations during post-incident recovery.

Information Security Analyst Intern

SLT-Mobitel

Jan 2022 – Jan 2023

- Performed log analysis and anomaly detection using IBM QRadar and Cortex XDR.
- Assisted in SOC alert triage, incident correlation, and escalation.
- Monitored web traffic via WAF, identifying suspicious access patterns.
- Gained exposure to volumetric traffic analysis and DDoS detection using NetScout Arbor.

EDUCATION

MSc in Cyber Security | University of Hertfordshire, UK *Expected Graduation: Nov 2025*

BSc (Hons) in IT (Specialization in Cyber Security) | SLIIT, Sri Lanka *Graduated: 2024*

TECHNICAL PROJECTS

Advanced BYOD Security Framework (MSc Project)

- Designed a secure BYOD access control system with AES 128 encryption and UUID-based device authentication.

- Implemented Isolation Forest ML models for anomaly detection and CNN-based facial recognition for suspicious logins.

Focused on endpoint security, access governance, and insider-threat prevention.

BYOD Data Protection System (BSc Final Project)

- Built a DLP-integrated file access solution linked to Active Directory.
- Prevented unauthorized access following employee off-boarding events.

CERTIFICATIONS

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

HONORS & AWARDS

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

VOLUNTEER EXPERIENCE

- **Scout Leader & District Inspector of Medals** – Sri Lanka Scouts Association (2022 – 2025)
- **Vice President** – Faculty of Computing Media Unit, SLIIT (2022 – 2024)

ADDITIONAL INFORMATION

- Experience working in regulated environments (Internet Service Provider, Banking & Aviation)
- Strong understanding of SOC escalation paths and incident workflows
- Comfortable working shift-based SOC operations
- Contributed to DDoS mitigation activities reducing service disruption during a live incident