RESHMI VIJAYAN

Nationality: Indian •
Address: Arkkal Krishna Vilasom, Ulloor, Medical College P.O, Kerala, Thiruvananthapuram - 695011, India
Phone number: +91 8590022990 • **Email address:** reshmivijayan05@gmail.com •
LinkedIn: linkedin.com/in/reshmi-vijayan-883b61179

Experienced and result-driven **cybersecurity professional with 5+ years of hands-on expertise in Security Operations Centers (SOC), incident management, and threat intelligence.** Skilled in managing and optimizing SOC operations, monitoring security events through SIEM tools, and developing playbooks for automated incident response. I am now seeking senior leadership roles such as Senior SOC L2, SOC Lead, SOC L3, or SOC Manager to leverage my skills in cybersecurity monitoring, threat detection, and team leadership to drive security initiatives and protect organizational assets.

Work Experience

04/2024 — present
India

Senior Associate Consultant (Senior L2 + Lead)
Infosys, Trivandrum

- Lead SOC operations using SIEM tools (IBM QRadar, Azure Sentinel, Splunk) for event analysis and incident management.
- Automated security playbooks in Cortex XSOAR, improving efficiency and response times.
- Managed L2 incident response, performed root cause analysis, and conducted proactive threat hunting.
- Mentored junior analysts and tuned use cases to reduce false positives and improve detection.
- Provided 24/7 client support, ensuring SOC uptime and handling escalated issues.
- Conducted threat hunting with EDR tools, optimized logs, and created new detection use cases.
- Onboarded/offboarded log sources and delivered weekly/monthly QBRs to banking clients from Europe and India.
- Led tabletop exercises for L1 teams, providing training and guidance for investigations.

09/2022 — 04/2024
India

Global L2 Security Analyst | *Cyber Proof UST Company, Trivandrum*

- Monitored security events using SIEM, IDS/IPS, and firewalls to detect and respond to potential threats.
- Conducted threat intelligence analysis and integrated feeds to address emerging security risks.
- Onboarded and configured log sources and use cases to improve detection accuracy.
- Mentored junior analysts, enhancing their technical and operational skills.
- Contributed to playbook development and process improvements to streamline incident response.
- Engaged with clients, including banking customers, to ensure security posture alignment and deliver comprehensive support.

Participation in Cybersecurity Drills & Audits

- IDRBT Cyber Security Drills
- Participated in multiple audit engagements, including HI TRUST, CREST, SOC2, KPMG, EY, Deloitte, and Microsoft Audits.

Work Experience

04/2021 — 09/2022
India

L1 Security Analyst & POC | Assurance Audit *UST Global - CyberProof UST Company,* Trivandrum

- Analyzed security incidents, correlated logs, and conducted initial investigations of low to medium-severity threats in the SOC.
- Assisted with audits (SOC2, CREST), preparing documentation and presenting findings to auditors.
- Supported integration of new log sources and configured SIEM rules to enhance threat detection.
- Contributed to security awareness training, improving SOC team knowledge and incident response readiness.

02/2020 — 04/2021
India

System Security Engineer | *IT Professionals Cooperative Society, Trivandrum*

- Developed **disaster recovery plans and security policies** to protect IT infrastructure.
- Managed firewall configurations, conducted security audits, and mitigated risks.
- Administered KSFE email server and ensured security compliance.
- Monitored firewalls through **Azure** and used **Zoho** and **Telnet** for ticket management.

Key Competencies & Skills

- **SIEM & Security Tools**: Expertise in IBM QRadar, Azure Sentinel, Splunk, Google Chronicle, Palo Alto Cortex XSOAR, and endpoint protection tools like CrowdStrike, Microsoft Defender ATP, and Sentinel One.
- **Incident Response & Automation**: Skilled in threat hunting, incident management, and automating SOC workflows, including playbook development for optimized incident response.
- **Log & Use Case Management**: Proficient in onboarding log sources, creating use cases, and tuning SIEM rules to enhance detection accuracy.
- **Threat Intelligence & Risk Management**: Experience in integrating threat intelligence feeds, identifying risks, and applying best practices for vulnerability assessments and security risk mitigation.
- **Scripting & Integration**: Strong in scripting (PowerShell, KQL), reporting, and integrating third-party tools/APIs with platforms like Cortex XSOAR.

Education

- **M.Tech in Network Engineering |** Government Engineering College, Barton Hill, Trivandrum | 2016 - 2018
- **B.E. in Computer Science and Engineering |** Noorul Islam University, Tamil Nadu | 2012 - 2016

Certifications

- Cortex™ XSOAR - Automation and Orchestration (EDU-380)
- Palo Alto - Troubleshooting Installations and Configuration Issues **|** Palo Alto - Content Management
- Palo Alto - Threat Intelligence Feeds and API Integration
- Palo Alto - Cortex XDR 3: Endpoint Protection **|** Palo Alto - Third-Party Integrations in Cortex XSOAR
- Google Chronicle - SIEM Fundamentals **|** Security Operation Center Analyst Certification - NASSCOM

Rewards and Recognitions

- 2023, Rising Star Award, UST- cyber-Proof account
- 2022, Super Star Award, UST- cyber-Proof account
- 2021, Rookie Rock star Award, UST- cyber-Proof account
- 2016, 2nd Rank in academic exam, Computer Science and Engineering Department, Noorul Islam University
- 2015, Best IET Academic Performance Award

Languages

- **English:** Fluent **| Malayalam:** Fluent **| French:** Beginner **| German:** Beginner **| Hindi:** Beginner **| Tamil:** Elementary **| Sanskrit:** Intermediate