Anand Mohankumar

anand.mohankumar@outlook.com • linkedin.com/in/anandmohankumar •
https://github.com/Anand-Mohankumar

Security Analyst

Security Professional with 3+ years in Security Operations of EQS Group, a leading international cloud software provider, I have a strong foundation in Incident Response Procedures and Vulnerability Management. Skilled at investigating alerts, analyzing emails and security logs, collaborating effectively with cross-functional teams to mitigate incidents and to improve organizational security posture.

WORK EXPERIENCE

Revenue Operations Analyst (Security and Compliance) • Full-time

EQS Group — **Kochi, Kerala • Oct 2024 - Present**

- Handling RFPs and Due Diligence requests from Customers and Prospects with focus on Organizational Compliance, Product Security and data protection.
- Collaborated with security and engineering teams to ensure customer assurance responses accurately reflected the organization’s security controls.
- Applied prior SOC experience to improve risk communication and strengthen secure business operations.

Associate Engineer - Information Security • Full-time

EQS Group — **Kochi, Kerala • Jun 2021 - Oct 2024**

- Led collaborative incident response with stakeholders, identifying threats, implementing mitigation and documenting the procedures
- Proficient in security tools like Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) and attack surface management tools
- Proactively monitored publications and advisories on emerging vulnerabilities, attack vectors and countermeasures. Conducted investigations to assess any potential threats to the organization and assets
- Experience with fine-tuning security tools by adding IOC's to improve detection capabilities
- Proficient in utilizing Email forensics to identify phishing campaigns
- Provided assistance in customer audits and assessments, addressing inquiries regarding organizational compliance, infrastructure security, and product security

CERTIFICATIONS

Certified in Cybersecurity (CC)

Jul 2024 - Jul 2027

ISC2

EDUCATION

Cyber Threat Hunting L1

Active Countermeasures — Feb 2024 - Feb 2024

- Knowledge of threat hunting processes.
- Knowledge on investigating endpoints
- Hands-on experience utilizing threat hunting tools to find C2 channels through coursework labs.

Intermediate - MITRE ATTACK

Attack IQ — Feb 2024 - Feb 2024

- Knowledge and understanding of Threat Landscape

Becoming a SOC Analyst - Level 1

Cybrary — Aug 2023 - Sep 2023

- Hands-on experience with Splunk for log analysis and investigation, developed through coursework labs.
- Hands-on experience in utilizing tools to create Forensic images of endpoint for analysis.
- Familiar with On Prem and Azure Active Directory

CCNA Routing & Switching (200-125)

Cisco Networking Academy — May 2019 - Nov 2019

- Networking fundamentals
- Security fundamentals

Bachelors in Electronics

School of Technology and Applied Science — Edappally, Kochi • Jul 2014 - Jul 2017

SKILLS

Industry Knowledge: Security Incident Management, OSINT, Cloud Computing, OWASP, Monitoring and Investigation, Networking concepts, Vulnerability Management, Log Analysis, Compliance Frameworks, Cyber Security, TCP/IP, TPRM, SCRM

Tools and Technologies: Wazuh, EDR, XDR, SIEM, Splunk, AWS, Linux, Nmap, OpenVAS, ZAP, MITRE ATT&CK, Active Directory, Email Forensics, Wireshark

Interpersonal Skills: Communication, Problem Solving

Interests: CTF, OSINT, Threat Hunting