MOHAMMAD ASHRAF *SOC Analyst*

K.asrf001@gmail.com 8766738319 linkedin.com/in/mohammad-asrf Mumbai

PROFILE

Cybersecurity professional with foundational expertise in threat detection, incident response, and vulnerability management. Skilled in network monitoring, Security Information and Event Management (SIEM), and threat analysis. Proven ability to identify and mitigate security risks, ensuring robust protection for organizational assets. Eager to leverage and expand technical skills in a dynamic cybersecurity role, contributing to the organization's security posture with dedication and innovation.

PROFESSIONAL EXPERIENCE

Capgemini, Analyst 02/2023 – Present | Mumbai, India

Project- 1 Global SIEM Monitoring
Role- Level 1 SOC Analyst
Client is a leading automotive manufacturing MNC based out of Europe, this project is intended to provide 24*7 monitoring services covering the EMEA, PSA, NA, LATAM and CHINA region.

Key responsibilities

- Perform initial triage and investigation of security incidents using SIEM tools, identifying root causes and mitigating risks, ensuring timely response within SLA guidelines.
- Analyze logs, network traffic, and data sources to detect and resolve security incidents, reducing average incident response time.
- Monitor and prioritize alerts generated by SIEM tools, escalating critical incidents based on severity and business impact.

Key Achievements

- Recognized as a Learning Champion in 2024 for my exceptional and consistent performance in the project.
- Recognized multiple times by senior management for consistently maintaining 100% SLA compliance and ensuring timely acknowledgment.

Project -2 MSSP Project
Role- Level 1 SOC Analyst
This project provides 24/7 monitoring services for 16 clients, including both internal and external customers, all integrated on a single SIEM platform.

Key responsibilities

- Monitor and analyze security events and logs from QRadar data sources, prioritizing issues for investigation. Perform regular health checks and gap analyses to identify monitoring blind spots.
- Provide daily, weekly, and monthly security reports with actionable insights, collaborating with teams to address vulnerabilities and ensure compliance with best practices.

Key Achievements

- Monitored team performance against SLA targets and led post- incident debriefs to identify improvements, ensuring faster resolution and consistent SLA and MTTR compliance.
- Successfully functioned as a dedicated SPOC for multiple clients, ensuring smooth communication between clients and internal teams.
- Consistently maintained SLAs above 90%, reduced MTTD by 25%, and ensured timely acknowledgment.
- Played a key role in automating the integration of all Indicators of Compromise (IOCs) into SIEM platforms via the Malware Information Sharing Platform (MISP), significantly improving the efficiency of threat intelligence workflows.

SKILLS

SIEM Tools — IBM QRadar, Microsoft Azure Sentinel, Devo, Swimlane
Ticketing Tools — Jira, ServiceNow, CONA
EDR Tools — CrowdStrike, Microsoft Defender
Threat Intelligence Tools — OpenCTI, IBM X-Force, Virus Total, AbuseIPdb
Others — Threat Hunting, Cyberkill Chain, MITRE Framework, Malware Analysis, Phishing Mail Analysis, KQL, Python (Basics), Windows, Network Administration, Centreon

CERTIFICATES

Microsoft Certified: Security Operations Analyst Associate(SC-200)
Microsoft Certified: Azure Security Engineer Associate(AZ-500)
Microsoft Certified: Azure AI Fundamentals (AI-900)

EDUCATION

D. Y. Patil College of Engineering, BE in Information Tecnology 07/2021 | Pune

M. H. Saboo Siddik Polytechnic, Diploma in Computer Engineering 06/2018 | Mumbai