afrozmohammad447@gmail.com
9494294010

MOHAMMAD AFROZ

CAREER OBJECTIVE

Result-oriented professional with 2.2+ years of experience in Information technology and Proven knowledge of Information security. Aiming to leverage my skills to successfully fill the SOC Analyst role at your company.

PROFESSIONAL SUMMARY

- Having 2.2+ years relevant experience in Information Security and currently working as Security Analyst (SOC Team)
- Experience on SIEM (Security Information and Event Management) tools like Monitoring real-time events using ArcSight, Qradar.
- Experience on SOAR Tool – Siemplify
- Investigating and creating case for the security threats
- Experience on performing log analysis and analyzing the critical alerts
- Recognizing attacks based on their signatures.
- Planned and executed routine repairs and system upgrades
- Preparing reports as per client requirements
- Worked on creation and modification of rules, use cases & playbooks in ArcSight and Siemplify
- Filling the Daily health checklist and status of Security Devices and Connectors
- Creating the tickets in ticketing tool.

SKILLS & ABILITIES

- SOC (Security Operation Center)
- SIEM (Security Information and Event Management) Tool: ArcSight & Qradar
- SOAR Tool: Siemplify
- Vulnerability Assessment Tool: Qualys Guard
- Phishing Email Analysis
- Malware analysis
- Create, Modify and Update Security Information Event Management (SIEM) Tools.

EDUCATION

- B. Tech in EEE from Hindustan University, Chennai – Batch of 2019
- Intermediate from Narayana Jr. college, Kadapa- Batch of 2015
- SSC from Nagarjuna Model school, Kadapa – Batch of 2013

WORK EXPERIENCE

Currently working as Security Analyst in HCL Technologies, Chennai from August 2019 to Till Date

PROFESSIONAL EXPERIENCE

Project - Security Monitoring and Operations
Role – Senior SOC Analyst
Responsibilities -

- Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Responding to various security alerts, incidents for various client's and scanning for vulnerabilities using tools like Qualys.
- Monitoring real-time events using SIEM tools like ArcSight, Qradar.
- Monitoring and working on Cases in Soar Platform like Siemplify.
- Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Created filters, active channels, queries, Dashboard etc. in ArcSight for monitoring purpose.
- Configured reports in ArcSight ESM and ArcSight Logger as per the requirement.
- Analyzing daily, weekly and monthly reports.
- Creating the tickets in ticketing tool.
- Preparing and publishing Advisories to Customers

CERTIFICATIONS

- SIEMPLIFY Certified Soar Analyst
- SOC Analyst 1 Elite
- SOC Analyst Training
- CNSS Certified Network Security Specialist
- Qualys Guard Vulnerability Management
- Splunk 7.1x Fundamentals
- Fortinet Network Security Expert Level 1: Certified Associate

PLACE:
DATE:

MOHAMMAD AFROZ