MOHD ATIF ANWAR

SOC ANALYST

chandpur Bijnor UP -246725 | anwarsoc7@gmail.com | 91+ 9149262301

PROFILE INFO

With **1.5 years** of experience as a **Security Analyst** at **FIRST CERT**, I have developed strong expertise in using **Q-RADAR**, **ManageEngine**, and Incident Response Review for effective escalation and case management. I am proficient in overseeing **24/7 SOC** operations, including **log monitoring**, **security information management**, global **threat monitoring**, and providing anti-phishing, anti-malware, and spam mail protection. Additionally, I have hands on experience with **EDR**, enhancing endpoint detection and response capabilities.

EDUCATION

2022 - 2025

RGPV UNIVERSITY

- B-tech in Mechanical

2017 - 2020

JAMIA MILLIA ISLAMIA UNIVERSITY

- Diploma in mechanical

2014 - 2016

MATRICULATION

- Fatherson public school

SKILLS

- Q-Radar (SIEM)
- EDR
- Manage Engine (Ticketing Tool)
- Zendesk HRone
- Threat Monitoring
- log monitoring
- phishing/malicious email Analysis
- CIA triad
- Cyber Kill Chain
- OSI model
- MITRE framework .
- Linux
- Python
- AUTOCAD
- Windows
- Excel
- word
- Power Point

WORK EXPERIENCE

Security Analyst SOC L1, FIRST CERT, Bengaluru, Karnataka 560078, India NOV 2023 - PRESENT

- Experienced Cyber Security Analyst with expertise in SIEM tools, EDR, incident response, and security monitoring. Skilled in phishing analysis, threat escalation, and trend analysis.

Accomplishments:

- Analyzed the latest alerts for relevancy and urgency.
- Created cases in Manage Engine and prepared notifications for technical teams on incidents.
- Handled and investigated escalated threats/events/incidents at **SOC Level 1**, utilizing SEIM for monitoring detection and response. Successfully handled **P3**, **P2**, and **P1** alerts within SLA with **98%** accuracy, ensuring critical incidents were managed with **98-99%** accuracy.
- Handled phishing/malicious emails reported to the security mailbox.
- Collaborated as a Security Analyst to create new trouble tickets in Manage Engine for alerts and escalated tickets to Tier 2/Incident Response.
- Monitored security events of critical systems (e.g., email servers, database servers, web servers, Active Directory).
- Analyzed offenses to differentiate between true positives and false positives.
- Followed escalation matrix for incident follow-ups, ensuring corrective actions aligned with incident severity and SLA standards.
- Documented and tracked inquiry statuses, coordinated responses, and ensured customer satisfaction.
- Updated the number of open incidents across all teams at the end of each shift.

LANGUAGES

- English
- Hindi

ENPHASE ENERGY Pvt Ltd
SOC Analyst

JAN 2022- AUG 2023

- As a Security Analyst, I was responsible for analyzing alerts to assess their relevancy and urgency, creating cases in ManageEngine, and notifying technical teams for incident action. I investigated phishing and malicious emails, escalated threats, events, and incidents at SOC **Level 1**, and created new trouble tickets for alerts while escalating critical issues to Tier 2/Incident Response. My role involved monitoring critical systems such as email servers, databases, web servers, and Active Directory, security controls using IBM QRadar, and distinguishing between true and false positives. I ensured incident follow-ups were handled efficiently, with corrective actions taken within SLA. Additionally, I provided regular SIEM and security device health status reports to stakeholders, maintained customer satisfaction through effective tracking and response coordination, and conducted daily and monthly trend analysis of security incidents to enhance the organization's security posture.

Accomplishments:

- Analyzed alerts, created cases in Manage Engine, and notified technical teams for incident action.
- Investigated phishing emails and escalated threats/incidents to SOC Level 1 and Tier 2.
- Monitored critical systems (email, database, web servers, Active Directory) and applied security controls using IBM QRadar.
- Managed incident follow-ups, ensuring corrective actions were taken within SLAs .

CERTIFICATION

- Tools of the trade: Linux and SQL
- Cyber Threat Intelligence 101
- Assets, Threat, Vulnerabilities
- Foundation of security
- Manage security risk

CORE COMPONENT

- Sound knowledge of Security Operations Center services, Incident Response, Email-Analysis.
- Well versed with MITER Attack & Cyber Kill Chain Methodology.
- Fundamental on Malware analysis.
- Knowledge with Linux and Windows servers.
- Sound Knowledge of encryption, hashing, HIDS, NIDS, and firewall technology familiar with AV, WAF, and VPN .

Willingness to Relocate

Open to relocating for the right opportunity.