Md Riyaz Ahmed

Contact No: **+91 7349466328**
E-mail ID: **mdriyazahmed1202@gmail.com**
LinkedIn: **https://www.linkedin.com/in/md-riyaz-ahmed/**

CAREER OBJECTIVE:

Dedicated SOC Analyst with 3+ years of experience in security monitoring, incident triage, and phishing investigations. Skilled in leveraging SIEM, EDR, and email security solutions to detect, analyze, and escalate threats in 24/7 SOC environments. Seeking to enhance organizational security posture by driving effective incident response, threat detection, and risk reduction through proactive monitoring and analysis.

PROFILE SUMMARY:

- Results-driven SOC Analyst with 3+ years of hands-on experience in 24/7 Security Operations, specializing in security monitoring, log analysis, and incident response.
- Skilled in leveraging SIEM platforms (Splunk Enterprise Security, IBM QRadar) and EDR solutions (CrowdStrike Falcon) to detect, triage, and contain threats.
- Proficient in malware detection, log correlation, phishing investigations, and SLA-driven incident escalations. Adept at analyzing network traffic, firewall logs, IDS/IPS alerts, DNS anomalies, and proxy activity to identify Indicators of Compromise (IoCs).
- Experienced in integrating threat intelligence feeds (VirusTotal, AlienVault OTX, MITRE ATT&CK) to enrich investigations and accelerate Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- Knowledgeable in security frameworks and compliance standards (NIST CSF, ISO 27001, CIS Controls, GDPR) with proven ability to document incident playbooks, standard operating procedures (SOPs), and knowledge base articles for process improvement.

CORE COMPETENCIES:

- SOC Monitoring & Incident Response
- SIEM Analysis & Rule Optimization
- Endpoint Detection & Response (EDR)
- Phishing & Email Security
- Threat Intelligence & TTP Analysis – VirusTotal, AlienVault OTX, MITRE ATT&CK mapping, IoC enrichment
- Log Analysis & Forensics (Windows/Linux)
- Network Security Monitoring – Firewalls, IDS/IPS, DNS, Web Proxy analysis, and anomaly detection
- SLA Compliance & Security Reporting

PROFESSIONAL EXPERIENCE:

SOC Analyst
ITC Infotech | June 2022 – Present

- Monitored and analyzed security alerts from SIEM (Splunk Enterprise Security), EDR (CrowdStrike Falcon), and Email Security (Proofpoint) to detect phishing, malware, endpoint, and network-based threats in a 24/7 SOC environment.

- Performed incident triage, log analysis, and evidence collection, ensuring accurate validation and timely escalation to L2/L3 in line with SLA commitments.
- Investigated and contained phishing campaigns by quarantining emails, blocking malicious domains/URLs, and raising end-user awareness through phishing simulations and security advisories.
- Managed the incident lifecycle using ServiceNow, maintaining accurate case records, escalations, and closure compliance with SOC policies.
- Enhanced SIEM efficiency by recommending rule tuning, correlation rule creation, and log source integration, leading to improved detection coverage and reduced false positives.
- Generated weekly threat intelligence and incident trend reports, highlighting recurring attack vectors, KPIs, and emerging Tactics, Techniques, and Procedures (TTPs) for management visibility.
- Documented and maintained SOPs, incident response playbooks, and knowledge base articles for repeatable use cases, improving SOC knowledge management and onboarding efficiency.
- Conducted daily health checks on Splunk instances, ensuring consistent log ingestion, correlation, and monitoring visibility.
- Delivered end-user phishing and social engineering awareness sessions, contributing to stronger security culture and reduced click rates on malicious emails.

TECHNICAL SKILLS:

• SIEM:	Splunk Enterprise Security, IBM QRadar (basic)
• EDR:	CrowdStrike Falcon
• Email Security:	Proof point ((phishing detection & response)
• Ticketing:	ServiceNow, JIRA
• Threat Intelligence & Analysis:	VirusTotal, AlienVault OTX, IPVoid, MITRE ATT&CK framework
• Operating Systems:	Windows, Linux
• Networking& Security:	Firewalls, IDS/IPS, TCP/IP, DNS, Web Proxy, VPN
• Frameworks& Compliance:	NIST CSF, ISO 27001, CIS Controls, GDPR (basic)

CERTIFICATIONS:

- ISC2 Certified in Cybersecurity (CC)
- Splunk Core Certified User (In Progress)

ACADEMIC OVERVIEW:

- B.E. (IT) – Muffakham Jah College of Engineering and Technology, 2021
- Intermediate – Sri Chaitanya IIT Academy, 2013
- AISSE (10th) – Jawahar Navodaya Vidyalaya, 2011