Nasir Ahmed

☎ +91-9572663528

Bengaluru, India

nasirahmed11198@gmail.com

https://www.linkedin.com/in/nasir-ahmed-a69038201

PROFILE

Experienced SOC Analyst with 3.7 years of expertise in cybersecurity, specializing in Security Information and Event Management (SIEM) tools such as IBM QRadar, AIsaac (in-house), and ArcSight. Skilled in monitoring, analysing, and responding to security incidents, ensuring the protection of enterprise networks and assets. Strong analytical and problem-solving skills with a proactive approach to threat detection and mitigation.

EDUCATION

Bachelor Of Science in Information Technology

Karim City College, Jamshedpur
October 2020

KEY SKILLS

- Security Operations Centre & Incident Response
- SIEM & EDR Solutions
- Active Directory (AD) Management
- Email Security & Phishing Detection
- Cyber Risk Assessment & Mitigation
- Power BI Dashboard & Report Development
- Security Policy & Compliance
- Log Analysis & Network Traffic Monitoring
- MITRE Framework Expertise
- Technical Training & Leadership

Certification:

- AWS Security: Monitoring and Alerting
- AWS Security: Encryption Fundamentals
- Microsoft: Analyze query results using KQL

Languages

PROFESSIONAL EXPERIENCE

Security Analyst – SOC Analyst
Atos India PVT LTD, Bangalore, India
February 2021 – September 2024

- Creating and managing alerts using in-house built MDR tool, and other SIEM tools such as Qradar and ArcSight to detect potential threats and vulnerabilities.
- Investigated security incidents, performed root cause analysis, and implemented corrective actions.
- Provided real-time threat intelligence and escalation of critical security events to mitigate risks.
- Created and fine-tuned SIEM use cases and correlation rules to improve threat detection accuracy.
- Conduct cyber risk assessments and develop mitigation strategies.
- Identify risks related to confidentiality, integrity, and availability; assign risk ownership.
- Generate detailed reports, dashboards, and fine-tune detection rules.
- Recognize and respond to intrusion attempts through event analysis.
- Monitor AWS VPC threats and correlate logs with other AWS component's logs like WAF and ELB/ALB.
- Analyse alerts from network security tools, identifying true and false positives.
- Provide training to team members and communicate with clients via email, calls, and meetings.
- Prepare daily shift reports and assist with client security requirements.
- Manage UBA/UEBA threats, blacklist/whitelist IPs, URLs, and User Agents.
- Lead anti-fraud initiatives, including phishing campaign management.
- Utilize Power BI to create and maintain automated dashboard reports for incident tracking.

Knowledge of Key Security Concepts

- Extensive knowledge in Anatomy of an Attack and APT attack process.
- Wide exposure in various attacks like Application Layer Attacks (HTTP, FTP, SNMP, DNS, Malwares and SQL injections, Cross Site Scripting), Network layer attacks (DOS/DDOS, IP & MAC address Spoofing, ARP Poisoning), SSL/TLS attacks.
- Good understanding of MITRE Framework and knowledge of correlation of attacks with MITRE.
- Good knowledge of OSI layers and clear understanding of protocols functioning at each layer.

Projects & Achievements

Hindi	First Language
English	Advanced C1

- Developed and optimized SIEM rules to reduce false positives and improve detection capabilities.
- Led a security awareness initiative to enhance organizational cybersecurity posture.
- Assisted in forensic investigations and incident handling for high-priority security events.