Mohammad Haneef Khan

✉ haneefmk09@gmail.com 📞 +91- 9030309043 LinkedIn: https://www.linkedin.com/in/haneef-khan

PROFESSIONAL SUMMARY

Cybersecurity professional with 3.5 years of experience as a Security SOC Analyst, specializing in incident response, threat hunting, and malware analysis. Proficient in leveraging SIEM tools, SOAR platforms, SOC automation, and EDR solutions to monitor, detect, and mitigate cybersecurity threats. Skilled in managing critical incidents, automating workflows, and fine-tuning SIEM detection rules to reduce false positives. Strong foundation in cybersecurity frameworks, cloud security, phishing analysis, and Threat Intelligence Platforms (TIPs). Passionate about continuous learning and process optimization.

Key Skills

- **Threat Detection & Analysis:** Incident management, phishing analysis, malware analysis, root cause analysis. Threat Intelligence Platforms (TIPs).
- **SIEM and SOAR Tools:** Microsoft Azure Sentinel, IBM QRadar, Splunk and AISaac.
- **EDR Solutions:** Microsoft Defender, CrowdStrike, Carbon Black.
- **Threat Hunting & Intelligence:** KQL, MITRE ATT&CK framework, IOC/IOA analysis.
- **Cloud & Network Security:** Azure Security Centre. Palo Alto Firewalls, Fortinet VPN, IDS/IPS.
- **Networking & Cybersecurity Frameworks**: MITRE ATT&CK, Lockheed Martin Cyber Kill Chain, NIST, OWASP.
- **Technical Proficiency**: Packet analysis, DLP, Web Application Security, Email Security, Snort, SLA, ServiceNow.

PROFESSIONAL EXPERIENCE

Security SOC Analyst: TCS | Bangalore, India **May 2023 – Present**

- Monitored, analyzed, and responded to 300+ security alerts monthly using SIEM tools such as QRadar and Azure Sentinel.
- Reduced false positives by 30% through fine-tuning detection rules and implementing automated alert correlation.
- Conducted threat detection and incident triage, analyzing the nature of incidents, containing their impact, and implementing remediation measures.
- Coordinated with cross-functional teams and system administrators to ensure a coordinated response to security incidents.
- Conducted in-depth phishing and malware analysis, reducing response time by 25%.
- Performed advanced threat hunting using KQL queries and rules, identifying persistent threats.
- Monitored and analyzed emails for threats and malware, recommending email rules to minimize malicious or undesirable emails.
- Proactively hunted for signs of compromise using threat intelligence and behavioral analytics tools.
- Handled security alerts, IOC management, exceptions, device control, host management, threat intelligence, and sandbox analysis using EDR solutions.
- Collaborated with the Incident Response team to handle critical security incidents, ensuring timely containment and remediation.
- Compiled detailed shift reports documenting ongoing activities, incident statuses, and relevant information for shift handover.
- Documented incident response processes and created playbooks for SOAR platform integration.

Associate Consultant: CAPGEMINI | Bangalore, India **Nov 2022 -Apr 2023**

- Investigated potential threats using Microsoft Defender ATP to identify anomalies and mitigate risks.
- Stayed updated on the latest security threats, vulnerabilities, and attack techniques, researching emerging threats and developing countermeasures.
- Collaborated with threat intelligence teams and utilized external sources to enhance the organization's threat detection capabilities.
- Designed and implemented custom detection rules aligned with the MITRE framework.

- Delivered weekly reports on SOC performance metrics to stakeholders.
- Performed cyber threat intelligence operations, including IOC collection, tracking threat actors, and monitoring malicious infrastructure.
- Continuously monitoring security events and alerts to identify potential indicators of compromise.
- Conducted in-depth analysis of security logs, network traffic, and system data to identify potential breaches.

Assistant Engineer: ATOS | Bangalore, India **Nov 2021 –Nov 2022**

- Operated in a 24x7 SOC environment, responding to incidents and performing monitoring activities.
- Enhanced SOC efficiency by optimizing security alerts in a 24x7 environment.
- Responded to security incidents promptly, following established protocols to mitigate threats.
- Orchestrated cybersecurity tools like Alert Logic, Email Gateway Protection, and Proxy Solutions.
- Developed incident response workflows for DLP incidents.
- Familiar with frameworks like MITRE ATT&CK, and Lockheed Martin Cyber Kill Chain.

Projects

- SOAR Implementation & Automation: Developed playbook-driven automation, reducing average incident response time by 20%.
- Conducted Advanced Threat Hunting: Conducted real-time log monitoring and Increased threat detection by 25% through enhanced log correlation for Firewalls, Office 365, and Microsoft Defender.
- Designed and maintained MIS reports (daily, weekly, monthly) to track alerts, user activity, and threat observations.

EDUCATION

JNTU Anantapur
Bachelors of Technology (B. Tech) in Engineering - 76% GPA

Technical SKILLS

- Microsoft Azure
- Risk Assessment
- Risk Management
- Incident Response
- Client relations
- OSI and OWASP
- EDR and XDR
- Palo Alto Firewall
- Cloud Security
- Network Security
- MS Excel
- Email Security
- Threat Modules
- KQL and SOAR
- WAF
- VAPT, IOC and IOA
- MITRE ATT&CK
- Phishing and Malware Analysis
- Threat Hunting and Intelligence
- Security Incident Management
- Web Application Security
- Qradar, Carbon Black
- DLP - Forcepoint
- SLA, Snow

CERTIFICATIONS

- Certified Cloud Security – Simplilearn
- Certified Cryptography – Simplilearn
- Certified CISSP Security Assessment & Testing and Security Operations
- Ethical Hacking Certificate – Simplilearn
- Fortinet NSE 1 and NSE 2
- Digital Security Fundamentals Certificate

Additional Information

- Strong analytical and problem-solving skills with a focus on continuous improvement.
- Excellent communication and collaboration skills, with experience working in cross-functional teams.
- Proficient in Microsoft Excel and other reporting tools.