Mohammed k

SOC Analyst

Address: Ernakulam, India
Phone: +91 7736762947
Email: mohammedbilal.k313@gmail.com
LinkedIn: LinkedIn Profile

PROFESSIONAL SUMMARY

Results-driven SOC Analyst with over one year of experience in monitoring, detecting, investigating, and mitigating security threats. Proven ability to reduce incident response time, enhance SOC tooling, and improve security operations. Skilled in SIEM, endpoint security, network security, and digital forensics. Strong understanding of MITRE ATT&CK, Cyber Kill Chain, threat hunting, and vulnerability assessments. Passionate about proactive security monitoring, automation, and continuous learning.

EXPERIENCE

SOC Analyst - Soffit, Ernakulam

December 2023 - Present

- Monitored security alerts from tools like SIEM, IDS/IPS, and endpoint protection systems.
- Investigated incidents, identified root causes, and implemented remediation steps.
- Monitored, detected, and responded to cybersecurity incidents in a 24x7 environment.
- Responded to incidents reported through various channels (email, calls, etc.).
- Collected logs for incident containment and investigation.
- Escalated confirmed incidents and performed preliminary analysis.
- Interpreted logs from sources like Firewalls, IDS, Windows DC, Cisco appliances.
- Reported alarms triggered or threats detected via ITSM Platforms.
- Managed client requests and changes through ticketing systems.

Penetration Tester Intern - Red Team, Malappuram

September 2023 - November 2023

- Conducted penetration testing on web applications and network infrastructures.
- Utilized tools like Nessus, OpenVAS, Burp Suite, Nmap, and Metasploit.
- Documented vulnerabilities and provided risk mitigation strategies.
- Assisted in reverse engineering malware and analyzing attack patterns.
- Conducted social engineering assessments to test security awareness.

SKILLS

Technical Skills:

- Security Operations & Incident Response
- Threat Analysis & Investigation
- Log Analysis & Event Correlation
- Network Traffic & Packet Analysis
- Malware Analysis & Threat Intelligence
- Vulnerability Detection & Exploit Analysis
- SIEM & Endpoint Security Solutions (Splunk, Wazuh)
- Network & Endpoint Security (Firewalls, IDS/IPS, EDR)
- Penetration Testing Tools (Nessus, OpenVAS, Burp Suite, Metasploit, Wireshark)
- OSINT Tools (theHarvester, Shodan, Recon-ng, Google Dorking)
- Forensic Analysis Tools (Ghidra, Volatility)

Security Frameworks & Compliance:

- MITRE ATT&CK, Cyber Kill Chain, ISO 27001

Soft Skills:

- Analytical Thinking, Communication, Collaboration, Problem-Solving, Attention to Detail

CERTIFICATIONS

- Certified Ethical Hacker (CEH)
- TATA Cybersecurity Internship Certificate
- CCNA (Cisco Certified Network Associate) - Completion

EDUCATION

- Bachelor's Degree in Computer Science (BCA) — SNGU Kerala
- Diploma in Cybersecurity — Red Team Academy

PROJECTS

SOC Analyst Technical Assessment

- Description: Simulated real-world SOC operations, focusing on security monitoring, log analysis, and incident response.
- Responsibilities:
  - Analyzed SIEM alerts, prioritized threats, and recommended containment actions.
  - Correlated logs and mapped attacks using the MITRE ATT&CK framework.
  - Responded to ransomware incidents, identifying IOCs and proposing remediation steps.
  - Prepared executive summaries with findings and actionable recommendations.
- Tools: SIEM, IDS/IPS, MITRE ATT&CK, Log Analysis Tools.
- Link: Project Link