MOHAMMED TAWHEED

+91-9980412233 | mohammedtawheed9317@outlook.com | LinkedIn | GitHub

SUMMARY

SOC Analyst with 1.5+ years of hands-on experience (plus 1 year cybersecurity internship) in SOC operations, SIEM monitoring, alert triage, threat detection, and incident response. Experienced analyzing events across Splunk, QRadar, firewalls, EDR, IDS/IPS, Windows Event Logs, and network traffic. Skilled in IOC analysis, MITRE ATT&CK mapping, threat intelligence checks, evidence documentation, and Python-based detection automation for Blue Team workflows.

KEY ACHIEVEMENTS

- **Reduced false-positive escalations by 20%** through improved alert triage and validation across Splunk and QRadar, while consistently handling 20-30 alerts/day.
- **Maintained SLA adherence above 95%** across P1-P3 incidents, ensuring timely escalation and response in a live SOC environment.
- **Cut average phishing investigation time by ~20%** by applying Python-based automation (from self-built SOAR and detection projects) to accelerate IOC lookups and evidence documentation.

SKILLS

SOC & SIEM: Splunk, QRadar, Security Onion, SOC Operations, Cyber Defense Center Support, SIEM Monitoring, Alert Triage, Incident Response, Security Monitoring, Security Reporting

Detection & Log Analysis: Windows Event Logs, Firewall Logs, EDR Alerts, IDS/IPS Alerts, Authentication Logs, Packet Analysis, IOC Analysis, Threat Detection, Basic Threat Hunting

Security Investigations: Phishing Investigation, Malicious URL Analysis, Incident Handling, Severity Classification, Evidence Documentation, Escalation, Basic Digital Forensics

Network & Vulnerability Security: Wireshark, Nessus, TCP/IP, DNS, VPN, Firewalls, IDS/IPS, Vulnerability Assessment, Risk Assessment

Scripting & Frameworks: Python, Bash, PowerShell, MITRE ATT&CK

CERTIFICATIONS

- **EC-Council Certified SOC Analyst (CSA)** - ECC8120457369
- **EC-Council Certified Ethical Hacker (CEH)** - ECC0562384197
- **Splunk Core Certified User**

EXPERIENCE

SOC Analyst L1 | HashSlash ***February 2024 - Present***

- Triaged 10-20 SIEM alerts/day across Splunk and QRadar, validating events and escalating confirmed incidents per SOC workflows while reducing false positives by 20%.
- Maintained SLA adherence above 95% across P1-P3 incidents by monitoring firewall, EDR, IDS/IPS, endpoint, server, authentication, and network traffic logs for suspicious activity and IOCs.
- Investigated 5-10 phishing and malicious URL cases/month plus brute-force and suspicious login alerts, documenting evidence, severity, impact, and recommended response actions.
- Mapped 10+ MITRE ATT&CK techniques across investigations and built Python-based automation for Blue Team workflows, cutting average phishing investigation time by ~30%.

Cybersecurity Intern | AndyInfosec ***January 2023 - January 2024***

- Supported SIEM monitoring, alert validation, incident response, phishing analysis, and vulnerability assessment using standard security tools.
- Performed threat analysis on 10+ cases/month using authentication logs, firewall events, and packet captures; prepared incident notes and security reports with senior analysts.

PROJECTS

SOC Log-Based Threat Detection System | Python | GitHub

- Built Python automation to detect brute-force login patterns and generate analyst-ready alerts mapped to MITRE ATT&CK.

Automated SOAR Incident Response System with MITRE ATT&CK | Python | GitHub

- Built an automated incident response workflow for IP blocking, host isolation simulation, MITRE context, and structured reporting.

SIEM AI Agent | Security Dashboard

- Created a dashboard workflow to ingest security events, generate alerts, score risk, enrich alerts with MITRE ATT&CK context, and support SOC triage.

EDUCATION

Bachelor of Engineering, Computer Science Engineering | BMS Institute of Technology & Management | Bengaluru, India