

# MOHAMMAD HANEEF ALI

Associate SOC Analyst | 24/7 Monitoring | Incident Response

[Haneefali5352@gmail.com](mailto:Haneefali5352@gmail.com) | +91 8341415384 | Hyderabad – 500021

[linkedin.com/in/haneef-ali-mohammad-467343288/](https://www.linkedin.com/in/haneef-ali-mohammad-467343288/)

---

## EXPERIENCE

---

### Associate SOC Analyst Training | HYD | 2024 - 2025

#### Cartel Software Pvt Ltd

- Proficient in using Security Information and Event Management (SIEM) tools such as Splunk and QRadar for real-time monitoring and analysis, achieving a 25% improvement in incident response time.
- Developed a strong understanding of firewall configurations and IDS/IPS functionality; used the Sort tool to identify malicious network activity and established custom rules to improve detection and block harmful traffic.
- Detected and responded to 50+ demo alerts, resolving issues and escalating incidents to L2; alerts included phishing, DDoS, malicious IPs, and suspicious traffic.
- Conducted vulnerability assessments and monitored network traffic using Wireshark, identifying 10+ misconfigurations and threats, and initiated correlation rules that enabled key fixes and improved system integrity

## SKILLS

---

- SIEM
- Qradar, Splunk, Wazuh
- EDR
- Crowd Strike, Sentinel One, Defender
- Networking, VPN
- IDS/IPS
- HTTPS, SMTP, SSH, FTP, DNS
- Incident Response
- SLA
- SOC
- Malware, Phishing, Brute force
- Communication, Attention to detail
- Log analysis
- Log correlation
- Incident response life cycle
- Firewall
- MITRE ATT&CK
- Wire Shark, Burp Suite
- OSINT
- Jira
- VMware
- Alert monitoring

## ACADEMICPROJECTS

---

### Log Correlation | Threat Detection Lab | Splunk, Wazuh, MITER ATT&CK, Sentinel One

- Correlated logs from firewalls, IDS/IPS, EDR, and authentication sources to detect multi-stage attacks (Nmap scans, brute-force logins, and suspicious DNS requests).
- Identified attacker IPs performing reconnaissance and blocked them at the firewall, then verified results using Wazuh and Splunk alerts.
- Mapped malicious activity to MITRE ATT&CK techniques (T1046, T1110, T1071) and documented the complete attack chain.
- Prepared structured incident reports with timelines, IOCs, and remediation steps, and simulated escalation to L2 analysis using Jira.

### Wazuh & Splunk Aggregation | Linux, Ubuntu, Wazuh, Bash, Splunk, Windows

- Built a real-world SOC lab environment with Windows and Linux VMs.
- Integrated Wazuh agents with Splunk for centralized log aggregation and monitoring.
- Configured File Integrity Monitoring (FIM) and created correlation rules to detect threats.
- Staged attacks, detected and escalated 20+ true-positive alerts, and reduced false positives through rule tuning.

# EDUCATION

---

Kakatiya University, Warangal, Telangana — B.Com. in Computer Applications, 2024

Telangana State Board of Intermediate — MPC, 2020

# CERTIFICATION

---

## **CERTIFIED ETHICAL HACKER (CEH) – EC COUNCIL**

Hands-on experience identifying and exploiting vulnerabilities using Burp Suite, Nmap, and Wireshark, while adhering to the OWASP Top 10 and MITRE ATT&CK frameworks.

## **CERTIFIED SOC ANALYST (CSA) – EC COUNCIL**

Hands-on experience with SIEM tools such as QRadar and Splunk for log analysis, EDR, XDR, IDS/IPS, Firewall, Incident response, and threat detection.