# Mohammad Ashraf

8766738319 | K.asrf001@gmail.com | Mumbai, India

## Profile Summary

I'm a results-oriented SOC Analyst with 2+ years of experience in monitoring, analyzing, and responding to security incidents. I have hands-on experience with top tools like SIEM, IDS/IPS, firewalls, Ticketing Tools, EDR, Jira, and web proxies to detect and mitigate cyber threats. I specialize in conducting thorough investigations, implementing security measures, and working with cross-functional teams to strengthen organizational defenses. Collaboration is key to my approach, as I work closely with fellow security professionals to improve the overall security posture. I'm committed to staying updated on new security trends and ensuring the integrity of networks and systems. I'm now looking to bring my skills and experience to a challenging SOC Analyst role in a dynamic cybersecurity team.

## Professional Experience

**Capgemini, India**
*SOC ANALYST L1* *February 2023 - Present*

- Monitor and investigate security events, using tools to identify false positives or real incidents, and detect potential intrusions or compromises.
- Analyze suspicious emails, provide feedback to users, and investigate threat intelligence feeds to identify Indicators of Compromise (IOCs)
- Track and manage security incidents in Jira, ensuring proper documentation, timely escalation, and facilitating team collaboration during active events.
- Monitored Microsoft Sentinel for security alerts and potential threats, escalating high-priority incidents to senior SOC analysts for further investigation.
- Assisted with the initial investigation of alerts in Microsoft Sentinel, using built-in queries to identify potential threats and provide data for incident response.
- Managed and reviewed Indicators of Compromise (IOCs), collaborating with vendors or internal teams to enhance detection coverage.
- Developed SOC monitoring use cases to proactively detect emerging threats and fine-tuned SIEM rules to minimize false positives and eliminate false negatives.
- Updated the incident response playbook to ensure effective cybersecurity readiness and monitored the health of security sensors and SIEM infrastructure.
- Analyzed security data using Microsoft Sentinel and CrowdStrike Falcon, identifying anomalous behavior and escalating potential threats for timely response.
- Delivered concise SOC reports to senior management, summarizing current security status, recent incidents, threat trends, and the effectiveness of security controls.

### Key Highlights

- Leadership and team management.
- Proactively detected threats through continuous event monitoring & Triage.
- Monitored events from various sources for comprehensive threat analysis.
- Responded swiftly to suspicious emails to enhancing security measures.
- Contributed to maintaining a 24x7 security operations centre for continuous vigilance.
- Monitored team performance against SLA targets and led post- incident debriefs to identify improvements, ensuring faster resolution and consistent SLA and MTTR compliance.

## Technical Skills

**SIEM**: Azure Sentinel, IBM Qradar
**EDR**: Crowdstrike, Microsoft Defender
**Ticketing Tools** : Jira, ServiceNow, CONA
**Threat Intelligence Tools** : OpenCTI, IBM X-Force, Virus Total, AbuseIPDB
**Others**: Centreon, Excel, Zscaler

## Education

**D. Y. Patil College of Engineering**

*BE in Information Tecnology*

**M. H. Saboo Siddik Polytechnic**

*Diploma in Computer Engineering*

## Certifications

**SC-200**: Microsoft Certified: Security Operations Analyst Associate
**AZ-500**: Microsoft Certified: Azure Security Engineer Associate
**AI-900**: Microsoft Certified: Azure AI Fundamentals