

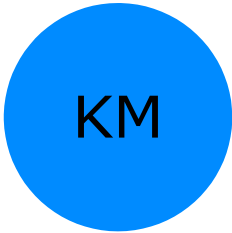
KHALID MULLA

CYBER SECURITY ANALYST

+91-9730855634

@kmulla1772@gmail.com

A/P-Bhalavani Tal-Khanapur Dist-Sangli, 415311



SUMMARY

I am a results-oriented cyber security professional with over 2.9 years of hands-on experience in Security Operations Center (SOC) operations, incident response, and threat mitigation. I am proficient in advanced security tools, optimizing SOC workflows, and conducting gap assessments. I excel at ensuring robust organizational security postures through strategic planning and operational excellence.

EXPERIENCE

Senior System Engineer |SOC L1 Analyst

Infosys Ltd.

05/2022 - Present

Pune, India

A leading global technology services company.

Utilized tools like IBM QRadar and Sentinel to monitor network traffic, identify vulnerabilities, and track potential threat actors.

Investigated incidents to differentiate false positives from true positives and escalated critical issues.

Developed custom use cases and maintained regulatory compliance.

Provided actionable threat intelligence to senior management, enhancing organizational decision-making.

Conducted regular gap analysis to refine security controls and strategies.

Monitored and responded to security incidents using SIEM platforms across diverse log sources including firewalls, DNS, DHCP, and proxy servers.

Led incident response efforts through containment, eradication, recovery, and post-incident analysis.

Conducted advanced threat hunting to identify Indicators of Compromise (IOCs) and proactively mitigate risks.

Automated security workflows by developing and fine-tuning use-cases, rules, and building blocks for cloud platforms like AWS.

Prepared daily incident reports and monthly summaries for stakeholders, incorporating actionable insights.

Collaborated with cross-functional teams to improve processes and implemented industry-standard operating procedures.

EDUCATION

B.Tech

D.BATU Raigad

08/2015-08/2021

Sangli

Diploma

MSBTE Mumbai

08/2014 - 06/2017

Solapur

SSC | 10th

Rayat Sikshan Sanstha

05/2013 - 04/2014

Bhalavani

KEY ACHIEVEMENTS

Enhanced Response Efficiency

Increased incident response efficiency by 30% with new automation scripts.

Reduced False Positives

Led team to reduce false positive alerts by 25% in six months.

Accelerated Threat Detection

Improved SOC process with 40% faster threat detection time.

Led Security Training

Conducted 30+ security training sessions, boosting awareness by 45%.

STRENGTHS

Professional Skills

Teamwork, Project Management, Time Management, Leadership, Effective Communication, Critical Thinking

LANGUAGES

English

Native

Hindi

Native

Marathi

Native

SKILLS

AWS

Cyber security

DHCP

DNS

EDR

firewalls

Nmap

Proxy

QRadar

Qualys

SIEM

Security Operations

Standard Operating Procedures

Threat Hunting

Threat Intelligence