Nikhil Dhoble
Technology analyst – SOC Analyst
Hinjewadi Phase 2, Pune 411057
Language: English, Hindi, Marathi

Email: nikhildhoble13307@gmail.com
Phone: +91 8180997823
www.linkedin.com/in/nikhil-dhoble-b61b09193/

SUMMARY

Experienced SOC analyst with 3.8 years of expertise in securing enterprise environments. My proficiency in SIEM tools like **Azure Sentinel** and **IBM QRadar,** along with endpoint security solutions such as **Microsoft Defender** and **CrowdStrike Falcon**, enables me to effectively detect, Investigate, and respond to threats. I excel at streamlining workflows through automation platforms like **Cortex XSOAR** and integrating ticketing Systems like **ServiceNow** and **JIRA** to enhance security workflows.

EXPERIENCE

Infosys Ltd. June 2021 – Present

MSS Projects - L2 SOC Analyst (Jan 2025 – Present)

- Worked on SIEM tools like IBM QRadar and Azure Sentinel.
- Worked on EDR tools like Microsoft Defender and CrowdStrike Falcon.
- Performed in depth analysis and provided impactful mitigation on that basis.
- Worked on fine-tuning security use cases to optimize threat detection and reduce false positives.
- Backtracing for IOC.
- Created multiple security related SOPs and having basic knowledge of usecase creation.
- Reference Sets for Whitelisting/Blacklisting entities.
- Worked on ticketing tools ServiceNow and JIRA.
- Effectively communicated with clients on a weekly basis to discuss and present Weekly Security Reports (WSR) and Monthly Security Reports (MSR).
- Managed and mentored L1 team members, providing guidance and clearing doubts.

MSS Projects - L1 SOC Analyst (June 2021 – Jan 2025)

- Real-time monitoring, identification, analysis and resolution of security alerts detected by Azure Sentinel, IBM QRadar, Microsoft Defender, & CrowdStrike Falcon
- Managed reports like Daily Activity Report, Daily Log Source Reports, and Critical Logs Report.
- Good knowledge about URL, IP, Hashes, and Domain Reputation checking in depth analysis of security alerts generated.
- Managed a team of 35+ L1 analysts, optimizing a 24/7 monitoring roster to provide continuous security support for 8 clients, resulting in improved incident resolution times and compliance with SLAs.
- Conducted security assessment, risk analysis, and root cause analysis of security incident.
- Utilized ServiceNow tool for creating tickets and diligently followed up on them for timely resolution.
- Worked in flexible hours-rotational shifts, weekends, and holiday shifts.

SKILLS

- SIEM tools: Azure Sentinel and IBM QRadar
- EDR tools: Microsoft Defender and CrowdStrike Falcon
- Automation: Palo Alto Cortex XSOAR
- Ticketing Systems: ServiceNow, JIRA
- Programming and Scripting: KQL
- Networking: Network Security, Protocols Analysis, MITRE ATT&CK, Cyber Kill Chain, OSI Model, TCP/IP Model
- Threat Intelligence: IPVoid, VirusTotal, AbuseIPDB, MxToolbox, URL Scan
- Incident Response Management
- Log Integration, Log Monitoring & Log Analysis
- Proactive threat hunting
- Security operations monitoring
- Security response and remediation
- Detecting Phishing Emails
- Sandboxing Tool: Any. Run, Browserling, URLScan
- Vulnerability Assessment
- Maintaining SLAs
- Knowledge of Firewall, IDS/IPS
- MITRE ATT&CK Framework

EDUCATION:

- **Bachelor of Technology (IT)**
  DKTE, Ichalkarnaji, Maharashtra 2016-2020
- **Diploma in computer engineering**
  Government Polytechnic, Miraj 2013-2016

CERTIFICATION:

- Applied Cybersecurity Essentials, Purdue University 2021
  1) Cybersecurity Foundations
  2) Vulnerability Management
  3) Enterprise Security
  4) Ethical Hacking
- SC-200: Microsoft Security Operations Analyst – Infosys
- Certified QRadar Analyst - SIEM Intelligence
- IBM QRadar SOC Analyst – Infosys
- Certified Ethical Hacker Certification Guide – Infosys
- SOC Incident handling response L1 mitigation – Infosys

ACCOMPLISHMENT:

- Received Appreciation and Infosys Insta Award - Feb 2024.