Devarapu Suneel

E-mail: suneel.devarapu28@gmail.com
Mobile: +91 7032418061

Experience Summary

Experienced Security Operations Center (SOC) Analyst with over 3 years of hands-on experience in monitoring, detecting, and responding to cybersecurity threats within 24/7 operational environments. Proficient in leading SIEM platforms including LogRhythm, IBM QRadar, Microsoft Defender, and Microsoft Sentinel. Skilled in incident detection, analysis, triage, escalation, phishing investigations, use case development, and SLA-driven incident handling.

Professional Experience

- ➢ Working as a Security Analyst for **IBM India Pvt Limited**, Bangalore from August 2022 to till date.

Responsibilities

- ➢ Monitored security events using SIEM tools LogRhythm, IBM QRadar, Microsoft Defender, and Microsoft Sentinel to enable real-time threat detection and ensure timely response to vulnerabilities.
- ➢ Investigated and responded to a wide range of cyber threats, including malware outbreaks, Distributed Denial-of-Service (DDoS) attacks, brute-force attempts, and OWASP Top 10 vulnerabilities.
- ➢ Performed deep-dive log analysis on critical alerts and generated comprehensive incident reports to support effective remediation.
- ➢ Conducted phishing email investigations, identified Indicators of Compromise (IoCs), and provided appropriate remediation guidance.
- ➢ Created and managed lists, saved searches, and watchlists in LogRhythm to streamline threat detection and enhance monitoring efficiency.
- ➢ Revoked user sessions and performed password resets in Microsoft Defender during investigations to mitigate threats and prevent unauthorized access.
- ➢ Blocked malicious indicators including file hashes, IP addresses, and URLs within Microsoft Defender to prevent further security threats.
- ➢ Created and managed incidents in ServiceNow, ensuring SLA compliance and maintaining accurate and complete documentation.
- ➢ Prepared and presented weekly reports to customers, highlighting recurring security issues, emerging trends, and delivering actionable tuning recommendations to improve overall security posture and operational efficiency.
- ➢ Experience on Azure Entra ID for checking Sign-in Logs, Audit Logs, Groups, Devices etc.
- ➢ Good understanding of KQL - Kusto Query Language that can be used to create alerts.

Academic Profile

- **B.Tech** in Electronics and Communication Engineering, Eswar College of Engineering, JNTUK, Andhra Pradesh (2021) — CGPA: 6.75

Technical Skills

SIEM Tools	: LogRhythm, IBM QRadar, Microsoft Sentinel
EDR	: CrowdStrike, Microsoft Defender for Endpoint
Email Security	: Microsoft Defender for Office 365
Ticketing Tools	: ServiceNow
Analysis Tools	: Any.Run, OSINT tools
Vulnerability Scanners	: Nessus, Microsoft Defender Vulnerability Management
Networking	: Switches, Routers, IPS, Firewalls, LAN, WAN

Core Competencies

- Incident Response & Escalation
- Malware & Phishing Analysis
- Intrusion Detection & Prevention (IDS/IPS)
- Endpoint Detection & Response (EDR)
- Log Analysis & Correlation
- Azure Entra ID
- Network Security Monitoring
- Knowledge of networking protocols: TCP/IP, HTTP/HTTPs, FTP, IRC, RPC, DNS, etc
- Threat Intelligence
- Firewall Management
- Knowledge of the MITRE ATT&CK Framework
- Vulnerability Management

Declaration:

I hereby declare that the above-mentioned information is true to the best of my knowledge and I take full responsibility for its accuracy.

Sincerely,

(Devarapu Suneel)