MANIKANTESHWAR REDDY GANGULA

EXPERIENCE – 2.3 YEARS OVERALL

SOC ANALYST

CONTACT

+91 7075068200

manikanteshwarreddy1@gmail.com

EXPERIENCE

- SOC Analyst at Tata Consultancy services since February 2023.

EDUCATION

Post-Graduation:

-UOH, London - Jan 2021 – Jan 2023

Graduation:

-JNTUH

-2014 – 2018

CERTIFICATIONS:

- SC 200 Certified

-CEH Trained

PROFILE

- Resourceful Information Security Professional with 2.6 Years of experience in IT Security operations with broad exposure on infrastructure/Network/IT security tools, security incident response and operations.

TOOLS & TECHNOLOGY

SIEM	Azure Sentinel, Splunk, ArcSight
EDR	MS Defender, Crowd strike (Falcon)
Web Application Firewall	Akamai
IDS/IPS	McAfee
Firewall	Palo Alto
DLP	Netskope
Phishing	Proof point Email Gateway
Ticketing Tool	BMC Helix (Genie) , Service Now
Vulnerability Assessment tool	Tenable Nessus

.

CORE QUALIFICATIONS AS A SECURITY ANALYST:

- Worked in SOC Team (Security Operations Center) Monitor and analyze various security alerts and incidents and report suspicious/malicious activity to a higher level.
- Experience working with EDR tool Crowd strike Falcon and MS Defender.
- Hands-On experience using Sentinel working on use cases and managing dashboards.
- Monitoring, detection of analysis through various input tools and systems (SIEM, IDS / IPS, Firewalls, AV, etc), through incident handling and incident response.
- Identified the phishing and spam emails and taken necessary actions.
- Conducted the phishing assessments and given reports to the respective teams
- Responding to alerts from the various monitoring/detection systems and platforms within defined SLAs.
- Following detailed processes and procedures to analyze, respond to and/or escalate cyber security incidents.
- Experience on working with Tenable Nessus VA tool and working on vulnerability scans and reports.
- Follow SOC Playbooks and escalation matrix
- Understanding of MITRE's Attack Framework
- Generate customer facing security reports like working on weekly and monthly reports.
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences.
- Good knowledge of common network protocols such as TCP, UDP, DNS, DHCP, IPSEC, HTTP, etc. and network protocol analysis suites.
- Knowledge on the fundamentals of Windows and Unix systems.
- Documentation of the Process/Procedures/Technology & contributing to the drafts/reviews of SOP's

OTHER TECHNOLOGIES:

- Functional knowledge of 3rd party cloud computing platform Azure & Azure Active Directory
- Familiar with Cybersecurity frameworks, such as MITRE ATT&CK, OWASP, NIST
- Understanding of SIEM Tool Azure Sentinel.
- Knowledge on TCP/IP & Network Fundamentals, Firewalls, IDS/IPS.
- Knowledge of network protocols and related technologies.
- Understanding of Threat Analysis, Network Event analysis.