Gudiwada, AP - 533437
(+91) - 9652886612
mandapaka.suresh1998@gmail.com

M. SURESH / SECURITY ANALYST

PROFESSIONAL SUMMARY

Dedicated and detail-oriented Security Analyst with **3.6 years** of hands-on experience in a **Security Operations Center (SOC)**, specializing in real-time monitoring, threat detection, and incident response. Proficient in using industry-leading SIEM tools such as **Splunk, QRadar, and Azure Sentinel** to analyze logs, detect anomalies, and mitigate security risks. Demonstrated expertise in vulnerability assessments using Qualys Guard and Nessus, as well as managing firewalls, IDS/IPS, and antivirus solutions. Adept at analyzing phishing attacks, and managing email and web security, with a proven track record of protecting enterprise environments. Strong collaborative skills with experience working in a Global Security Operations Center (GSOC) environment, handling security incidents across multiple clients. Committed to enhancing cybersecurity defenses through continuous threat hunting and process optimization.

EXPERINCE

Information Security Analyst | TCS | Bangalore - IND **Apr 2021 - Present**

Roles & Responsibilities:

- Working in the **Security Operation Centre** Monitor 24x7 for **P1, P2, and P3** alerts in SOC operations, **analyzing logs** from various security/industrial appliances using SIEM tools like **Splunk, QRadar, and Azure Sentinel**.
- Perform real-time **security monitoring, detection, and response** using SIEM tools **(Splunk, QRadar, and Azure Sentinel).**
- Investigate security alerts by analyzing **logs** and **network traffic** to identify **potential threats and vulnerabilities**.
- Collaborate with L2 and L3 to resolve **security breaches** and **mitigate risks** as part of our **incident response** efforts.
- Fill the **daily health checklist** and **create, modify**, and **update Security Information and Event Management (SIEM)** tools.
- Work within the **GSOC (Global Security Operations Center)**, managing multiple clients and their security environments.
- Perform in-depth analysis of suspicious activities across **firewalls, endpoints, web security, and email security**.
- Analyze **phishing emails** to identify risks and block malicious content.
- Conduct **cyber and technical threat analyses** to assess security posture and recommend corrective actions.
- Configure and manage firewalls such as **Checkpoint and Cisco Firepower, implementing security policies**.
- Ensure the proper functioning of **IDS/IPS systems, proxies,** and **VPNs** to safeguard network traffic.
- Monitor **networking protocols, primarily TCP/IP, to detect anomalies and security breaches**.

- Conduct regular vulnerability assessments using **Qualys Guard** and **Nessus** to identify and prioritize vulnerabilities.
- Administer and monitor antivirus solutions to **detect malware and prevent endpoint compromises**.
- Utilize endpoint detection and response tools such as **Carbon Black and Microsoft Defender** to secure endpoints.
- Oversee Office 365 security configurations and monitor for **phishing and malware attacks**.
- Manage web security tools to protect against **web-based threats**.
- Generate detailed reports on **security incidents, trends, and threat intelligence** for SOC management.
- Maintain documentation of **security processes, incident handling, and remediation efforts**.
- Collaborate with cross-functional teams to enhance **security monitoring** capabilities.
- Participate in **threat-hunting** exercises and contribute to improving **security response** strategies.

EDUCATION

B.Tech, EEE | GODAVARI INSTITUTE OF ENGINEERING AND TECHNOLOGY - Percentage – 50%
Duration: 2016 - 2020

TECHNICAL SKILLS

- SOC **(Security Operation Centre)**
- SIEM **(Security Information and Event Management)**: **Splunk, QRadar & Azure Sentinel**
- **Web Security, Email security O365**
- Vulnerability Assessment **(Qualys Guard & Nessus)**
- **Antivirus**
- **Phishing Email Analysis**
- firewall: **Checkpoint**
- Perform Cyber and Technical Threat Analyses
- All networking protocols (Primarily TCP/IP) Internet/Network Security skills - **firewalls, VPN, Azure Sentinel, (IDS, IPS, Cisco firepower) proxies, etc.**