CURRICULUM VITAE

NAVEEN.T

E-MAIL: tnaveen70977@gmail.com
MOBILE: +91 9441161287

PROFILE SUMMARY

I am an IT professional with over 4 years of experience as a Cybersecurity SOC Analyst. I am expertise in monitoring, analyzing, and responding to security events to protect enterprise systems. Proficient in threat intelligence, vulnerability assessment, and incident management to safeguard networks. As a Technical Support Officer, I delivered comprehensive support to resolve technical issues related to computers and networks, enhancing system performance for end users.

PROFILE SNAPSHOT

Skilled IT professional with a strong focus on malware detection, network security, and technical troubleshooting, dedicated to protecting and maintaining IT infrastructures. Proficient in utilizing SIEM (Security Information and Event Management) tools like Azure Sentinel, and EDR (Endpoint Detection and Response) solutions such as Microsoft Defender, with extensive experience securing email environments through Office 365. Knowledgeable in security frameworks like MITRE and the Cyber Kill Chain process, I am adept at providing L1 support and assisting L2 analysts to ensure comprehensive incident response and effective security operations.

- Managed 24/7 Security Operations Center (SOC) activities, including event monitoring, incident detection, real-time threat analysis, and report generation.
- Performed real-time monitoring of network security components, including firewalls, routers, system applications, Windows devices, and web servers.
- Recommended improvements to security systems and procedures through continuous assessments.
- Hands-on experience with Azure Sentinel, Endpoint Detection and Response (EDR) and Nessus tools.
- Investigated security threats, creating detailed cases and escalating them to appropriate teams.
- Strong knowledge of networking concepts such as OSI layers, Subnetting, TCP/IP, Ports and Protocols.
- Proficient in using security solutions like antivirus, firewalls, proxies, IPS, and email security.
- Experienced in responding to malware and phishing attacks with effective mitigation strategies.
- Generated daily, weekly, and monthly security reports tailored to client requirements.
- Carried out day-to-day duties accurately and efficiently.

EXPERIENCE

Custologix Solutions India Private Limited (16th April 2021 – present)

- Monitored real-time events using SIEM tools such as Microsoft Sentinel and Splunk.
- Handled alerts from multiple security log sources such as proxy and antivirus systems.
- Performed phishing and spam email analysis using Microsoft 365 email protection.
- Conducted regular vulnerability assessments to identify and fix security weaknesses.
- Implemented patches or updates to address identified vulnerabilities.
- Responded to and investigated security alerts in real-time.
- Created incident reports and collaborated with other teams to prevent future breaches.
- Documented security incidents, actions taken, and post-incident analysis to improve the organization's incident response process.
- Generated detailed security reports in Azure Sentinel and Nessus, highlighting key findings, remediation actions, and trends for upper management.
- Reviewed and maintained a list of trusted applications to prevent false positives by allowing approved applications to bypass security controls while ensuring they were not exploited by attackers.
- Identified and maintained a list of trusted applications to prevent false positives by allowing approved applications to bypass security controls while ensuring they were not exploited by attackers.
- Continuously monitor security systems, logs, and alerts to detect and mitigate potential security breaches and vulnerabilities.
- Act as a first responder to investigate and resolve security incidents, ensuring prompt recovery from breaches.
- Ensure the organization complies with security policies, standards, and regulatory requirements by conducting periodic security audits.
- Assess security risks associated with new software or systems and implement appropriate security controls.
- Document all security incidents and breaches, preparing reports for management and contributing to post-incident reviews.
- Performed regular network scans using Nessus to identify vulnerabilities in systems,
- Monitored endpoints using Microsoft Defender for Endpoint to detect malware, Ransomware, and suspicious endpoint activities, reducing the risk of data breaches.
- Manage and configure security tools like firewalls and antivirus.

AWARDS & APPRECIATIONS

- Achieved best quality award within first 3 months.
- Appreciation from Team leader for sharing product knowledge to team members.

TECHNICAL SKILLS

❖ **SIEM**	**:**	Azure Sentinel
❖ **EDR**	**:**	Microsoft Defender for Endpoint
❖ **Firewall**	**:**	FortiGate
❖ **Proxy Server**	**:**	McAfee Web Gateway
❖ **Email Security**	**:**	Office 365
❖ **Vulnerability Management**	**:**	Nessus
❖ **Ticketing tools**	**:**	ServiceNow
❖ **Anti-Virus**	**:**	Symantec Endpoint Protection.
❖ **Windows Servers**	**:**	Windows 2003 & 2008

PERSONAL SKILLS

- Good Communication skill and leadership qualities.
- Adaptive to new technologies and Quick learner.
- Can be molded to fit into any position.
- Problem solving ability.
- Responsible & Hardworking.

ACADEMIC CHRONICLE

- **B.tech. from SK University in the Year of 2017.**

PERSONAL PROFILE

Name	:	Thirugabathini Naveen
Father's name	:	Ramachandraiah.T
Gender	:	Male
Nationality	:	Indian
Languages known	:	Telugu, English, Tamil.

DECLARATION

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear the responsibility for the correctness of the above-mentioned particulars.

PLACE:

(T Naveen)

DATE: