R. Ganesh Shankar

Email: ganeshshankar.soc2025@gmail.com
Mobile No: +91 6305600106

Objective

I'll be glad to work on challenging tasks with my subordinates and professionals in which I will develop my technical as well as management skills. Provides knowledge to lead my carrier in TOP IT SECURITY PROFESSIONALS.

TECHNICAL SKILLS

SIEM Solutions	: Splunk, Microsoft Sentinel, Wazuh
Dark Web Monitoring	: Cyble
ETP	: Trellix
Firewall	: Palo Alto, Pfsense
IDS/IPS	: Snort
EDR	: Symantec, Microsoft Defender
Vulnerability	: Qualys
Proxy	: Bluecoat
Sandbox	: VM-Ray
Network	: Netskope, Wireshark
Cloud Security	: Azure, AWS
Code Review	: VS Code
Ticketing Tool	: Service Now, Jira

PROFESSIONAL EXPERIENCE

Holding experience with **PARAMATRIX TECHNOLOGIES** as Network Security Engineer, worked from **Dec-2022** to **March-2025**.

Roles & Responsibilities:

- Managed **24x7 SOC operations**, ensuring timely task completion and consistent performance.
- Responsible to **monitor Dark web activity** like Compromised Endpoints, Data Exposure, Leaked Credentials, Brand Abusing.
- Handling **ETP alerts** and analyzing **phishing emails** executed thorough investigations and provided prompt and accurate responses to clients.
- Contributed to **security awareness training** and education for employees.
- Responsible for investigation of **proxy logs**.
- Utilized **VM-Ray sandbox** for malware analysis.
- Monitored endpoint logs using **EDR** solutions to detect suspicious activities.
- Monitoring **massive uploads, port scan, login attempts, API calls,**

SharePoint operation and interacting with users for conformation.

- Acknowledging and closing **false positives** and raising tickets for validated **true positives** incidents.
- Using **FS-ISAC** service, to find out new **vulnerabilities**.
- Performed daily **health check** of SIEM and share the same daily status to Soc-L2.
- **Managed ticket** follow-ups and closures, ensuring effective communication and resolution based on client feedback.
- Prepared, validated, and delivered comprehensive **daily, weekly, and monthly reports** to stakeholders, highlighting key insights and actionable recommendations.
- Draft **shift handover** for next shift engineers.

Holding experience with **SUNRAISE SOLUTIONS PVT Ltd** as an **Android Developer** worked from **Dec 2021 to Oct 2022**.

Roles & Responsibilities:

- Developed initial **wireframes** and interactive **prototypes** to visualize application flows, collaborating with designers to ensure alignment with user experience goals.
- Created flowcharts to guide **UI and UX design** processes, ensuring cohesive user experiences across the application.
- Ensured UI responsiveness across various devices, optimizing layouts for different screen sizes and **enhancing accessibility**.
- Conducted thorough **performance assessments** to identify bottlenecks and improve application speed and efficiency.
- Maintain clear **documentation for code** and development processes for future reference.

Holding experience with **CENTRUM TECH** as an **Erection & Commission Engineer**, worked from **Sep 2020 to Oct 2021**.

Roles & Responsibilities:

- Generated and issued **purchase orders for RMU** components, ensuring compliance with project specifications and budget constraints.
- Coordinated with the **Tamil Nadu Electricity Board** for necessary approvals, ensuring adherence to local regulations and safety standards.
- **Executed wiring** of RMU and implementing proper phase connections and grounding practices.
- Conducted **comprehensive testing**, including insulation resistance and operational tests, to verify RMU performance and integrity.

PROJECT

- Hands on integration & configuration of SIEM tools such as Wazuh, to monitor AWS & Pfsense firewall logs for enhanced security visibility.
- Developed and implemented use cases within the SIEM to detect and respond to security events like unauthorized access, remote access, PowerShell execution, and other critical activities.
- Created Standard Operating Procedures (SOPs) for SOC operations, establishing standardized processes to ensure efficient and effective response to security incidents.

CERTIFICATION

- Certified in C, Python.
- Certified in CCNA, MCSE, Linex, CEH.
- Certified in AZ-500.

EDUCATION

- Completed Bachelor of Technology Education from Aditya Engineering College 2015-2019.
- Completed Intermediate from Sri Chaitanya Junior College, Rajahmundry 2013-2015.
- Completed SSC from Manuel Mony Metric Hs School, Chennai in 2013.

DECLARATION

I hereby declare that the above information is correct to the best of my knowledge, and I bear the full responsibility for the correctness of the above mentioned.

Date:

Place: (R. Ganesh Shankar)