RESUME

SAI RAVI KIRAN
Email:cravikiran44@gmail.com
Mobile No: +91 7386763176

Objective

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

TECHNICAL SKILLS

SIEM Solutions	: IBM QRadar
ETP	: Trellix
XDR	: CORTEX
EDR	: Symantec
Vulnerability	: Qualys
Proxy	: Bluecoat
Sandbox	:CrowdStrike Falcon
Network	: Wireshark
Cloud Security	: Azure
Ticketing Tool	: Service Now

Professional Experience

I am currently working with **QUANTED TECHNOLOGIES PVT LTD** as SOC Analyst working from **MAY-2021** to till now.

Roles & Responsibilities:

- Managed **24x7 SOC operations**, ensuring timely task completion and consistent performance.
- Conducted real-time log monitoring across security devices including **SIEM, EDR**,XDR.
- Handling **ETP alerts** and analyzing phishing emails, executed thorough investigations, and provided prompt and accurate responses to clients.
- Responsible for checking **Phishing mail** and delivery details of user on mail gateway for analysis.
- Contributed to **security awareness training** and education for employees.

- Responsible for analyzing the **URLreported** by the user, based on investigation we provide access as per company policy.
- Utilized **VM-Ray sandbox** to analyses files for potential malicious behavior, determining legitimacy through detailed threat intelligence.
- Conducted **malware analysis** using techniques to evaluate file behavior
- Monitored endpoint logs using **EDR** solutions to detect suspicious activities and ensure endpoint security across the organization.
- Monitoring **massive uploads** and interacting with users for conformation.
- Acknowledging and closing **false positives** and raising tickets for validated incidents.
- Using FS-ISAC service, we inform customers of new vulnerabilities.
- Submitting weekly scanning report and identifying the not fixed **vulnerabilities** to patch.
- Monitored for **internal security alerts**, such as RAT detections and unauthorized command usage...etc.
- Responded promptly to real-time alerts, prioritizing actions based on risk assessments and **escalating incidents** to higher level SOC analysts for further analysis.
- Performed daily **health check** of SIEM and share the same daily status to admin team and IT Security Team.
- **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**

- Strong analytical and problem-solving skills.
- Proficiency in system architecture and design principles.
- Knowledge of programming, scripting, and automation tools.
- Familiarity with network systems, databases, and cybersecurity practices.
- Excellent communication and collaboration abilities
- Project management and time management skills.

TRAINING & CERTIFICATIONS

- Certified in CCNA, MCSE
- Course Completed in CEH.
- Pursuing Threat Hunting, Digital Forensic

EDUCATION

- Completed Bachelor of Technology Education from J N T U A

DECLARATION

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

Date:

Place: (C RAVI KIRAN)