

KISHORE D

Chennai ,Tamil Nadu

+91 6382052095

Kishoredasarathan4@gmail.com

Kishore Dasarathan - [LinkedIn](#)

PROFILE SUMMARY

Cybersecurity and IT infrastructure professional with hands-on experience in network security, endpoint protection, and system monitoring. Skilled in web application testing, firewall management, and SOC-level analysis. Proficient in maintaining core IT services and tools like Zabbix, Tactical RMM, and ESET. Adept at automation, vulnerability assessment, and enhancing security posture through proactive monitoring and continuous improvement.

PROFESSIONAL EXPERIENCE

10-SEP-2024 - PRESENT

Dr. MEHTA'S HOSPITALS PVT LTD

INFORMATION TECHNOLOGY SECURITY

Roles & Responsibilities

- **Managed and monitored antivirus protection** using **ESET** for endpoint security; enforced policies for USB/CD restrictions and web control, conducted daily scans, and addressed threat detections.
Antivirus & EDR: ESET
- **Utilized Tactical RMM** to perform automated daily checks on user endpoints for Windows updates, disk space, system uptime, and overall health; **also executed scripts for temporary file cleaning, speed testing, and provided remote access support.**
EDR & RMM: Tactical RMM
- **Administered Zabbix Network Monitoring System (NMS)** to track server and network device health, resource utilization, and availability. Created custom dashboards, alerts, and enabled proactive issue detection.
Monitoring Tools: Zabbix
- **Implemented and integrated new security tools and systems** to strengthen IT security posture and proactively mitigate emerging threats.
Cybersecurity Solutions & Integration
- **Reviewed and analyzed firewall logs, system events, and failed login attempts** to identify and escalate potential security incidents or unauthorized access.
Security Monitoring & Incident Response
- **Performed preventive maintenance (PMS)** on switches, routers, and networking hardware to reduce downtime and improve infrastructure reliability.
Network Maintenance
- **Managed and maintained Unifi Access Point Controller**, monitoring AP health, troubleshooting wireless issues, and taking regular configuration backups.
Wireless Network: Unifi
- **Conducted weekly backups** of switch configs, Unifi Controller, ESET, Zabbix, Tactical RMM, Wazuh, and Grafana to ensure disaster recovery readiness.
Backup & Disaster Recovery: ESET, Zabbix, Tactical RMM, Wazuh, Grafana
- **Led weekly internal knowledge-sharing sessions** focused on threat alerts, tool updates, and cybersecurity awareness for team development.
Team Collaboration & Cybersecurity Training
- **Provided hands-on support for networking issues**, including VLAN configuration, port assignments, and troubleshooting with system administrators to ensure stable connectivity.
Network Support & Switching
- **Performed basic administration of DHCP and Active Directory AD** for IP scope allocation, user account provisioning, and permission management; **also managed QNAP File Server** for shared storage access and user permissions.
Server Management: DHCP, Active Directory, QNAP File Server

INTERNSHIPS

- **Code Alpha** – Cybersecurity Analyst Internship - September-2024
Worked on security tool implementation projects, including developing a basic network sniffer to analyze and capture traffic data. Gained hands-on experience in security tool development, network traffic inspection, and basic packet analysis.
- **Prodigy Infotech** – Cybersecurity Internship - August-2024
Learned fundamental concepts of cybersecurity, including threat types, vulnerability assessment, and defensive practices. Participated in basic security tasks to understand real-world cybersecurity operations.

TECHNICAL SKILLS

Endpoint & Network Security
Web Application Security (OWASP Top 10)
Incident Response (Detection, Containment, Recovery)
Vulnerability Assessment & Management
Basic Cryptography & Data Protection
Security Monitoring & Alert Analysis
Network Support & Troubleshooting

TOOLS & TECHNOLOGIES

Antivirus & EDR: ESET, Wazuh, Tactical RMM
Web Security Testing: Burp Suite
SIEM Platforms: Wazuh, Splunk
Network Monitoring: Zabbix, Wireshark
Threat Intelligence & Analysis: VirusTotal
Offensive Tools: Metasploit

SOFT SKILLS

- Strong analytical and problem-solving skills
- Effective communication in cross-functional teams
- Ability to work under pressure during incident response

CERTIFICATIONS

- CCNA – Cisco Certified Network Associate (Suren Networks) – Currently Pursuing
- EHE - Ethical Hacking Essentials([EC-Council](#))
- FCA - Fortinet Certified Associate in Cybersecurity ([7580581793KD](#))
- SQL Injection Attacks([EC-Council](#))
- Python([GUVI](#))
- OWASP TOP 10([LinkedIn](#))
- CyberSecurity Essentials([CISCO](#))

ACHIEVEMENTS

- Deployed Zabbix with custom dashboards and WhatsApp alerts for real-time infrastructure monitoring.
- Configured Wazuh (SIEM) for centralized log monitoring across firewall, switch, and server systems.
- Integrated Grafana to visualize metrics from Zabbix, Wazuh, and other tools for improved IT visibility.
- Automated Netgear switch configuration backups to enhance network reliability and disaster recovery.
- Reported 30+ web vulnerabilities; several acknowledged via bug bounty programs.
- Gained hands-on experience with CTFs, pentesting, and SIEM tools via TryHackMe and PortSwigger.

EDUCATION

YEAR	DEGREE	INSTITUTE	MARKS
2021-2024	BCA	Apollo Arts and Science College - Chennai	71.6 %
2021	HSC	Little Jacky Matriculation School - Chengalpattu	76.3 %
2019	SSLC	Little Jacky Matriculation School - Chengalpattu	67.6 %

MINI PROJECT

A Web Based KeyLogger - A malicious tool designed to record keystrokes entered by users on a website. It captures keyboard input and sends it to a remote server controlled by the attacker. This type of keylogger can compromise sensitive information such as usernames, passwords, credit card numbers, and other confidential data entered by unsuspecting users.