KISHORE D

Network Security-focused professional experienced in CrowdStrike Falcon EDR, SIEM monitoring, and firewall operations, with hands-on SOC alert triage and network expertise in routing, switching, and monitoring using Zabbix.

No:29/12, 7th Street, BV Nagar
Nanganallur, 600114
Chennai, Tamilnadu
+91 6382052095
kishoredasarathan4@gmail.com

EXPERIENCE

Dr.Mehta's Hospitals — *Network Security Analyst*

SEP 2024 - PRESENT

Roles and Responsibilities:

- **Endpoint Security & SOC Operations**
  Worked with CrowdStrike Falcon EDR for endpoint protection, alert triage, and incident response, with operational exposure to Falcon Next-Gen SIEM for security monitoring and investigation support.
- **Network Monitoring & Alerting**
  Administered Zabbix NMS with custom dashboards, alerts, and proactive monitoring of servers and network devices.
- **Firewall & Network Security**
  Managed firewall, including policy configuration and enforcement, rule audits, traffic monitoring, and performance tuning to ensure secure and reliable network operations.
- **Wireless Network Administration**
  Managed UniFi AP Controller with health monitoring, troubleshooting, and configuration backups.
- **LAN & Switch Management**
  Provided network support through VLAN setup, port management, and troubleshooting, managed L2 and L3 (Core) switches to ensure stable and efficient network performance.
- **Server & Storage Administration**
  Administered Windows servers (DHCP, DNS, AD) and managed NAS Storage server for storage, permissions, and user access.
- **Virtualization Management**
  Managed VMware ESXi servers, including provisioning and configuring virtual machines to support business operations.
- **Ticketing & Issue Management**
  Utilized SHIVAM ticketing tool to efficiently track and resolve network issues, ensuring timely incident management and service continuity.
- **Information Security & Compliance**
  Supported ISO 27001 compliance activities related to security policies, access control, and audit readiness.

SKILLS

Endpoint Security

SIEM

IP Addressing & Subnetting

Wireless Networking

DHCP, DNS, AD Servers

Routing & Switching

Network Monitoring System

Web Pentesting & Bug Hunting

Server Virtualization

Network Troubleshooting

Linux Administration

CERTIFICATION

CCNA - Suren Networks

EHE Ethical Hacking Essentials - EC Council

FCA Fortinet Certified Associate - Fortinet

SQL Injection Attacks - EC Council

Python - GUVI

CyberSecurity Essentials - CISCO

Intro to Splunk - SPLUNK

EDUCATION

Apollo Arts and Science College, Chennai — *BCA*

MAR 2021 - APR 2024

Little Jacky Matriculation School, Chengalpattu — *HSC*

MAR 2021 - MAR 2021

Little Jacky Matriculation School, Chengalpattu — *SSLC*

MAR 2019 - MAR 2019

PROJECTS

Wazuh SIEM Deployment for Threat Detection & Incident Response
Configured Wazuh to monitor endpoints, switches, and firewalls via Syslog, providing real-time threat detection, dashboards, and automated alerts for faster incident response.

Zabbix Monitoring System with WhatsApp Alerts
Implemented Zabbix with custom dashboards and WhatsApp alerts via API for real-time notifications, boosting incident response and proactive infrastructure monitoring.

Tactical RMM Implementation
Deployed and configured Tactical RMM for remote monitoring and automated maintenance, improving endpoint management and overall IT operations visibility.

Automatic Backup Script for Network Devices
Developed a Python script with Paramiko to automate network device backups via SSH, organizing files by date for easy management and improved reliability.

ONLINE PRESENSE

Github: https://github.com/KishoreDasarathan
Portfolio: https://kishoredasarathan.github.io/portfolio/
LinkedIn: https://www.linkedin.com/in/kishore-dasarathan-39a9b6277

AREA OF INTEREST

SOC Analyst

Network Security

NOC Analyst

CyberSecurity Analyst

Server Management

TOOLS & TECHNOLOGIES

Falcon Crowdstrike EDR

Wazuh

Zabbix NMS

ESET

Burp Suite

WireShark

Nmap

Metasploit

Virus Total

SOFT SKILLS

Problem Solving

Curiosity & Learning

Adaptability

Attention to Detail

OPERATING SYSTEM

WINDOWS

LINUX