Chandru M

Thanjavur, TamilNadu | 9003843212 | chandrum1410@gmail.com | LinkedIn

PROFESSIONAL SUMMARY

Cybersecurity & Technical Support Engineer with 1.9 years of hands-on experience in Security Operations, SIEM monitoring, endpoint security, and incident response across global on-prem and cloud environments. Skilled in alert triage, log analysis, threat investigation, malware analysis, vulnerability assessment, and security policy configuration. Experienced in monitoring and responding to security events using EDR/XDR and SIEM tools, improving endpoint hardening, and supporting incident containment and remediation. Strong understanding of the MITRE ATT&CK framework, Cyber Kill Chain, and security best practices. Immediate joiner.

SKILLS

S**ecurity Technologies:** EDR/XDR, SIEM, DLP, IDS/IPS, Firewalls, Endpoint Security, Threat Detection, Malware Analysis(basics)

Security Operations: SIEM Monitoring, Alert Triaging, Incident Detection & Response, , Log Analysis, Threat Investigation, Endpoint Hardening, Vulnerability Assessment

System & Network Skills: Networking Concepts, TCP/IP, DNS, DHCP, VPN, Linux Administration, Windows Administration

Security Management: Patch Management, Encryption Management, Policy Configuration, Access Control, Compliance & Security Monitoring

Tools & Platforms: Kaspersky (EDR/XDR), SIEM (KUMA), Burp suite, Nmap, DLP (InDefend)

EXPERIENCE

Cyber Security – Technical Support Engineer
Ecaps Computer Private Limited - Coimbatore
April 2024 – Oct 2025

- Provided advanced technical support for Kaspersky Endpoint Security across on-premises and cloud environments, ensuring high availability and security compliance.
- Monitored, analyzed, and triaged security alerts and events generated from SIEM and EDR/XDR platforms to identify potential threats and security incidents.
- Performed log analysis, incident detection, investigation, and response activities, including malware analysis, suspicious process analysis, and endpoint behavior monitoring.
- Supported incident containment and remediation by isolating affected endpoints, applying security policies, and validating remediation actions.
- Configured and managed security controls including EDR, XDR, SIEM integration, encryption, patch management, and policy enforcement.
- Collaborated with SOC teams to escalate high-severity incidents, providing detailed analysis, proper documentation, and root cause analysis (RCA).
- Supported and integrated additional security solutions such as firewall configurations and DLP tools, improving network security and data protection.

Penetration Testing Intern
HackersForYou
April 2024 – Nov 2024

- Conducted vulnerability assessments and penetration testing using tools such as Burp Suite, Nmap, Sublist3r, and other OSINT/scanning utilities.
- Performed complete VAPT cycles including Reconnaissance, Scanning, Exploitation, Post-Exploitation, and Reporting for web applications and internal systems.

- Practiced and simulated real-world attack scenarios through TryHackMe, building hands-on expertise in web attacks, privilege escalation, misconfigurations, and exploitation workflows.
- Assisted in strengthening client security posture by validating fixes and verifying remediation implementation after VAPT.

EDUCATION

- **M.Sc in Cybersecurity**
  Bharathiar University, Coimbatore
  June 2021 – May 2023

- **Bachelor of Computer Applications (BCA)**
  Periyar Maniammai University, Thanjavur
  July 2018 – April 2021

CERTIFICATIONS

- Kaspersky Next EDR Optimum
- Kaspersky Next XDR Expert
- Kaspersky Secure Mail Gateway
- Network Defense Essentials – EC-Council
- Cybercrime Police Station Internship

LANGUAGES

- English
- Tamil