Pavankumar Khot

Pune, Maharashtra — +91 9307268996 — khotpavankumar27@gmail.com
linkedin.com/in/pavankumar-khot — github.com/ItsBenign-Pavan — MyPortfolio.io

Summary

Endpoint Security Engineer with hands-on experience in threat analysis, incident response, and escalation. Contributing to Microsoft's DEX-E project at LTIMindtree to strengthen enterprise endpoint security posture.

Technical Skills

Security Operations	SIEM , Threat Hunting, Alert Triage, Log Analysis
Security Tools	Burp Suite, Wireshark, Nmap, Metasploit
Networking	TCP/IP, DNS, VPN, Firewalls, Proxy, Packet Analysis
Programming	Python (automation), Bash, PowerShell
Platforms	Windows Server, Linux (Kali/Ubuntu), VMware, Active Directory
Frameworks	MITRE ATT&CK, NIST, Cyber Kill Chain, OWASP Top 10

Professional Experience

Endpoint Security Engineer (Threat Hunter) 2024 – Present
LTIMindtree Limited — *Client: Microsoft DEX-E (Defender Experts for Endpoint)* (2 years)

Responsible for triaging endpoint security incidents, escalating high-severity threats, and collaborating with Microsoft's Defender Experts to enhance threat detection.

Projects

Project Name: Microsoft DEX-E (Defender Experts for Endpoint) 2024 – Present
Organization: LTIMindtree Limited, Client: Microsoft (2 years)

- Investigated and responded to 10,000+ endpoint security incidents and 500+ high-severity escalations, improving threat detection and response efficiency.
- Investigated and triaged high-severity security incidents related to info-stealer, credential theft, privilege escalation and lateral movement.
- Handled targeted threat campaigns (e.g., ClickFix), including exploitation attempts on server vulnerabilities such as SharePoint RCE and WSUS spoofing.
- Developed KQL-based hunting queries to track ongoing threats, including targeted campaigns.
- Investigated Windows logs and mapped findings to MITRE ATT&CK techniques.
- Conducted KT sessions and shadowing for new team members, improving team productivity and reducing onboarding time.

Certifications

TryHackMe: Pre Security Certificate
TryHackMe: Cyber Security 101
Udemy: Ethical Hacking Masterclass
EC-Council: SQL Injection Attacks

Education

Bachelor of Technology (B. Tech) in ICE (CGPA: 8.95) 2023
From Vishwakarma Institute Of Technology (VIT), Pune (Affiliated with Savitribai Phule Pune University)

Achievements

Completed practical cyber-security labs and SOC investigations on TryHackMe and LetsDefend, gaining hands-on experience in threat hunting, log correlation, and real-time incident response.

TryHackMe: tryhackme.com/p/ItsBenignPavan
LetsDefend: letsdefend.io/user/khotpavankumar27