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 endpoint threat detection, incident response, and alert escalation. Currently contributing to Microsoft Defender Experts for Endpoint (DEX-E) at LTIMindtree, supporting enterprise-scale security operations.

Technical Skills

Security Ops	SOC L1, Alert Triage, Incident Response, Threat Detection, Threat Hunting, Logs
Endpoint Security	EDR/XDR/MDR, Microsoft Defender for Endpoint, Windows Security, Malware Analysis
SIEM & SOAR	Splunk, Microsoft Sentinel, SOAR Playbooks
Networking	TCP/IP, DNS, VPN, Firewalls, Proxy, Packet Analysis
Security Tools	Wireshark, Nmap, Burp Suite, Metasploit
Scripting	Python (Automation), PowerShell, Bash
Platforms	Windows Server, Linux (Kali, Ubuntu), Active Directory, VMware
Frameworks	MITRE ATT&CK, NIST, Cyber Kill Chain, OWASP Top 10

Professional Experience

Endpoint Security Engineer — Microsoft Defender Experts (DEX-E) 2024 – Present
LTIMindtree Limited — Client: Microsoft

- Triaged and investigated **10,000+ endpoint alerts**, escalating **500+ high-severity incidents** across enterprise environments.
- Investigated advanced attack techniques including **credential theft, privilege escalation, lateral movement, and info-stealers**.
- Responded to **targeted attack campaigns** (e.g., ClickFix), including **SharePoint RCE** and **WSUS spoofing**.
- Performed **endpoint forensics and Windows log analysis**, mapped to **MITRE ATT&CK**.
- Built and executed **KQL threat-hunting queries** and collaborated with Microsoft experts to improve detections.

Projects

Microsoft Defender Experts for Endpoint (DEX-E) 2024 – Present
LTIMindtree Limited — Client: Microsoft

- Supported managed threat detection and response (MDR) operations for global enterprise customers.
- Created custom KQL threat-hunting queries to track active campaigns and anomalous endpoint behavior.
- Delivered knowledge transfer (KT) sessions and mentored new team members, reducing onboarding time and improving operational efficiency.

Recognition & Certifications

Hi-Five Spot Award — Honored for taking strong initiative and consistently delivering tasks with impeccable accuracy.
Certifications: TryHackMe (Pre Security, Cyber Security 101, SOC Level 1), EC-Council (SQL Injection Attacks), Udemy (Ethical Hacking Masterclass)

Education

Bachelor of Technology (B.Tech) – ICE 2023
Vishwakarma Institute of Technology (VIT), Pune — **CGPA: 8.95** — Savitribai Phule Pune University

Achievements

Hands-on experience through TryHackMe and LetsDefend SOC labs, performing threat hunting, log correlation, and real-time incident response.

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