Mayur Mahajan

Cybersecurity Analyst | SOC L1 | Incident Response | SIEM | Threat Hunting
Pune, Maharashtra — +91 8390800964 — mayurmahajan.020@gmail.com
linkedin.com/in/mayur-mahajan-160b84224 — mayurmahajan.netlify.app

Summary

Cybersecurity Analyst with hands-on experience in SOC operations, phishing analysis, malware investigation, and incident response. Currently working on the Microsoft Anti-Phishing project at LTIMindtree, contributing to enterprise-scale email and URL threat detection using SIEM platforms including Splunk.

2+ Years of Enterprise-Scale Security Operations Experience

Technical Skills

Security Ops -	SOC L1, Alert Triage, Incident Response, Threat Hunting, Phishing Analysis, Malware Analysis
SIEM & SOAR -	Splunk, Microsoft Defender
Endpoint -	EDR/XDR, Log Analysis, Sandboxing (VirusTotal, Hybrid Analysis), Sophos
Networking -	TCP/IP, DNS, HTTP/S, IDS/IPS, VPN, Firewall, DHCP, Packet Analysis
Security Tools -	Wireshark, Burp Suite, Nmap, VirusTotal, Hybrid Analysis, OSINT Tools
Frameworks -	MITRE ATT&CK, OWASP Top 10
Platforms & OS -	Windows, Linux (CLI), Microsoft Azure
Ticketing -	ServiceNow · SOP / SLA Management · IOC Identification

Professional Experience

Cybersecurity Analyst — SOC Operations Dec 2024 – Present
LTIMindtree Limited (LTM) — Client: Microsoft

- Handle 40–60+ security alerts daily — phishing, spam, and malware incidents — performing real-time monitoring, triage, investigation, and escalation across enterprise environments.
- Use Splunk SIEM platform to detect security breaches, correlate events, and perform root-cause analysis per client SOPs.
- Conduct email header analysis, URL/domain analysis, and sandbox malware investigation using VirusTotal and Hybrid Analysis via static and dynamic techniques.
- Analyse phishing emails and malicious URLs using OSINT tools; classify phishing techniques (credential harvesting, BEC, spear phishing) and document IOCs.
- Reduced false positives by ~20–25% through refined detection rules; blocked 100+ malicious URLs monthly via proactive threat intelligence.
- Manage incident tickets in ServiceNow, maintaining SLA compliance; prepare daily, weekly, and monthly incident reports in client-specified format.
- Report phishing URLs for Microsoft SmartScreen filter updates; contribute to blocking/whitelisting and global phishing trend monitoring.

Cybersecurity Analyst May 2024 – Dec 2024
LTIMindtree Limited (LTM) — Pune

- Supported cloud security monitoring, identity protection, and security event triage across Microsoft Azure environments.
- Transitioned from cloud infrastructure to dedicated SOC cybersecurity operations, strengthening detection and incident response capabilities.
- Assisted in threat correlation, alert investigation, and SIEM rule management.

Graduate Engineer Trainee Mar 2024 – May 2024

LTIMindtree Limited (LTM) — Pune

- Completed cybersecurity domain onboarding covering **SOC workflows, SIEM platforms, and enterprise security tooling**.
- Gained foundational exposure to threat detection processes, ticketing systems, and incident response procedures.

Projects

Microsoft Anti-Phishing Intelligence & Threat Detection 2024 – Present

LTIMindtree Limited (LTM) — Client: Microsoft

- End-to-end investigation of **phishing emails, malicious URLs, and suspicious domains** using OSINT and third-party intel tools.
- Performed **email header, sandbox-based URL analysis** using Burp Suite, VirusTotal, Hybrid Analysis; identified IOCs and phishing infrastructure.
- Classified phishing techniques (credential harvesting, BEC, domain spoofing); reported URLs for Microsoft SmartScreen updates.
- Monitored global phishing trends; updated internal SOPs and collaborated with the client on escalated campaigns.

Recognition & Certifications

Super Crew Award — Recognised for exceptional initiative, accuracy, and high-impact execution in SOC operations at LTIMindtree (iWkn).

Team Player Award — Formally recognised for collaborative excellence and consistent contribution to SOC team goals.

Creative Award — Awarded for innovative thinking and creative problem-solving in security detection workflows.

Hi-Five Spot Award — For taking the initiative and completing all tasks with impeccable accuracy and speed.

Certifications: Microsoft Azure AI Fundamentals (Microsoft), Generative AI (Coursera), Programming for Everybody — Python (Coursera), SQL, Full Stack Development Bootcamp, Decentralized Voting System using Blockchain (Copyright).

Education

Bachelor of Engineering (B.E.) — Computer Engineering 2023

Dr. D.Y. Patil Institute of Engineering, Management & Research — Savitribai Phule Pune University

Portfolio: mayurmahajan.netlify.app **LinkedIn:** linkedin.com/in/mayur-mahajan-160b84224