TANVI KAMDI

SOC Analyst | Incident Triage & Response | Digital Forensics | SIEM Monitoring

+91-9307595845 | tanvikamdi38@gmail.com | Mumbai, India | LinkedIn | GitHub | Portfolio

PROFESSIONAL SUMMARY

Forensic investigation professional transitioning into SOC Analyst roles, with hands-on experience in incident triage, SIEM monitoring (Splunk, Sentinel, Wazuh), and log/evidence analysis, backed by foundational scripting in PowerShell and Python.

EDUCATION

Master's in Forensic Science — Chandigarh University, Punjab

Bachelor's in Forensic Science — G.H. Raisoni University, Amravati

TECHNICAL SKILLS & COMPETENCIES

Incident Response & Forensics: Security Incident Triage, NIST IR Lifecycle, Chain of Custody, Evidence Preservation, FTK Imager, Autopsy, TheHive, Windows Event Log Analysis, Metadata & Steganography Analysis

SIEM & Security Monitoring: Splunk, Microsoft Sentinel, Wazuh, Log Review & Analysis, Alert Triage

Endpoint & Threat Analysis: Microsoft Defender, Process Explorer/Monitor, VirusTotal, CyberChef, MITRE ATT&CK, Cyber Kill Chain, IOC Analysis, YARA, Remediation & Containment

Networking & Systems: TCP/IP, DNS/DHCP, Firewalls, Windows, Linux, Vulnerability Management

Scripting & Tools: SQL, Python, PowerShell, Git/GitHub

PROFESSIONAL EXPERIENCE

Forensic Expert **2024 – 2025**

Spylens Forensic Investigation | Vashi, India

- Performed security incident triage and log/evidence review across 10+ fraud and cybercrime cases — conducting disk imaging, Windows event log and metadata analysis, and evidence recovery from emails, documents, and digital artifacts — improving investigation efficiency by 20% while maintaining 100% chain-of-custody compliance.
- Prepared detailed forensic reports and case documentation to support investigation and remediation outcomes, improving reporting accuracy by 15%.

Business Associate **2025 – 2026**

Stellar Organisation | Andheri, India

- Managed end-to-end client acquisition and relationship management for a sales and CRM-driven business, onboarding 200+ clients and exceeding acquisition targets by 25%+ through targeted outreach and structured communication.
- Handled team management and hiring, including recruiting and onboarding new team members to support business growth.

CYBERSECURITY PROJECTS (INDEPENDENT / HOME-LAB PRACTICE)

Windows Persistence Investigation & Malware Analysis

- Investigated a suspicious Windows persistence incident using Process Explorer, Process Monitor, Task Scheduler, and Registry analysis — identified a hidden scheduled task executing an obfuscated JavaScript loader via a masquerading executable to establish multiple persistence mechanisms.
- Performed evidence preservation, endpoint-based static malware analysis, and threat intelligence correlation via VirusTotal; validated successful remediation by disabling the persistence mechanism and confirming no recurrence post-reboot.

Phishing & Email Threat Investigation

- Triaged a suspicious email as evidence — analyzed headers, footers, and metadata to validate sender authenticity, trace origin, and support incident response decision-making.
- Extracted and hashed attachments, cross-referenced indicators against VirusTotal, and performed sandbox and steganographic analysis to uncover hidden content and document IOCs and findings.

CERTIFICATIONS & TRAINING

- HTB Academy – Incident Handling Process
- Cybrary – SOC Analyst
- Fortinet Training Institute – Fortinet Certified Fundamentals
- Riskpro India – Fraud and Forensic Audit
- Google – Foundations of Cybersecurity
- Great Learning – Advanced Cybersecurity