CHETAN KHARATMAL

Cybersecurity Enthusiast · SOC Analyst Aspirant · Security Researcher
chetankharatmal931@gmail.com | +91 7385216644 | Pune, India
linkedin.com/in/chetankharatmal | github.com/chetankharatmal

PROFESSIONAL SUMMARY

Detail-oriented cybersecurity student (B.Sc. Cyber Security) seeking a SOC Analyst role. Hands-on skills in SIEM monitoring, log analysis, threat detection, DFIR, and incident response. Published researcher on human factors in cybersecurity. Certified by Deloitte, Tata, and MIT; actively completing TryHackMe SOC Level 1.

TECHNICAL SKILLS

SIEM & Logs	Splunk (home lab), Elastic SIEM, Windows Event Log Analysis, Syslog
Networking	TCP/IP, OSI, DNS, DHCP, VLANs, Wireshark, Firewall & IDS/IPS, Traffic Analysis
Threat Detection	MITRE ATT&CK, Incident Response, Vulnerability Management, Risk Assessment
DFIR & Intel	Log Correlation, IOC Analysis, Malware Traffic Analysis, VirusTotal, AlienVault OTX
OS & Scripting	Linux (Kali, Ubuntu), Windows Server, AD Fundamentals, Python, PowerShell, Bash, SQL
Other	Basic Cryptography, Authentication Mechanisms, OWASP Top 10, OSINT techniques

CERTIFICATIONS

Deloitte Australia Cyber Job Simulation · **Tata Cybersecurity Analyst Simulation** · **Computer System Security — MIT/Cursa** · **TryHackMe SOC Level 1** (In Progress) · **Google Cybersecurity Certificate** (In Progress)

EDUCATION

B.Sc. Cyber Security | Indira College of Commerce and Science, Pune *July 2024 – May 2027*
Coursework: Network Security, Digital Forensics, Cryptography, OS, Ethical Hacking · Cyber Club member · Class Representative

PROJECTS

Home Lab SOC Environment · DFIR / SOC *2025*
GitHub: https://github.com/chetankharatmal
- Built VirtualBox lab (Kali, Windows 10, Ubuntu); deployed Splunk to ingest Windows Event Logs & Syslog; built detection dashboards; practised log correlation for suspicious logins, privilege escalation & lateral movement

Windows Investigation Lab · DFIR *2025*
GitHub: https://github.com/chetankharatmal
- Analysed Windows artifacts, event logs & persistence mechanisms; reconstructed attack timelines; mapped findings to MITRE ATT&CK; documented IOC reports

Network Security Lab Simulation · Infrastructure Security *2025*
GitHub: https://github.com/chetankharatmal/Network-Security-Lab-Simulation
- Simulated network security environment: configured VLANs, subnetting, firewall rules & IDS/IPS; performed Wireshark packet analysis to identify anomalous traffic

Phishing Email Analysis Lab · Threat Intelligence *2025*

- Analysed phishing samples: extracted headers, inspected URLs via VirusTotal, identified spoofed domains; documented findings in structured SOC-style incident reports

CMS Security Assessment · VAPT / OWASP *2025*

- Structured assessment covering auth, authorisation, plugin security & OWASP Top 10; produced risk-ranked findings with remediation recommendations

Incident Triage Workflow · Incident Response / SOC *2025*

- Designed IR process (alert validation → evidence collection → impact analysis → escalation) aligned to NIST IR framework phases

The Invisible Leak · AI Security Research *June 2026*

- Research on how generative AI usage creates unintentional insider data leakage; key findings: exposure largely non-malicious, orgs lack visibility, traditional policies insufficient

Other Projects · OSINT / Threat Intel / Python *2025*

- Digital Footprint Analysis (OSINT recon & attribution) · External Asset Mapping (attack surface visibility) · ISP Network Security Review (hardening methodology) · Password Generator (Python, secrets module)

EXPERIENCE & ACTIVITIES

Cybersecurity Researcher & Student Member | ICCS, Pune *June 2024 – Present*

- Published 'Human Factors in Cybersecurity: User/Human Behaviour Analysis' at Anveshan 2026 – 10th Student Conference of SOIT, Indira University (Jan 2024)
- Research on social engineering, user behaviour & insider threats; Cyber Club member; CTF participant (PicoCTF, TryHackMe CTF)

Administrator | CP Constructions (Family Business) *Jan 2022 – Dec 2025*

- Managed operations & vendor coordination; led digitisation of paper records; implemented access controls and data management practices

COMPETENCIES & LANGUAGES

Analytical Thinking · Attention to Detail · Report Writing · Team Collaboration · Leadership · Adaptability · Continuous Learning · Decision Making Under Pressure

Languages: English (Professional) · Marathi (Native) · Hindi (Fluent) | **Interests:** CTF Competitions · Home Lab Projects · Cybersecurity Research · Badminton