SHANTANU UDAY VEDANTE

Cybersecurity Analyst | MSc Cyber Security | SOC & Digital Forensic

Canterbury, Kent | 07927648196 | shantanuvedante3@gmail.com

linkedin.com/in/shantanuvedante23 | github.com/coderx0319

PROFILE

Cybersecurity analyst with hands-on experience in SOC operations, incident response, and digital forensics, gained through a government-level internship with Maharashtra Cyber-India's state cybercrime authority. Skilled in SIEM analysis (Splunk), threat hunting, malware investigation, and IOC extraction, with proven ability to automate triage workflows and produce forensic evidence for active law enforcement cases. Familiar with GDPR, Cyber Essentials, and UK data protection principles. Currently completing an MSc in Cyber Security at the University of Kent, specialising in Digital Forensics and Cyber Analysis. Seeking an entry-level SOC Analyst or Cybersecurity Analyst role where real-world investigative experience and technical rigour can deliver immediate impact.

EDUCATION

MSc Cyber Security | University of Kent, Canterbury, UK Sept 2025 – Sept 2026

- Specialisations: Digital Forensics and Cyber Analysis
- Modules: Forensic Investigation, Malware Analysis, Incident Response, Network Security, Threat Intelligence, AI in Cybersecurity, Cryptography and Security Systems

BE Computer Engineering | University of Mumbai, India Dec 2021 – May 2025

- Grade: CGPI 8.34/10 — equivalent to UK First Class Honours (top 10% of cohort)
- Core modules: Networking, Cryptography, Computer Systems, Data Protection, Artificial Intelligence, Data Science

WORK EXPERIENCE

Cybersecurity Analyst Intern Jan 2025 – Jul 2025

Maharashtra Cyber – Government of Maharashtra, India

- Investigated 10+ active phishing and financial fraud cases, analysing logs and network artefacts to map adversary behaviour to MITRE ATT&CK TTPs and support law enforcement decision-making.
- Delivered forensic evidence across the full incident response lifecycle — from initial triage through containment and post-incident reporting — in direct collaboration with law enforcement agencies.
- Performed malware and memory forensics using Autopsy and Volatility; extracted and documented IOCs in structured technical reports used in live criminal investigations.
- Reduced manual triage effort by ~70% by developing bespoke Python automation tools for log parsing and artefact extraction, accelerating case throughput across the team.

PROJECTS

Network Intrusion Detection and SIEM Lab March 2026

- Designed and deployed a simulated network environment using Splunk, Zeek and Wireshark to monitor and detect malicious activity.
- Developed custom Splunk correlation rules to detect lateral movement and privilege escalation, reducing alert-to-detection time by 40% compared to default rule sets.
- Produced detailed incident reports mapping attack chains to MITRE ATT&CK, replicating real SOC analyst workflows.

Phishing Email Analysis and Threat Intelligence Tool June 2025

- Built a Python automation tool to parse phishing emails, extract IOCs, and query VirusTotal and AbuseIPDB APIs, significantly reducing manual triage time per case.
- Generated structured, machine-readable threat intelligence reports aligned with SOC analyst output standards.

MAPLMS – Full Stack Learning Management System 2024 – 2025

- Designed and built a production-ready LMS from scratch addressing real-world academic challenges; now adopted by 20+ educational institutions.
- Research paper accepted and presented at ICCCNT 2025, demonstrating applied research and technical communication skills.

TECHNICAL SKILLS

SIEM & Monitoring: Splunk, log analysis, threat hunting, alert triage, SOC workflows
Incident Response: Full lifecycle IR, IOC analysis, attacker timeline reconstruction, MITRE ATT&CK mapping, OSINT
Digital Forensics: Autopsy, Volatility, FTK Imager, memory forensics, chain of custody management
Vulnerability Assessment: Nmap, Burp Suite, OWASP Top 10, CVSS scoring, phishing triage
Networking & Security: Wireshark, TCP/IP, IDS/IPS, network traffic analysis, AWS security fundamentals
Scripting & Development: Python, Bash, PowerShell, Git/GitHub
Frameworks & Standards: MITRE ATT&CK, Cyber Kill Chain, NIST CSF, ISO 27001, GDPR, Cyber Essentials

CERTIFICATIONS

- Google Cybersecurity Certificate
- CompTIA Security+ — in progress (expected completion: September 2025)
- Microsoft & LinkedIn Cybersecurity Career Essentials
- IBM Python for Data Science & AI Certification
- AICTE Cybersecurity Virtual Internship

LEADERSHIP & AWARDS

- President, Computer Education Student Association (2024) — led 100+ member society, coordinating technical events and industry speaker sessions.
- Best Publicity Head, National Service Scheme (2023)
- VPP Student Excellence Award (2025)

INTERESTS

- Cybersecurity research and emerging threat trends
- Technology blogs and continuous learning
- Fitness and wellbeing
- Travel and cultural exploration

REFERENCES

Available on request.