PRATHAMESH SANGAI

Philadelphia, PA / +1-662-877-1789 / prathamesh.sangai@outlook.com / LinkedIn / GitHub

Cybersecurity graduate with experience in malware analysis, digital forensics, SOC operations, and security research, seeking full-time cybersecurity roles in the U.S. with a strong focus on threat detection, incident response, and secure system analysis.

Education

Drexel University Philadelphia, PA
M.S. in Cybersecurity December 2025 — GPA: 3.93
Focus: Malware Analysis, Digital Forensics, Cloud Security, Network Defense, Cryptography
Vishwakarma Institute of Information Technology (VIIT) Pune, India
B.Tech in Information Technology Aug 2019 – Jun 2023

Skills

Programming: Python / C / C++ / Java / Shell / SQL / HTML / CSS
Security Domains: Malware Analysis / Reverse Engineering / DFIR / Threat Hunting / Incident Response / Mobile & Web Penetration Testing / Cloud Security
Blue Team: Splunk / ELK / Wazuh / Wireshark / Sysmon / OSQuery / CrowdStrike Falcon
Red Team: Nmap / Metasploit / Burp Suite / OWASP ZAP / Nessus / Nikto
Forensics: Cellebrite / FTK Imager / Magnet Axiom / Autopsy / Chain of Custody
Cloud & Frameworks: AWS (IAM, EC2, S3, CloudTrail) / Docker / MITRE ATT&CK / NIST CSF / OWASP Top-10

Experience

Drexel University – Security & Privacy Analytics Lab (SePAL) Philadelphia, PA
Research Assistant – Cybersecurity & Malware Analysis Jan 2025 – Present

- Analyzed Android and Windows malware to identify payload execution, persistence, and network exfiltration behavior.
- Built Frida hooks and Xposed modules to intercept sensitive API parameters and plaintext data prior to encryption.
- Inspected TLS and QUIC traffic to map telemetry endpoints, encryption workflows, and indicators of compromise.
- Developed YARA and Sigma rules to automate malware classification and behavioral detection in lab environments.
- Produced structured research summaries and maintained reproducible analysis notes to support ongoing lab workflows.

Sana Cyber Forensics Maharashtra, India
Cybercrime Investigator Intern Aug 2022 – Nov 2023

- Supported CID Pune Police and DGGI in fraud and identity-theft investigations involving mobile and computer evidence.
- Performed forensic imaging and artifact analysis using UFED, FTK Imager, Magnet Axiom, and Splunk.
- Correlated firewall, proxy, and application logs to validate suspicious activity and evidence timelines.
- Prepared chain-of-custody documentation and forensic reports suitable for legal proceedings.

Projects

SOC Incident Simulation Lab 2025

- Built a SOC lab using Splunk and Wazuh to generate alerts mapped to MITRE ATT&CK techniques and scenarios.
- Conducted log analysis and threat hunting to identify anomalous authentication and network behavior.
- Tuned detection rules to reduce false positives and improve alert fidelity across simulated incidents.
- Documented investigation workflows and incident response steps for repeatable SOC analysis and training.

QUIC Secure Chat Application Apr 2024 – Jun 2024

- Developed an encrypted chat system using QUIC and TLS 1.3 with FastAPI-based authentication mechanisms.
- Implemented secure key exchange and session handling logic to enable low-latency and reliable communication.
- Analyzed protocol handshakes and packet flows to validate encryption integrity and session security guarantees.
- Evaluated transport-layer performance behavior under unreliable and high-latency network conditions.

Web Application Penetration Testing Lab 2024

- Performed OWASP Top-10 testing on DVWA and Juice Shop using Burp Suite, Nmap, and Metasploit tools.
- Identified XSS, SQL injection, and authentication flaws with proof-of-concept exploitation results.
- Documented vulnerability impact, severity levels, and remediation recommendations for developers.
- Produced professional penetration testing reports according to industry assessment standards.

Certifications & Leadership

Certifications: Cisco – Introduction to Cybersecurity / CompTIA Security+ (Planned) / EC-Council – Ethical Hacking Essentials (EHE) / Digital Forensics Essentials (DFE) / Microsoft + LinkedIn – Career Essentials
Leadership: Advisory Board Member – EDC VIIT / Documentation & Design Head – MIC.IIC.VIIT