Twinkle Kamdar

tkamdar@andrew.cmu.edu | +1 (956) 278 4371 | linkedin.com/in/twinklekamdar | github.com/hell-99

Work Authorization: F-1 (CPT/OPT eligible)

EDUCATION

Carnegie Mellon University — **Pittsburgh, PA**
Masters of Science in Information Security (MSIS) — **December 2026**
- Coursework: Introduction to Information Security, Network Forensics, Cloud Security, Security in Networked Systems, Host-Based Forensics, AI & Security

Pandit Deendayal Energy University — **Gandhinagar, India**
B.Tech. in Computer Science Engineering | CGPA: 9.44/10 — **May 2025**

EXPERIENCE

Floatbot.AI — **Remote · Milpitas, CA**
Security Analyst Intern — **May 2026 – Present**
- Building PCI DSS v4.0.1 compliance infrastructure — controls tracker, evidence mapping, and scoping docs across GCP US, Azure UAE, and GCP India CDE environments
- Drafted System Security Plan for FTI data protection; produced WAF vendor comparison, Coalition cyber insurance checklist, and IRS Pub 1075 training materials

Silver Touch Technologies — **Ahmedabad, India**
SOC Intern — **May 2024 – July 2024**
- Performed information security risk assessments and VAPT for enterprise clients; triaged 50+ CVEs applying CVSS scoring and CWE classification for accurate risk prioritization and remediation
- Monitored SIEM for alert triage; coordinated compliance evidence collection ensuring NIST CSF, SOC 2 compliance; developed automation scripts reducing manual SOC workload
- Conducted SAST/SCA scan reviews and source code review supporting secure SDLC improvements across Linux/Unix systems

PROJECTS AND RESEARCH

IRIS — LLM Agent Security Monitor | GitHub | iris-hell99.streamlit.app — **Jan 2026 – Present**
- Built 5-layer real-time detection engine for indirect prompt injection, cross-agent collusion & behavioral drift using LangGraph + FastAPI; **93.1% precision, 0.43ms latency**; live Streamlit demo; pip-installable (PyPI)

AEGIS — Autonomous Cybersecurity Intelligence System | GitHub — **Dec 2025 – Present**
- 3-layer ensemble ML IDS/IPS (99% accuracy, 2.5M+ flows, <5ms blocking) in Mininet SDN; post-quantum crypto (Dilithium3 + Kyber768), SHA-256 audit ledger, NIST CSF IR automation, Kubernetes Zero Trust

AWS Security Posture Scanner | GitHub — **Feb 2026 – Present**
- CLI platform detecting 13+ S3/EC2/IAM/VPC misconfigurations via AWS REST APIs; SAST integrated into CI/CD; open-sourced, 1,680+ lines; modular Python automation for ETL across CloudTrail, VPC

Mirai Botnet Detection & Network Forensics | Network Forensics — **Aug 2025 – Dec 2025**
- Simulated full Mirai lifecycle; custom Suricata IDS signatures and Zeek scripts correlating 15,500+ pps across Elasticsearch/Kibana SIEM — 100% detection coverage, zero false positives, full forensic timeline

SKILLS

Programming Languages: C | C++ | Python | Go | Bash | JavaScript | TypeScript | Java | SQL | x86 Assembly | React JS

Offensive Security: Penetration Testing | SQLi | XSS | CSRF | RCE | Privilege Escalation | Web Application Security

Tools: Burp Suite | Metasploit | Nessus | Wireshark | Suricata | Zeek | Elastic Stack | Security Onion | DNS Security | WAF | DDoS Protection | Git | Splunk | Microsoft Sentinel

Cloud: AWS (EC2, S3, IAM, VPC) | GCP | Azure | CloudTrail | CloudWatch | Kubernetes | Docker | Terraform | CI/CD

Networking & OS: Linux/Unix | TCP/IP | BGP | OSPF | DNS | VLANs | OpenFlow | OSI Model | Packet Analysis

Security Frameworks: MITRE ATT&CK | NIST CSF | OWASP | Zero Trust | CVSS | CWE | Vulnerability Management | Incident Response | Detection Engineering | Threat Intelligence | AI Security | LLM Security | PCI DSS v4.0.1 | ISO 42001

Certifications: IBM Threat Intelligence & Hunting | Cisco Introduction to Cybersecurity

Cybersecurity | PicoCTF: Carnegie Mellon University