Harish Kolla

+1 (814) 321-6866 | hkolla03@gmail.com | linkedin.com/in/hkolla/ | github.com/Har1sh-k

Experience

Security Research Engineer - Center for Cyber Security Research, UND Jun 2024 – Present

- Shipped an end-to-end **agentic security pipeline** fusing EDR and SIEM data with ML and embedding-based retrieval for confidence-scored, explainable alert correlation and automated triage, **saving 32+ analyst-hours/week**.
- Designed and deployed scalable **AWS security architecture** integrating IDS, Logstash, Lambda-driven response, and ElasticSearch alert correlation for real-time threat detection, **cutting detection time from hours to under 5 mins**.
- Led **APT adversary emulation** (MITRE ATT&CK–mapped TTPs) across the Edge AI Infra (**1K+ devices**), working across teams to identify weaknesses, validating and hardening controls to **close 50+ high-risk control gaps.**

Security Research Assistant - Penn State Aug 2022 – May 2024

Transparent 5G Rogue Basestation Detection Interface*(with **Purdue University**)*

- Designed and developed a transparent UI incorporating CellID-based baseband firewall, Log Anomaly detection, and Cellular Digital Packet Data (CDPD) Analysis, resulting in the detection and mitigation of 80% of RBS threats.

Secure Multi-Channel Automated Operations Through 5G *(with **IBM Watson Research, AT&T**)*

- Automated 20+ security workflows and policies for Virtual Multi-Factor Authentication(MFA), **configured Next-Gen Firewall using Zero-Trust Architecture**, strengthening secure multi-channel communications by 5x.

Senior Software Security Engineer - Capgemini, India Feb 2021 – Jul 2022

- **Performed threat modeling**, static/dynamic code testing, manual code inspection and development, architecture reviews, and penetration testing of web applications and IT architectures to identify vulnerabilities and security defects.
- Collaborated with stakeholders to identify mitigation strategies by **recognizing points of vulnerability**, non-compliance with established information assurance standards and regulations, enhancing the company's security posture by 20%.

Security Engineer - Siemens & HBL , India May 2019 – Feb 2021

Application Security Engineer | *Jan 2020 – Feb 2021*

- **Implemented endpoint isolation and quarantine workflows** within Cisco Secure Endpoint (EDR), improving real-time threat detection and containment by 25%, addressing advanced malware and insider threats effectively.
- Mitigated 22+ critical vulnerabilities through **Vulnerability Assessment and Penetration Testing(VAPT)**, static and dynamic analysis, app-layer firewalls& Data Loss Prevention (DLP) measures,resulting 40% increase in app security

Security Intern | *May 2019 – Dec 2019*

- **Deployed Network-based Intrusion Detection System** (NIDS) by analyzing traffic in Wireshark to identify 65+ security issues; implemented and monitored firewall, IDS, and access controls to comply with industry standards (RDSO)

Skills

Programming & Operating Systems: Python, C#, C++, PostgreSQL, MongoDB, VectorDB, ElasticSearch, S3, Docker.
Security Tools: Nessus, Splunk, SecurityOnion, Burp Suite Pro, Suricata, Zeek, SonarQube, Nmap, Wireshark, Metasploit.
Frameworks: AWS Security Architecture, NIST AI RMF, OWASP AI/LLM, CVE/CWE, Zero-Trust, MITRE ATT&CK.
Network Security: Next-Generation Firewalls, VPN, SIEM, SOAR, Intrusion Detection and Prevention Systems.
AI/ML Security: LLM Red-Teaming, Prompt Injection/Guardrail Testing, Multi-Agent Orchestration, RAG, MCP.
Concepts: Secure Code Review & Development, SAST/DAST, Pen Testing Agentic Frameworks, Agentic Automation.

Education

Master of Science in Cybersecurity Analytics and Operations University Park, PA
The Pennsylvania State University Aug 2022 – May 2024

Bachelor of Technology in Electronics and Communication Engineering Visakhapatnam, India
Gandhi Institute of Technology and Management Jul 2016 – May 2020

Projects

XFire (CrossFire) – Multi-Agent Adversarial Security Review Tool | *Python, CI/CD* Mar 2026

- Built **security tool (PyPI) for automated PR reviews via GitHub Actions**, runs 3 AI agents in parallel blind review to detect vulnerabilities and production-breaking bugs, routes disputed findings via adversarial debate engine.

XSpark – Agentic Pentesting Orchestrator | *Python, CLI, Adversary Emulation* Jan 2026

- Developed a meta-agent pentesting orchestrator that spawns on-the-fly subagents via modular tool adapters, drives testing with a headless browser, and iterates/pivots using confidence scoring; achieved **73% on XBOW benchmarks**.

SecureVibes – AI-Native Multi-Agent AppSec Scanner | *Python, Claude Agent SDK & Skills* Dec 2025

- Contributed to an architecture-aware, multi-agent AppSec scanner; implemented Code-review agent(SAST) and DAST agent/skills to validate SAST findings via dynamic requests, producing lower-noise reports across 11+ languages.

Open Source Contributions

NVIDIA Garak – LLM Red-Teaming Framework | *Contributor (PR #1489)* Nov 2025

- Implemented **BadCharacters probe** to jailbreak LLM with perturbations (ZWS, homoglyphs, BiDi, backspace deletion) using differential evolution, and Levenshtein distance to optimize on the fly and enable reproducible evasion testing.