Harshith Suresh

San Jose, CA | 408-549-4216 | harshiths2004@gmail.com
www.linkedin.com/in/harshith-suresh-056079216/ | https://harshith24.github.io/

EDUCATION

Purdue University **May 2026**
B.S. in Computer Science (Cybersecurity Focus) West Lafayette, IN

SKILLS

- Certifications: AWS Certified Cloud Practitioner, **AWS Solutions Architect Associate**
- Programming: Python, Java, C/C++, Go, SQL, PromQL, Typescript, Bash
- Cloud/Infra: AWS, Azure, Prometheus, Grafana, Docker, Kubernetes, PostgreSQL, MongoDB, InfluxDB, MQTT, Tailscale, Telegraf, Terraform, Ansible, Networking (BGP, OSPF, VLANs, DNS, Subnetting, ZTP, DHCP)
- Cybersecurity: Penetration Testing (Nmap, Nessus, Metasploit, Wireshark), Cloud Security (Azure Defender, IAM, Private Endpoints, NACLs), HITRUST Compliance, Vulnerability Management, Active Directory/Entra ID Security

PROFESSIONAL EXPERIENCE

Software Engineering Intern (Network Infrastructure) **August 2025 – December 2025**
Tesla Inc. Fremont, CA

- Engineered real-time NextJS/React based network topology visualization with live traffic heatmaps and alerts for Tesla's datacenters, factories, retail stores, and Supercharger network, **cutting MTTR** for latency and congestion by **50%**.
- Strengthened **network observability and security audit capabilities** by enhancing scrapers to ingest critical routing tables, VLANs, DNS, ARP, DHCP and BGP data, providing 100% visibility into Tesla's production network state.
- **Accelerated network intelligence** by designing a **RAG** pipeline that reduced complex metric query time by **90%**, enabling non-technical stakeholders to perform instant natural-language audits of network performance.
- **Scaled AI infrastructure** by implementing Zero Touch Provisioning (ZTP) and Grafana based real-time monitoring for NVIDIA Blackwell GPUs, enabling rapid deployment of high-performance compute clusters**.**

Cybersecurity Consultant Intern **June 2025 – August 2025**
Crowe LLP Chicago, IL

- Accelerated **HITRUST certification readiness** for public sector clients by identifying and remediating critical configuration gaps in Active Directory and network architecture.
- Strengthened client security posture by executing comprehensive **penetration tests** and audits against common CVEs, uncovering high-risk vulnerabilities that, once patched, **reduced potential attack surfaces by 60%**.
- Improved consultant productivity by **75%** by automating the deployment of standardized security testing environments using **Ansible and Packer**, reducing setup time from hours to minutes.

Security Engineering Intern **June 2024 - August 2024**
Munich Re New York, NY

- Mitigated data breach risks by engineering an automated **Malware Scanning pipeline** on Azure, ensuring **100% of files** on SFTP servers are isolated and scanned before reaching internal systems.
- Reduced infrastructure deployment errors and improved network isolation by implementing **Infrastructure as Code (Terraform)**, securing sensitive data transfers via **Private Endpoints, IAM policies, and subnetting**.
- Reduced onboarding friction for **6 internal developers** by authoring technical documentation that resolved critical integration gaps between Azure and Terraform, improving deployment velocity.

PROJECTS

Agentic Red Team Framework **February 2026 – Present**
Personal Project West Lafayette, IN

- Designed and built an agentic red team framework that automates reconnaissance, vulnerability discovery, and exploitation against web targets using LLM-driven planning and tool orchestration (Python, **MCP**-style tool integration).
- Developed an intentionally vulnerable Next.js application featuring OWASP-aligned flaws (SSRF, command injection, XSS, IDOR) to validate the red team agent and practice secure coding vs. attack techniques.
- Implemented offensive security tooling in **Go**, including a concurrent TCP port scanner, key logger, and subdomain scanner, and Osint using goroutines and mutexes for fast, low-overhead host discovery in pentest workflows.
- Applied **OWASP Juice Shop** as a practice target for manual and automated testing, reinforcing understanding of OWASP Top 10 and real-world vulnerability chaining.

Geothermal IoT Sensing **January 2026 – Present**
Personal Project West Lafayette, IN

- Engineered a **Pub/Sub** telemetry system using **ESP32** and **DS18B20** sensors to monitor geothermal thermal profiles.
- Developed a real-time data pipeline via **MQTT** and **Telegraf** for secure, high-frequency ingestion into **InfluxDB**.
- Architected a private **Tailscale** mesh network and **Grafana** dashboards to visualize system efficiency and trends.