Saniya Bhaladhare

Email | +1 425-667-3748 | Seattle, WA | Portfolio | LinkedIn | GitHub | Medium

Professional Summary

Cybersecurity engineer with **2+ years of hands-on experience** spanning **AI security**, **GRC**, **product security**, and **DevSecOps**. Built and shipped production **LLM audit tooling** operationalizing 227 controls across **NIST AI RMF** and **ISO/IEC 42001**; led enterprise compliance assessments across 7 regulated financial institutions. Skilled at translating regulatory frameworks into executable engineering controls and risk-informed remediation roadmaps. *(F-1 OPT Eligible)*

Work Experience

AI Security Engineer Intern — Avaly.AI | United States Jun 2025 – Aug 2025

- Architected a **Python/FastAPI LLM Audit Agent** containerized with **Docker** and integrated into **GitHub Actions CI/CD**, operationalizing **227 compliance controls** across **NIST AI RMF** & **ISO/IEC 42001**, reducing manual audit effort by ∼20%.
- Designed a **vendor self-assessment framework** spanning **7 AI trustworthiness domains**, enabling structured evidence validation, **control traceability**, and maturity-based scoring across simulated **GenAI deployment scenarios**.
- Conducted **AI threat modeling** mapping **OWASP LLM Top 10 (2025)** attack vectors (prompt injection, model inversion, data leakage) to **NIST AI RMF** mitigations; translated risk findings into actionable engineering tasks.

Cybersecurity Analyst — KPMG | India Jan 2023 – Jul 2024

- Led **cybersecurity maturity assessments** across **7 RBI/SEBI-regulated financial institutions**, evaluating **70+ controls per engagement** aligned to **NIST CSF**, **ISO 27001**, and regulatory mandates.
- Identified **80+ control gaps** during a large-bank **CSMA engagement**; drove targeted remediation elevating maturity from **2.5** → **3.8** prior to supervisory review.
- Drafted **5 enterprise security policies** (Asset Management, Change Management, BCP/DR, Security Awareness, Tabletop Exercises) aligned to **ISO 27001**; presented risk posture findings to **CISOs** across 7–10-stakeholder sessions.
- Executed **ITGC testing**, **vendor risk assessments**, **IAM configuration reviews**, and **cloud security evaluations** (AWS, Azure, GCP); assessed **QRadar SIEM**, **McAfee DLP**, and **RSA Archer GRC** control effectiveness.

Projects & Leadership

SecurePipe – DevSecOps CI/CD Security Pipeline Mar 2026

- Architected a **GitHub Actions** pipeline with intentionally vulnerable Python services, integrating **Bandit** (SAST), **Semgrep**, **pip-audit** (SCA), and **OWASP ZAP** (DAST) to automate end-to-end **vulnerability detection** on every commit; deployment gates block on critical findings.

InboxGuard – ML-Powered Phishing Detection Tool Apr 2025

- Built **Python**-based **ML security tool** applying heuristic and algorithmic analysis to detect **AI-generated spoofing**, malicious URL behavior, and brand impersonation; achieved **95% detection accuracy** on 10K+ emails, reducing manual triage by **65%**.

President, Women in Cybersecurity (WiCyS) – UW Bothell Student Chapter Aug 2025 – Present

- Leading **8-member executive team** to deliver technical workshops, hackathons, and industry events for **80+ students** across security, AI, and automation topics.

Education

University of Washington Bothell | M.S. Cybersecurity Engineering | GPA: 3.7/4.0 May 2026 (Expected)
Thesis: *30-Control AI Compliance Framework for LLM Deployments (NIST AI RMF & ISO 42001 vs. OWASP LLM Top 10 2025)*

SNDT Women's University, Mumbai | B.Tech, Information Technology | GPA: 3.54/4.0 May 2023

Technical Skills

AI/LLM Security: OWASP LLM Top 10 (2025), **NIST AI RMF**, **ISO/IEC 42001**, prompt injection, model inversion, data leakage, AI threat modeling, GenAI risk assessment

GRC & Compliance: ISO 27001, **NIST CSF**, **NIST RMF**, **SOC 1/2**, **PCI DSS**, **GDPR/CPRA**, **COBIT**, ITGC, TPRM, vendor risk, tabletop exercises

DevSecOps & AppSec: GitHub Actions, **Docker**, **Bandit** (SAST), **Semgrep**, **pip-audit** (SCA), **OWASP ZAP** (DAST), **FastAPI**, cloud security evaluation (AWS, Azure, GCP)

Security Tools: QRadar SIEM, **RSA Archer GRC**, **McAfee DLP**, Burp Suite, Nmap, Nessus, Wireshark, Jira, MS Office

Languages: Python, Bash, PowerShell, HTML/CSS

Certifications & Achievements

Certifications: CompTIA Security+ | **ISO/IEC 27001 Associate** | AWS Certified AI Practitioner *(In Progress)* | Multi-Cloud Red Team Analyst – Cyberwarfare Labs | EC-Council: Network Defense Essentials, Ethical Hacking Essentials

Achievement: CTF Winner – UWB GreyHats (OSINT, cryptography, web exploitation, reverse engineering)