

Saniya Bhaladhare

saniyabhaladhare@gmail.com | saniyabhaladhare.me | linkedin.com/in/saniyb/ | github.com/Sann0311

Professional Summary

Cybersecurity engineer with 1.7 years' experience in AI security, governance, risk, and compliance. Skilled in authoring and automating technology and information-security policies across the policy and controls management lifecycle using NIST AI RMF and ISO 27001. Experienced in AI-driven risk management strategies, vendor assessments, and cloud security controls to enhance enterprise-wide resilience and compliance.

Work Experience

AI Security Engineer Intern, Avaly.AI - United States Jun 2025 – Aug 2025

- Designed and deployed a secure LLM-based audit agent using Dockerized FastAPI, enabling automation of AI risk assessments and reducing manual evidence processing by 60%, aligned with NIST AI RMF.
- Developed dynamic AI security control mappings and threat-informed question flows for automated risk evaluations; aligned with LLM safety practices and improved audit coverage by 10%.

Cybersecurity Analyst, KPMG - India Jul 2023 - Jul 2024

- Led CSMA assessments for 4 banking institutions, identifying 80+ control gaps across five NIST CSF domains and aligning remediation with ISO 27001.
- Presented findings to client CISOs, driving adoption of standardized maturity scoring and improved risk visibility.
- Populated and maintained risk assessment templates and compliance checklists, contributing to ISO 27001 and NIST CSF initiatives.
- Supported adversarial scenario analysis and system hardening exercises, contributing to threat modeling efforts across financial sector clients using NIST CSF and OWASP guidance.
- Created and maintained security control checklists for AWS, Azure, and GCP, ensuring detection of cloud misconfigurations and providing actionable remediation guidance to system owners.

Cybersecurity Intern, KPMG - India Jan 2023 – Jul 2023

- Supported development and refinement of cybersecurity policies and standards, ensuring alignment with organizational risk appetite and international frameworks.
- Validated SOC tool network architecture to identify security gaps and optimize deployment.
- Collaborated with internal and external teams including engineering and compliance to assess risk, align remediation plans, and communicate control effectiveness.

Projects and Leadership

InboxGuard – Phishing Email Analysis Tool Apr 2025

- Built Python-based phishing detection system to flag AI-generated spoofing patterns, malicious URL behavior, and brand impersonation; achieved 98% detection on 10K+ emails and reduced manual triage by 65%.

Keylogger Malware Simulation (Python) May 2024

- Simulated real-world malware TTPs through a keylogger project using Python; implemented anti-forensics, persistence, and selective logging features to test system abuse resilience.

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

- Leading 8-member team to host hackathon and events for 80+ students.

Education

University of Washington Bothell, Bothell, WA Mar 2026 (Expected)
Master of Science in Cybersecurity Engineering | GPA: 3.7/4

Usha Mittal Institute of Technology, SNDT Women's University, Mumbai, India Aug 2019 - May 2023
Bachelor of Technology in Information Technology | GPA: 3.54/4

Technical Skills

Tools: Burp Suite, Kali Linux, Nmap, Nessus, Wireshark, IDA, PowerShell, API Integration, Jira, MS Office, Git, FastAPI, Docker.
Frameworks & Standards: NIST CSF, ISO 27001, MITRE ATT&CK Framework, NIST RMF, OWASP LLM Top 10, COBIT, SOC 1, SOC 2
Core Areas: Vendor Assessment, Tabletop Exercises, Vulnerability Assessment, Security Control Gap Assessment, TPRM, SIEM Alerts, Incident Response, IAM, Secure Configuration, AI/LLM Security.
Languages & Scripting: Python, Bash, HTML/CSS.

Achievements & Certificates

Certifications: CompTIA Security+, AWS Certified AI Practitioner (In-Progress), Multi-Cloud Red Team Analyst by Cyberwarfare Labs, EC-Council CodeRed Series: Network Defense Essentials, Ethical Hacking Essentials, Dark Web.

Achievements: CTF Winner at UWB GreyHats - solved OSINT, cryptography, web-exploitation, and reverse-engineering challenges