

Saniya Bhaladhare

bhaladharesaniya02@gmail.com | saniyabhaladhare.me | linkedin.com/in/saniyb/ | github.com/Sann0311

Professional Summary

Cybersecurity professional with experience in security analysis, risk assessment, and AI-driven security solutions. Skilled in incident response, compliance frameworks, and threat modeling.

Work Experience

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

- Integrated LLM agent with Dockerized FastAPI backend to automate security audit workflows, improving evidence handling and reducing manual review effort by 60%.
- Collaborated with cross-functional teams to map self-assessment forms to NIST AI RMF controls, ensuring comprehensive AI-specific compliance coverage and developed dynamic audit question flows, increasing assessment completion rate by 10%

Cybersecurity Analyst, KPMG - India Jul 2023 - Jul 2024

- Conducted 5+ cybersecurity maturity assessments for public and private sector banks, identifying control gaps and recommending NIST CSF and ISO 27001-aligned remediation plans, raising maturity from 2.4 to 3.7/5.
- Assisted in post-incident root cause analysis for 8+ security events, leveraging IBM QRadar log data, and contributed to drafting 5+ after-action reports to refine SOC playbooks.
- Conducted vulnerability assessments using Nessus, Nmap, and Burp Suite, identifying critical misconfigurations in network devices, firewalls, and third-party integrations, reducing potential security incidents by 25%
- Executed third-party risk reviews and drafted 15 detailed policy and procedure documents, reducing client compliance risk by an estimated 15%.

Cybersecurity Intern, KPMG - India Jan 2023 – Jul 2023

- Validated SOC tool network architecture to identify security gaps and optimize deployment.
- Conducted reconnaissance using Maltego and Kali Linux to map network entities and identify exposures.
- Delivered 5 detailed breach reports with actionable mitigation strategies, improving posture by 20%.

Projects and Leadership

InboxGuard – Phishing Email Analysis Tool Apr 2025

- Built Python/ML phishing detection pipeline to flag sender spoofing, suspicious/shortened links (sandbox URL surf), and brand impersonation; achieved about 98% detection across 10K labeled emails in lab testing and cut manual review volume by >65% via risk scoring & evidence extracts.
- Packaged as a Chrome extension for real-time user protection in corporate email environments.

Keylogger Malware Simulation (Python) May 2024

- Designed a stealth keylogger with persistence, selective logging, and anti-forensics to simulate real attacker TTPs.

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

- Elected President for 2025–26; will launch inaugural hackathon and mentorship programs to boost women’s engagement.

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, Maltego, IDA Freeware, PowerShell, API Integration, MS Office.

Frameworks & Standards: NIST CSF, ISO 27001, MITRE ATT&CK Framework, NIST RMF, OWASP Top 10 for LLM Applications.

Core Areas: Vendor Assessment, Tabletop Exercises, Vulnerability Assessment, Security Control Gap Assessment, TPRM, SIEM Alerts, Incident Response, IAM, Secure Configuration.

Languages & Scripting: Python, Bash, HTML/CSS.

Platforms: TryHackMe (Web Exploitation, Network Security).

Achievements & Certificates

Certifications: CompTIA Security+ (In Progress), AWS Certified AI Practitioner (Target: Aug 2025), EC-Council CodeRed Series: Network Defense Essentials, Ethical Hacking Essentials, Dark Web.

Achievements: CTF Winner at UWB GreyHats.