Saniya Bhaladhare

bhaladharesaniya02@gmail.com | Seattle, WA, 98011 | http://www.linkedin.com/in/saniyb | https://github.com/Sann0311

WORK EXPERIENCE

AI Security Engineer Intern, Avaly.ai – United States (Remote) Jun 2025 – Present
- Designing and improving self-assessment forms to evaluate AI system security against industry best practices.
- Assisting in the creation of tabletop exercises simulating AI-specific security incidents and response planning.
- Supporting threat modeling and risk assessments for GenAI and LLM-powered applications.
- Collaborating on internal documentation efforts, helping to translate complex risks into actionable insights.
- Researching emerging threats in the AI landscape and integrating findings into internal frameworks.

Cybersecurity Analyst, KPMG – Mumbai, India Jul 2023 – Jul 2024
- Implemented ISO 27001 for 3 clients, achieving certifications with zero non-conformities.
- 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.
- Performed NIST CSF assessments for 5 clients, raising maturity from 2.4 to 3.7/5.
- Investigated and resolved 220+ security incidents, maintaining 98% compliance with Reserve Bank of India (RBI) cybersecurity standards; led 7 cross-functional initiatives with a 93% on-time delivery rate.
- Conducted TPRM assessments for 12+ vendors; guided data classification across 6 units, reducing incidents by 15%.
- Performed vulnerability assessments using internal tools and open-source scanners, identifying misconfigurations in network devices, firewalls, and third-party integrations.
- Designed and implemented a cloud security control checklist to assess AWS, GCP, and Azure environments, delivering strategic infrastructure recommendations for a banking client aligned with regulatory standards.

Cybersecurity Intern, KPMG – Mumbai, India Jan 2023 – Jul 2023
- Executed Cyber Security Maturity Assessments for 4 public banks, identifying 85+ control gaps.
- Assisted in creating 25+ ISMS-aligned policy documents, ensuring 90% compliance.
- Validated SOC tool network architecture to identify security gaps and optimize deployment.
- Reviewed and fine-tuned SIEM rules and log reports in IBM QRadar to improve alert accuracy.
- Conducted reconnaissance and footprinting across digital assets before initiating compliance testing.

Cybersecurity Web Dev Intern, Xciteducation Foundations – Remote Feb 2022 – Mar 2022
- 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

InboxGuard - Phishing Email Analysis Tool **Apr 2025**
- Developed a Flask-based phishing detector integrating Google's Gemini API, providing detailed AI-driven email analysis, risk scores, and clear phishing indicators.
- Implemented real-time URL inspection with sandboxed link previews, automatically identifying suspicious domains, insecure connections, and deceptive URLs.
- Designed intuitive frontend with interactive reports, enabling user-friendly phishing awareness through clear explanations and visual risk assessments.

Keylogger Malware Simulation (Python) **Dec 2024**
- Designed a stealth keylogger with persistence, selective logging, and anti-forensics to simulate real attacker TTPs.

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 ATTCK 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).

EDUCATION

University of Washington – M.S. Cybersecurity Engineering Expected Jun 2026
GPA: 3.5/4; Courses: Malware and Attack Reverse Engineering, Ethical Penetration Testing, Secure Software Development.

Usha Mittal Institute of Technology, SNDT Women's University – B.Tech Information Technology Aug 2019 – Aug 2023
GPA: 3.54/4; Courses: Cloud Computing, IoT, Artificial Intelligence, Computer Networks, Cryptography and Network Security.

CERTIFICATIONS

- CompTIA Security+ (In Progress – Expected Jul 2025)
- EC-Council CodeRed: Ethical Hacking Essentials, Dark Web
- Internshala: Ethical Hacking Fundamentals

AWARDS

2nd Place – Gray Hats CTF Apr 2025
Placed 2nd of 45 participants in challenges on cryptography, web exploitation, OSINT, and malware reverse engineering.