Manav Thakkar

Dallas, Texas | manavsutd@gmail.com | 6823718177 | linkedin.com/in/thakkarmanav

Cybersecurity Professional | AI Security Expert | Penetration Testing Specialist | GRC & IAM Specialist

Professional Experience

AI Security Engineer (Emerging Tech), Worldlink US – Frisco, TX — Nov 2024 - Present

- Improved security for LLM chatbot development by 35%, reducing AI hallucinations, prompt engineering attacks, and training data poisoning
- Led AI Red Teaming and PenTesting operations for internal systems, increasing overall risk posture by 40%
- Researched and presented emerging AI vulnerabilities, solutions, and market trends around GenAI security for executive stakeholders

AI Governance & Data Privacy Consultant, CG Infinity – Plano, TX — May 2024 - Oct 2024

- Implemented data handling protocols compliant with EU AI Act and NIST AI RMF in OneTrust and BigID, improving client AI security
- Spearheaded NIST CSF Assessment achieving 48% risk reduction for enterprise client
- Provided technical leadership using secure GenAI tools to identify malicious activity through ML models and automation

Cyber Security Specialist, DigitalXForce – Southlake, TX — May 2023 - May 2024

- Conducted advanced log analysis and network penetration testing, resolving 50+ security issues and increasing organizational security by 30%
- Performed pen testing for GRC generators, identifying and fixing 50+ vulnerabilities with 30% product improvement
- Executed in-depth hardware security assessments through reverse engineering and controlled attack simulations
- Developed working autonomous car and health monitoring prototypes to demonstrate IoT security vulnerabilities

Cyber Security and IAM Consultant, Inkwood Research – India — Sep 2021 - Nov 2022

- Delivered scalable Active Directory and Intune policy solutions, significantly improving endpoint security
- Conducted white box penetration testing on cloud applications, identifying critical vulnerabilities
- Provided expert guidance on OWASP Top 10, SANS 25, and MITRE ATT&CK frameworks
- Designed custom proof-of-concept attack prototypes to demonstrate security gaps to clients

Education

Master of Science, Cybersecurity, The University of Texas at Dallas — 2022 - 2024

Bachelor of Technology, Computer Engineering, K.J. Somaiya Institute of Technology — 2018 - 2022

Technical Skills

Security Frameworks: NIST CSF/RMF/AI RMF, SOC 2, ISO 27001, EU AI Act, GDPR, CCPA, FedRAMP

Security Tools: OneTrust GRC, BigID, Burp Suite, Wireshark, Nmap, Metasploit, ZScaler, Service Now

Specializations: AI/LLM Security, Penetration Testing (VAPT), Network Security, Risk Mitigation, Incident Response, AWS IAM, Active Directory, MFA, Malware Analysis, Ethical Hacking

Certifications & Publications

IEEE-ICAST 2022 Research Publication – WiFi Deauth and Cloning using ESP8266 (ID: CS_122) — 2022

IBM Security Analyst Certification – https://www.credly.com/badges/44982782-3ba1-43e7-8170-e6220ec0b5af/linked$_{i}n_{p}rofile$ — 2020