Dr. Anya Arora
anya.arora@cyberguardians.com

713-888-9999

Texas

Summary

Visionary and highly accomplished Principal Cybersecurity Architect with over 20 years of experience leading complex security initiatives for global enterprises, specializing in **AI/ML security, threat intelligence, and large-scale enterprise security architecture**. Possesses a unique blend of deep technical expertise, strategic leadership, and academic rigor in securing advanced technological landscapes. Proven ability to design and implement robust security frameworks, develop proactive defense strategies against sophisticated cyber threats, and build high-performing security teams.

Experience

Chief AI Security Architect Cognitive Defense Solutions Houston, TX 2020 - Present

- Established and led the industry's first dedicated **AI Security department**, developing a comprehensive framework for securing Machine Learning models against adversarial attacks (data poisoning, model evasion) and ensuring the integrity of AI pipelines.
- Designed and implemented a **Confidential AI Computing platform leveraging homomorphic encryption and federated learning** to enable secure data collaboration and model training across sensitive datasets without exposing raw data.
- Developed novel threat intelligence methodologies integrating AI-driven anomaly detection and predictive analytics to identify zero-day exploits 6 months faster than traditional methods.
- Architected and deployed a secure MLOps (Machine Learning Operations) pipeline, ensuring security controls are embedded from data ingestion to model deployment and monitoring.
- Published over 15 peer-reviewed papers on AI security and privacy-preserving AI, positioning the company as a thought leader in the field.
- Directed security audits and penetration testing specifically tailored for AI systems, identifying and remediating critical vulnerabilities.

Principal Cybersecurity Architect Global CyberSafe Corp. Dallas, TX 2012 - 2020

- Led the design and implementation of enterprise-wide cybersecurity architecture for a Fortune 100 financial institution, overseeing security for over 100,000 endpoints and critical data assets.
- Developed and enforced security policies and standards (NIST, ISO 27001, GDPR) across on-premises, cloud (AWS, Azure), and hybrid environments.
- Spearheaded the adoption of advanced threat detection and response capabilities, including SOAR (Security Orchestration, Automation, and Response) and EDR (Endpoint Detection and Response) systems.
- Built and managed a 24/7 Security Operations Center (SOC) team, significantly improving incident response times and reducing breach impact.
- Implemented Zero Trust Network Architecture (ZTNA) across the enterprise, enhancing access control and reducing attack surface.

Senior Security Consultant Secure Solutions Texas Austin, TX 2005 - 2012

- Provided expert cybersecurity consulting to diverse clients, ranging from healthcare to technology sectors.
- Conducted comprehensive security assessments, penetration tests, and vulnerability management programs.
- Developed incident response plans and provided tabletop exercise facilitation.
- Designed and implemented SIEM solutions (Splunk, QRadar) for real-time security monitoring and log analysis.

Education

Ph.D. in Computer Science (Specialization in Cybersecurity & AI) University of Texas at Austin Austin, TX 2005

Master of Science in Cybersecurity Texas A&M University College Station, TX 2002

Bachelor of Science in Electrical Engineering Rice University Houston, TX 2000

Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Cloud Security Professional (CCSP)

- Offensive Security Certified Professional (OSCP)
- Certified Machine Learning Engineer (Google Cloud / AWS equivalents)

Niche Skills:

- **AI/ML Security & Adversarial AI:** Expertise in understanding and defending against attacks specifically targeting AI models and data (e.g., data poisoning, model evasion, model extraction) and ensuring the trustworthiness and ethical deployment of AI systems. This is a highly specialized and emerging field.
- **Confidential AI Computing (Homomorphic Encryption, Federated Learning):** Deep knowledge and practical experience with advanced cryptographic techniques that allow computations to be performed on encrypted data, and distributed machine learning approaches that train models on decentralized datasets without exchanging raw data, crucial for privacy-preserving AI.
- **Secure MLOps & AI Governance:** The ability to embed security controls and governance policies throughout the entire machine learning lifecycle, from data collection and model training to deployment, monitoring, and retraining, ensuring secure and compliant AI systems.