Hemangi Ahir

726-209-1852| hemangi2396@gmail.com |https://www.linkedin.com/in/hemangi-ahir/|https://github.com/HemangiAhir| Richmond, VA, USA (Relocating to CA)

Introduction

Cybersecurity professional focused on OT/ICS, hardware, firmware, and cloud environments. Enthusiastic about advancing into penetration testing and exploring AI-driven security solutions. Comfortable reading and writing basic Python scripts for automation and analysis. Well-versed in threat modeling, risk mitigation, NIST, ISO 27001, and IEC 62443 frameworks, with a constant drive to deepen offensive security skills and stay ahead of evolving threats.

Professional Experience

AI FOR ZERO-TRUST POLICY OPTIMIZATION: TOWARDS INTELLIGENT ACCESS CONTROL IN MODERN NETWORKS

Research Project, Richmond, VA | Oct 2025-Present

- Created a next-generation security system that learns optimal access policies from network behavior, achieving measurable improvements in threat detection and operational efficiency. Leveraged Claude AI as a development partner to rapidly prototype and implement production-grade machine learning code, demonstrating effective human-AI collaboration in building complex security infrastructure.

CYBERSECURITY SPECIALIST

Schneider Electric, Richmond, VA | Apr 2024-Present

- Conducted threat modeling, risk assessments, and vulnerability scans for OT/ICS environments; identified misconfigurations on Cisco switches using SolarWinds Orion and drove remediation of high-risk findings.
- Implemented Sepio Hardware Access Control (L1/physical layer) to detect and block rogue devices
- Designed and managed secure sandbox environment for shift-left security testing and hardened configuration of OT tools.
- Managed Palo Alto Panorama for centralized NGFW policy and zone-based segmentation in OT networks
- Enforced identity-based micro-segmentation and zero-trust policies using Elisity Dynamic Edge Segmentation in converged IT/OT environments.
- Deployed and tuned Claroty xDome for real-time OT asset discovery, network visibility, anomaly detection, and incident response.
- Developed global OT security policies and incident response playbooks.

TECHNOLOGY INTEGRATION SPECIALIST & TELECOM AND NETWORKING TA

UTSA, San Antonio, Texas | Sep 2022-Mar 2024

- Mentored 60+ undergraduate students in telecommunications and networking courses, guiding hands-on lab assessments including Cisco network configuration, VMware ESXi deployment, and virtual lab environments
- Designed and delivered practical Bluetooth protocol and wireless networking labs, resulting in 90% of students reporting significantly improved real-world skills
- Prepared women-in-cybersecurity cohort for CompTIA Security+ certification, achieving a 95% first-attempt pass rate
- Provided one-on-one technical support, debugged student lab issues, graded assignments/projects, and enforced consistent lab standards

NCAEC CYBER GAMES PARTICIPATION

UTSA, San Antonio, Texas | Feb 2024

- Participated in NCAEC Cyber Games, a Capture The Flag (CTF) competition, demonstrating cybersecurity skills on Linux systems: teamwork, problem-solving, and practical application of tools in diverse challenges.

WIRESHARK PACKET SNIFFER

UTSA, San Antonio, Texas | Sep 2023

- Developed a packet sniffer that reads Wireshark PCAP files to distinguish between malicious and benign network traffic per frame.

INSIDE PRODUCT SPECIALIST

Dell, Panama City, Panama | Nov 2018-Dec 2021

- Delivered pre-sales technical support to Latin American B2B sales teams, specializing in enterprise warranty,

ProSupport, and SLA solutions
- · Consulted directly with clients and channel partners to recommend optimal service contracts, driving higher win rates and deal sizes
- · Maintained expert-level knowledge of Dell's server, storage, and networking portfolio to strengthen customer relationships and brand trust

Technical Skills
- · Security Tools: Claroty xDome, Sepio, Elisity, Armis xSA, Palo Alto Panorama, SolarWinds Orion, Wireshark, Metasploit, Hashcat, John the Ripper, Flipper Zero
- · Platforms & Cloud: Windows, Linux, Google Cloud Shell
- · Frameworks: NIST 800-53, IEC 62443, ISO 27001, MITRE ATT&CK
- · Programming: Python (scripting & automation)
- · Hardware/OT: Raspberry Pi, Flipper Zero, Wireless Wi-Fi Adapter

Certifications
- · CompTIA Security+ COMP001022455481 – Mar 2024
- · Generative AI: Boost Your Cybersecurity Career – IBM - UX3GIOKJS5L2
- · Google Certificate: Introduction to Security Principles in Cloud Computing
- · Preparing for CEH

Education
MS-IT Cybersecurity | Dec 2023 | University of Texas at San Antonio

Bachelor's in Industrial Engineering | Apr 2019 | USMA Panama