Nicholas Massei

nikofmassei@gmail.com • (918) 209-0667 • LinkedIn Profile • CyberClarityHQ (Portfolio & Blog)

Education

Northeastern State University, *B.S. in Cybersecurity* Broken Arrow, OK, Aug 2024 - Present

Coursework – Information & Network Security, System & Network Admin, Pen. Testing, Log Analysis, TCP/IP

Tulsa Community College, *A.S. in Enterprise Development* Tulsa, OK, May 2022 – May 2024

Coursework – Data Analysis, Python, MS Office, Algorithms & Statistics, IT Infrastructure

Work Experience

Grainger, *Branch Sales Associate* Tulsa, OK, Apr 2024 – Present

- Provide excellent support to customers while maintaining positive metrics by providing efficient service.
- Utilize critical thinking throughout daily operations to troubleshoot operational and service challenges.
- Led return processing to introduce effective solutions that streamlined high-volume workflows and service
- Collaborate with team members to identify bottlenecks to streamline processes, increasing order fulfillment time

Dr. Lisa AI, *Cybersecurity Intern* Hybrid, August 2025 – Present 2025

- Collaborated with the CTO to lead research projects for security risks in AI/LLM deployments and for example tech stacks, proposing effective mitigation strategies for client systems.
- Gained experience implementing security controls in mock AI models, focusing on data integrity, model resilience, and access management.
- Produced internal documentation and reports that translate complex AI security controls into actionable controls and guidance for technical and non-technical stakeholders.

Certifications

- CompTIA Security + (SY0-701) – May 2025
- CompTIA Network + (N10-009) – June 2025
- Google Cybersecurity Certificate – Sep 2025
- Blue Team Level 1 (Security Blue Team) – Sep 2025

Select Projects

Phishing Analysis - Used phishing emails through open-source datasets and used Sublime Text to extract email artifacts, identify IOCs, and triage phishing emails for reporting and analysis.

Vulnerability Assessment - Conducted assessments of Windows and Linux machines for reporting, while performing system and network remediation efforts, including wireless network configuration

Splunk Investigation - Efficiently investigated malicious activity across multiple indexes using Splunk, correlating logs and identifying indicators of compromise to support incident response.

Skills Summary

Tools: Splunk, Wireshark, Wazuh, Shuffle, ZAP, Autopsy, PowerShell, Python, Nmap, VirtualBox, TheHive, Volatility
Skills: Threat Hunting, Log Analysis, Incident Response, Pen Testing, Vulnerability Assessment, System Hardening