Austin A. DeFrancesco

Cleveland, Ohio, US austin@defcesco.io in/austin-defrancesco defcesco.io

EXPERIENCE

Team Lead | Cleveland Clinic | Cleveland | September 2021 - Present

- Led team collaboration with 6 detection engineers and threat hunters for **threat detection**, trend analysis, and incident investigation. Established formalized **detection-as-a-service** program using MITRE ATT&CK framework and **detection lifecycle** methodologies for enterprise healthcare.
- Engineered and automated **detection-as-code pipelines** (Azure CI/CD/DevOps) using a **Python-based content manager** with multi-cloud authentication to deploy detection rules and **SOAR playbooks**.
- Served as Google Customer Advisory Board member on MCP implementations, onboarded team to **AI-driven** SOAR and SIEM practices.
- Performed **vulnerability research**, threat modeling, and exploit development for enterprise applications using Binary Ninja, WinDBG, Wireshark, BooFuzz, Angr's CLE, and Unicorn Engine (**CVE-2024-25003, CVE-2024-25004, CVE-2024-23749**).
- Conducted **attack simulations** and **purple teaming** across enterprise infrastructure, medical devices, and IoT systems using Cobalt Strike.

Cybersecurity Engineer | OMNI Systems | Cleveland | January 2019 - January 2021

- Led security operations in critical infrastructure. Implemented enterprise security technologies including **PKI**, hardening and **SIEM** systems.

Researcher | VividHex | Pittsburgh | September 2020 - December 2020

- Researched phishing threat detection methodologies and developed malware analysis tooling using **AWS**, **GCP**, **Python**, **TensorFlow**, and **Docker**.

Technical Summer Associate, Security, Privacy, Risk & Compliance | RSM | Cleveland | May 2017 - August 2019

- Performed **penetration testing** and security evaluations for enterprise clients, engineered internal security tools for driver analysis and testing infrastructure, and developed King Phisher plugin while maintaining 20+ wiki pages across security tool documentation.

INVOLVEMENT

VECTR Advisory Board Member | Philadelphia | Security Risk Advisors (SRA) | March 2025 - Present

Detection Engineering Special Interest Group Founder |
Cleveland | North East Ohio Cybersecurity Consortium (NEOCC) | September 2021 - Present

Presenter & Member | Cleveland | CLEpy | January 2021 - Present

AWARDS & HONORS

Second Place | North East Ohio Cybersecurity Consortium | 2024

First Place | North East Ohio Cybersecurity Consortium | 2023

- Stored XSS, Redis Cache Poisoning, and Pickle Deserialization RCE in the NEOCC Capture the Flag Tournament.

PUBLICATIONS & TALKS

Tripwires Trigger Change: How Detection Engineering Elevates Cybersecurity | Cleveland Clinic ConsultQD | 2025

Detection Engineering at International Scale & Geopolitical Ramifications on Domestic Entities | Talk |
North East Ohio Cybersecurity Consortium Best Practices & Threat Sharing Round Table | 2025

Detection Engineering: CI/CD Driven Defense | Talk | Cleveland Area Python User Group (CLEpy) | 2025

Supply Chain Attacks on Hospitals & Critical Vendors | Talk | Health & Personal Care Logistics Conference | 2024

EDUCATION

BA Administration of Justice, Cyber Crime | University of Pittsburgh | Pittsburgh, PA | 2016 - 2020

Technical InfoSec Courses | DePaul University | Chicago, IL | 2015 - 2016

High School Diploma | University School | Hunting Valley, OH | 2015