John K. DeMarzo

TARGETING SOC ANALYST / DETECTION & IDENTITY ROLES — AUSTIN–SAN ANTONIO OR REMOTE

New Braunfels, TX | 512-227-1837 | jdemarzo@gmail.com | linkedin.com/in/j-demarzo | github.com/j-demarzo | demarzo.dev

PROFESSIONAL SUMMARY

Cybersecurity graduate (UTSA, Aug 2026) and CompTIA Security+, CySA+, PenTest+, and Network+ certified professional transitioning from public-safety operations into security operations. Hands-on lab work spans SIEM detection engineering, network segmentation, packet and alert review, cloud honeypot monitoring, and hybrid Active Directory / Entra ID identity administration.

Brings structured incident triage, escalation, documentation, and after-action review discipline from time-critical emergency response. Available now.

Security monitoring experience is lab-based, not commercial SOC employment.

CERTIFICATIONS & EDUCATION

CompTIA Security+ (SY0-701) · CySA+ ce (CS0-003) · PenTest+ ce (PT0-003) · Network+ ce

Google Cybersecurity Professional Certificate (2024) · AWS Cloud Support Associate Professional Certificate (2024) · CISA 100W ICS Cybersecurity Practices (2026)

BBA, Cybersecurity — The University of Texas at San Antonio Awarded Aug 2026

GPA 3.84

AS, Computer Information Systems — San Antonio College Awarded Aug 2024

TECHNICAL SKILLS

Security operations & monitoring: Splunk and Wazuh local deployments; Snort alert review; Zeek, Suricata, tshark, Wireshark; SANS Internet Storm Center log review; DShield and Cowrie honeypots; Nmap.

Identity & access: Hybrid Active Directory / Microsoft Entra ID; Entra Connect sync; Conditional Access, MFA, Identity Protection, PIM; access governance.

Network defense & infrastructure: Seven-VLAN segmentation; TP-Link Omada SDN; Proxmox SDN; firewall access rules; OPNsense and UFW; DHCP/DNS; Proxmox VE; AWS EC2 and security groups.

Systems & methods: RHEL, Ubuntu, Windows 10/11; Bash; Ansible lab playbooks; NIST and SANS incident-response guidance; MITRE ATT&CK; technical reporting.

OT/ICS lab exposure: Modbus/TCP, DNP3, OPC UA, BACnet; PLC/RTU register reads; IT/OT segmentation and zone-and-conduit concepts.

TECHNICAL PROJECTS & SECURITY LABS

Enterprise Homelab — SOC & Detection Engineering 2023 – Present

github.com/J-DeMarzo/enterprise-homelab

- Segmented a seven-VLAN Proxmox environment with Splunk as the SIEM — Sysmon, Windows, DNS, and firewall log onboarding — plus an isolated attack VLAN with Linux targets, to run the full SOC loop: emulate, detect, investigate, document.
- Verified default-deny firewall isolation between VLANs with before/after testing; documented architecture, design decisions, and SPL detections as code. Status: first attack-to-case write-ups in progress.

SC-300 Identity Lab — Hybrid Entra ID 2026 – Present

github.com/J-DeMarzo/sc300-identity-lab

- Built a hybrid identity lab on an isolated Proxmox software-defined network: on-premises Active Directory synced to Microsoft Entra ID, with staff signing in as @demarzo.dev.
- Scoped for Microsoft SC-300 exam coverage — Conditional Access, MFA, Identity Protection, PIM, and identity governance. Status: network layer in progress.

Cloud Honeypot Deployment & Security Monitoring Spring 2025

- Deployed Ubuntu Server 22.04 in AWS EC2 with DShield and Cowrie sensors; validated service status, log paths, firewall rules, and reporting workflows.
- Restricted administrative SSH to one approved source IP and a nondefault port via AWS security groups; reviewed SANS Internet Storm Center submissions and documented scanning observations.

OT/ICS Network Security & Protocol Analysis Summer 2026

- Reviewed Zeek, Suricata, tshark, and Grafana evidence for reconnaissance and anomalous industrial-protocol activity in

controlled lab environments; documented Modbus/TCP state changes, process restoration, and mitigation priorities.

PROFESSIONAL EXPERIENCE

Texas State University — ALERRT Program
Feb 2017 – Dec 2024

Contract Instructor / Lead Instructor / Subject Matter Expert — national active-attack integrated-response training program serving multidisciplinary public-safety audiences.

- Delivered repeatable response training for classes typically ranging from 15–30 participants by facilitating scenario-based exercises and adapting instruction to operational and safety requirements.
- Coordinated instructor teams on approximately 40% of assignments as Lead Instructor; developed and delivered 20+ scenario-based exercises and incorporated performance feedback into course delivery.

Bexar County ESD #12 Fire / Rescue
Sep 2019 – Aug 2023

Engineer / Lieutenant / Acting Captain — fire/rescue agency providing time-critical emergency response, multi-station readiness, and mutual-aid operations.

- Directed response and resource prioritization across two stations as Acting Captain, coordinating 5–7 personnel and 7–9 apparatus by applying incident command and clear operational communications.
- Improved inspection visibility for PPE assigned to 40+ personnel by administering PS Trax checks and accountability workflows; reviewed incident records and facilitated after-action reviews to inform procedures.

Hays County ESD #3 — South Hays Fire
Oct 2011 – Jun 2022

Training Captain / EMT — combination fire/rescue organization supporting response, training, personnel readiness, and mutual aid.

- Increased training attendance, hands-on engagement, and learner retention by 150% over one year, measured through participant counts and retention surveys, by introducing blended onboarding and structured mentoring.
- Supported classes of 15–30 and up to 80 members through Moodle, Pearson, IFSTA, and FireRescue1 training workflows; documented plans, SOPs, and operational reports.

ADDITIONAL EXPERIENCE

JM Electronic Engineering, Inc. — Senior Service Technician / Installation Supervisor
May 2012 – Sep 2017

Programmed, tested, and troubleshot commercial fire-alarm systems and IP/cellular monitoring links.

Texas Fire Academy — Lead Fire Instructor / EMS Instructor
Jan 2013 – May 2021

Delivered practical training and documented after-action findings.

Massachusetts Army National Guard — Cannon Crewmember (13B), Specialist (E-4)
Feb 2001 – Dec 2007

Planned and reviewed time-sensitive security-detail missions; honorable discharge.

1 Beyond, Inc. — Systems Engineer / Tech Support Lead
Nov 2002 – Jun 2004

Configured mobile workstations and troubleshot client systems on location.