TIMOTHY CORRADO

TimothyCorrado@gmail.com | (402) 649-8672 | LinkedIn | GitHub

SUMMARY

Security+ certified cybersecurity analyst with hands-on experience in cloud-leaning SOC workflows, identity attack surface analysis, detection engineering, and security automation. Built Azure-aligned labs, CI-driven security pipelines, and identity enumeration tooling. Strong foundation in log analysis, network segmentation, and incident triage. Targeting Cloud SOC / Security Operations roles.

TECHNICAL SKILLS

- **Cloud & Identity:** Azure fundamentals (AZ-900), identity attack surface analysis, account lifecycle risk
- **SIEM & Detection:** Wazuh, Splunk, Sysmon, Windows Event Logs (4624/4625), MITRE ATT&CK mapping
- **Network Security:** pfSense, firewall rule enforcement, segmentation, Wireshark
- **Automation & DevSecOps:** Python, PowerShell, GitHub Actions (CI security validation workflows)
- **Systems:** Windows, Linux

PROJECT EXPERIENCE

Identity Attack Surface Analysis

GitHub: github.com/TimothyCorrado/identity-attack-surface

- Developed Python automation to enumerate identity exposure and simulate adversarial reconnaissance.
- Generated structured security artifacts to support defensive remediation planning.
- Demonstrates cloud-relevant identity risk awareness and attack surface mapping.

Security Automation & CI Pipeline

GitHub: github.com/TimothyCorrado/small-biz-cybersecurity-toolkit

- Built daily GitHub Actions workflow generating SOC-style validation reports.
- Automated repository security checks and lightweight secret scanning aligned with DevSecOps practices.

Mini SOC Detection Lab

GitHub: github.com/TimothyCorrado/mini-soc-detection-lab

- Analyzed Windows and Sysmon telemetry to detect authentication anomalies.
- Performed SOC-style alert triage mapped to MITRE ATT&CK techniques.

Network Segmentation & Firewall Lab

- Implemented least-privilege firewall policies and validated restricted lateral movement via log analysis.

PROFESSIONAL EXPERIENCE

Technical & IT Roles | 2013–2020

- Supported account provisioning and access control processes aligned with security policies.
- Maintained audit-ready documentation of system and access changes.

Sergeant (E-5) | U.S. Marine Corps | 2016–2024

- Led mission-critical system operations under strict procedural compliance.
- Applied structured decision-making and incident response mindset in high-pressure environments.

Security-Sensitive Roles | 2022–2026

- Managed confidential financial and healthcare data under compliance standards.
- Identified workflow risks and reinforced data protection practices.

EDUCATION & CERTIFICATIONS

- B.S. Computer Science – University of Nebraska at Kearney
- CompTIA Security+ (SYO-701)
- Microsoft Azure Fundamentals (AZ-900) – In Progress