TIMOTHY CORRADO

Omaha, NE | TimothyCorrado@gmail.com | (402) 649-8672 | linkedin.com/in/timothy-corrado | github.com/TimothyCorrado

PROFESSIONAL SUMMARY

Security+ certified cybersecurity analyst skilled in log analysis, firewall policy enforcement, Windows event monitoring, SIEM workflows, and incident triage. Hands-on experience building a mini SOC detection lab using Windows Security Logs, Sysmon, and Splunk, along with a pfSense firewall lab enforcing least-privilege access and network segmentation. Former U.S. Marine with strong discipline, communication, and operational reliability. Actively seeking a SOC Analyst or IT Security Engineer I role.

CORE SKILLS

Blue Team Tools: Splunk, Wazuh, Sysmon, Wireshark, pfSense | **SOC:** Alert triage, MITRE ATT&CK, detection engineering, incident documentation | **Logs:** 4624/4625, Sysmon ID 1 | **OS:** Windows, Linux | **Scripting:** Python, PowerShell | **Network Security:** Firewall policy design, least-privilege access, network segmentation

FEATURED PROJECTS | *Full Portfolio: github.com/TimothyCorrado*

PfSense Firewall & Network Segmentation Lab
GitHub: https://github.com/TimothyCorrado/small-biz-cybersecurity-toolkit/tree/main/siem-labs/firewall-lab
Tools: pfSense, VirtualBox, Windows 10, TCP/IP, Firewall Logs

- Deployed and configured a pfSense firewall enforcing least-privilege outbound network access.
- Removed default permissive rules and implemented explicit allow rules for DNS, ICMP, and web traffic.
- Validated firewall policy enforcement by generating authorized and unauthorized traffic and reviewing firewall logs.
- Implemented internal network segmentation to restrict lateral movement between security zones.
- Verified segmentation by confirming blocked host-to-host communication across internal networks.

Mini SOC Detection & Windows Event Monitoring Lab
GitHub: github.com/TimothyCorrado/mini-soc-detection-lab
Tools: Wazuh SIEM, Windows 10, VirtualBox, MITRE ATT&CK, PowerShell, Python, Sysmon, HTML Dashboard

- Reviewed Windows security and authentication events to identify authentication failures and anomalous behavior.
- Correlated endpoint logs with simulated security scenarios to support SOC-style triage.

Small Business Cybersecurity Assessments
GitHub: github.com/TimothyCorrado/small-biz-cybersecurity-toolkit/assessments
Tools: PowerShell, Python, Windows 10, Google Sheets, Command Prompt

- Assessed network, Wi-Fi, endpoint security, access controls, backups, and physical security.
- Identified high-risk issues such as shared accounts, lack of MFA, exposed RDP, and weak backup strategies.
- Produced executive-friendly Markdown & PDF reports with severity-based findings and clear remediation steps.
- Built reusable SMB assessment templates, checklists, and severity logic for consistent evaluations.

PROFESSIONAL EXPERIENCE

Technical & IT Roles | *C&A Industries, Daycos, Northeast Community College | 2013–2020*

- Performed technical troubleshooting and incident handling for employee access requests.
- Documented account changes and maintained audit-ready records to support compliance.
- Resolved user issues efficiently using ticketing systems, contributing to organizational security posture.

Heavy Equipment Mechanic (Sergeant, E-5) | *U.S. Marine Corps | 2016–2024*

- Led teams maintaining mission-critical systems, emphasizing reliability, security, and procedural compliance.
- Built strong situational awareness and fast decision-making—directly useful for SOC triage and incident response.
- Trained Marines in troubleshooting, documentation, and operational safety — transferable to IT incident response.

Other Experience | *Mutual of Omaha, Alliance Medical Staffing, Lyft, Family Heritage | 2022–2026*

- Analyzed data and workflows to identify risks and ensure compliance.
- Managed confidential healthcare data under HIPAA standards.
- Handled contracts and financial data securely.
- Educated clients on policy risks and privacy.

EDUCATION & CERTIFICATIONS

Bachelor of Science in Computer Science – *University of Nebraska at Kearney | 2020*
Associate of Science in Computer Science – *Northeast Community College | 2016*
CompTIA Security+ (SYO-701) – *Earned November 2025*
Microsoft Azure Fundamentals (AZ-900) – *In Progress*