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, detection engineering, Windows event monitoring, SIEM workflows, and incident triage. Hands-on experience building a 7-day mini SOC detection lab using Windows Security Logs, Sysmon, and Splunk SIEM, plus a custom Windows Event Monitor & Analyzer for authentication analysis. Currently doing SMB assessments as well for real world application experience. Former U.S. Marine with exceptional discipline, communication, and reliability. Actively seeking a SOC Analyst role to apply blue-team skills and grow within a cybersecurity team.

CORE SKILLS

Blue Team Tools: Splunk, Wazuh, Sysmon, Wireshark | **SOC:** Alert triage, MITRE ATT&CK, detection engineering, incident documentation | **Logs:** 4624/4625, Sysmon ID 1 | **OS:** Windows, Linux | **Scripting:** Python, PowerShell

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

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.

Mini SOC Detection Lab

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

Tools: Wazuh SIEM, Sysmon, Windows 10, VirtualBox, MITRE ATT&CK

- Built a 7-day SOC lab using Windows Security Logs, Sysmon, and Splunk for end-to-end detection workflows.
- Onboarded Windows + Sysmon logs into Splunk and validated sourcetypes, indexing, and key event visibility.
- Created SPL detections for failed logons, success-after-failure patterns, and suspicious processes (MITRE T1110).
- Simulated authentication activity, triaged alerts, and delivered a SOC investigation report with recommendations.

Windows Event Monitor & Analyzer

GitHub: github.com/TimothyCorrado/Windows-Event-Monitor-Analyzer

Tools: PowerShell, Python, Sysmon, Windows Event Logs, HTML Dashboard

- Parsed Event IDs 4625 and 4624 to identify failed logons, successful logons, and suspicious sign-in patterns.
- Integrated Sysmon logs to track process creation, command-line arguments, and network connections.
- Generated HTML summary reports of log activity with timestamps, user accounts, and alerting indicators.
- Correlated event logs during simulated RDP brute force behavior to validate detection accuracy.

PROFESSIONAL EXPERIENCE

Technical & IT Roles | *C&A Industries, Daycos, Northeast Community College | 2013–2016*

- 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 | 2016–2022*

- 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 | 2022–2025*

- 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 Omaha*

Associate of Science in Computer Science – *Metropolitan Community College*

CompTIA Security+ (SYO-701) – *Earned November 2025*