

# TIMOTHY CORRADO

Omaha, NE | TimothyCorrado@gmail.com | (402) 649-8672 | [linkedin.com/in/timothy-corrado](https://linkedin.com/in/timothy-corrado) | [github.com/TimothyCorrado](https://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 mini SOC environment with Wazuh, Sysmon, and Windows Security Logs. Strong ability to identify failed authentication patterns, correlate events, and map activity to MITRE ATT&CK. 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:** Wazuh, Sysmon, Wireshark | **SOC:** Triage, MITRE, Detection Eng. | **Logs:** 4624/4625, Sysmon ID 1 | **OS:** Windows, Linux | **Scripting:** Python, PowerShell

---

## FEATURED PROJECTS | Full Portfolio: [github.com/TimothyCorrado](https://github.com/TimothyCorrado)

### Windows Event Monitor & Analyzer

GitHub: [github.com/TimothyCorrado/Windows-Event-Monitor-Analyzer](https://github.com/TimothyCorrado/Windows-Event-Monitor-Analyzer)

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

- Designed and built a Windows event log analyzer to detect authentication anomalies and process activity.
- 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.

### Mini SOC Detection Lab (In Progress)

GitHub: [github.com/TimothyCorrado/mini-soc-detection-lab](https://github.com/TimothyCorrado/mini-soc-detection-lab)

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

- Building a 7-day mini SOC using Windows logs, Sysmon, and Wazuh SIEM to practice detection engineering.
- Creating detection rules for failed logons, brute-force activity, suspicious PowerShell usage, and privilege escalation.
- Simulating attacker behavior to trigger alerts and analyze triage data inside Wazuh.
- Mapping findings to MITRE ATT&CK techniques and producing SOC-style triage notes and incident reports.

### PowerShell Log Parser (Mini Project)

- Parsed Event ID 4625 logs and summarized failures by username and source IP.
  - Generated CSV triage output and mapped activity to MITRE T1110.
- 

## PROFESSIONAL EXPERIENCE

### Technical & IT Roles | C&A Industries, Daycos, Northeast Community College | 2015–2019

- 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, TJC Property Group, Family Heritage | 2020–2025

- 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