Nicholas Garcia

Aspiring Security Analyst | Cybersecurity Student | Hands-On Defensive Skills

Baytown, TX • (713) 516-3528 • Nich7.garcia@gmail.com

GitHub Portfolio: https://github.com/Nich-Garcia/cybersecurity-portfolio

Professional Summary

Motivated and detail-oriented cybersecurity student transitioning from a strong background in construction, risk management, and field leadership. Experienced in system hardening, log analysis, Linux administration, security auditing, incident documentation, and hands-on defensive projects. Demonstrates excellent problem-solving, communication, and analytical skills. Actively building technical capabilities through coursework, homelab projects, and practical security labs. Seeking a Security Analyst or SOC Analyst I role to apply growing cybersecurity skills.

Technical Skills

- • Security Auditing (NIST CSF, PCI DSS, SOC, GDPR basics)
- • Linux Administration & File Permissions
- • SIEM Platform Familiarity (Splunk, Chronicle)
- • Log Analysis & Event Correlation
- • Network Fundamentals (TCP/IP, Ports, Firewalls)
- • Python Scripting for Automation
- • SQL for Security Filtering & Analysis
- • Incident Documentation & Reporting
- • Risk Assessment & Vulnerability Identification
- • Version Control with Git & GitHub

Tools & Technologies

- • Linux (Ubuntu, Kali)
- • Windows 10/11 Admin Tools
- • Wireshark
- • Nmap
- • Splunk / Chronicle SIEM
- • VirtualBox
- • Python 3
- • Nessus Essentials
- • Burp Suite (Beginner Familiarity)
- • MITRE ATT&CK Navigator

Cybersecurity Projects

Security Audit – Botium Toys

Performed an internal security audit using NIST CSF, identifying missing controls, compliance gaps, and risks. Developed recommendations and completed the full controls and compliance checklist.

Linux File Permissions Hardening

Configured secure file and directory permissions using chmod, chown, and group access controls. Demonstrated least-privilege principles and system hardening techniques.

SQL Filtering Lab

Queried log data using SQL to identify failed logins, anomalies, and suspicious activity. Demonstrated filtering, sorting, and data-driven security analysis.

Incident Handler’s Journal

Documented an account compromise scenario using structured incident response methodology including timeline, impact analysis, containment steps, and lessons learned.

Python Log Parsing Automation

Developed a Python script to parse authentication logs and extract failed login events. Demonstrated automation, regex basics, and log triage workflow.

Cybersecurity Homelab

Built a virtualized homelab using VirtualBox with Ubuntu Server, Kali Linux, and Windows 10. Practiced system hardening, network analysis, SIEM ingestion, and hands-on testing.

Professional Experience

Foreman / Heavy Equipment Operator

Branch Construction Group — May 2025 to Present

- • Supervise crews, enforce safety, and manage production in complex field operations.
- • Conduct risk assessments, document findings, and resolve operational issues under pressure.
- • Interpret blueprints, coordinate with inspectors, and ensure compliance with regulations.
- • Maintain detailed daily reports (production logs, issues, safety notes) — directly transferable to incident documentation.

Lead Dry Ice Technician

Onsite Oilfield Services — Aug 2022 to Apr 2025

- • Led a 3-person crew in high-risk environments with strict safety controls.
- • Resolved customer issues onsite and ensured high-quality service delivery.
- • Maintained equipment, followed standardized procedures, and documented work activity.

Project Manager / Carpenter

Professional Contracting Services — Jul 2019 to Apr 2022

- • Managed multi-phase residential projects, coordinated teams, workflows, and timelines.
- • Interacted with clients to clarify requirements and document scope changes.
- • Applied problem-solving and root-cause analysis to jobsite challenges.

Education

San Jacinto College — Houston, TX

Associate of Applied Science (AAS) in progress — Cybersecurity-aligned coursework underway

Planned Coursework / In-Progress Learning

- • Google Cybersecurity Professional Certificate (In Progress)

- • CompTIA Security+ (Planned)
- • CompTIA Network+ (Planned)
- • Python for Cybersecurity (Planned)
- • SIEM Analysis and Threat Detection Labs (Planned)
- • TryHackMe / HackTheBox Beginner Pathways (Planned)

Certifications

- • TWIC Card — Valid Through 2027
- • McGraw Hill: Level 1 Access White Belt — Credential ID 162864745
- • McGraw Hill: Level 1 Excel White Belt — Credential ID 161971441
- • McGraw Hill: Level 1 PowerPoint White Belt — Credential ID 160132141
- • McGraw Hill: Level 1 Word White Belt — Credential ID 160786580
- • CompTIA Security+ (Planned)
- • CompTIA Network+ (Planned)