Daniel Chavez

Glendale, AZ | Worcester, MA | (480) 709-5202
contact.dchavez@gmail.com | www.linkedin.com/in/daniel-chavez7/ | GitHub

EDUCATION

College Of The Holy Cross **Worcester, Massachusetts**
Bachelor of Sciences in Computer Science - Specialization in Cybersecurity and AI/ML Expected Graduation: May 2026
Relevant Coursework: Data Structures & Advanced Algorithms, Computer Systems & Organization, Networking & Cybersecurity, Advanced Machine Learning

PROFESSIONAL EXPERIENCE

Western Alliance Bancorporation **Phoenix, Arizona**
Cybersecurity Engineering Intern *May 2025 – August 2025*
- Built ML-powered log analysis pipelines in Elasticsearch using Python, replacing static thresholds with adaptive anomaly detection that reduced false positives by 60% and accelerated incident response by 70%
- Automated incident response processes with Python and Ruby, integrating workflows into Palo Alto XSOAR and enabling faster triage.
- Designed and tested ML autoencoder models for anomaly detection.

College Of the Holy Cross ITS Department **Worcester, Massachusetts**
Information Security and Vulnerability Management Intern *May 2024 – August 2024*
- Spearheaded migration from Nessus to Rapid7, accelerating vulnerability scanning by 50% and enabling detection of critical vulnerabilities within minutes of emergence across campus infrastructure
- Conducted vulnerability scanning, asset discovery, and risk reporting using Nessus and Rapid7 across campus infrastructure.

TECHNICAL PROJECTS

WardenAI – Autonomous Cybersecurity Sentinel **Glendale, Arizona**
Lead Developer / Security Engineer *July 2025 – Present*
- Architected an autonomous cybersecurity AI agent, "The Warden," to monitor network traffic, system logs, and security events in real time with a projected goal of reducing false positives by 90% and accelerating critical infrastructure response time by 70%
- Developed detection pipelines and alerting mechanisms to identify anomalies and potential threats in simulated enterprise environments.

Elasticsearch Home Lab **Phoenix, Arizona**
Personal Project *May 2024 – Present*
- Built a personal lab environment using Elastic Stack, Docker, and vulnerable VMs to simulate network attacks and defensive monitoring.
- Implemented Python scripts for log ingestion, anomaly detection, and automated alerting.
- Practiced penetration testing, network monitoring, and incident response workflows in a controlled environment.

APEX Finance **Worcester, Massachusetts**
Front and Backend Application Developer *August 2024 – December 2024*
- Developed a full-stack stock brokerage platform with Django, Flask, Python, JavaScript, and SQLite, integrating real-time market data APIs.
- Built AI-powered chart analysis tools and an asset allocation calculator to enhance user trading experience.
- Implemented secure authentication and transaction workflows to ensure reliability and compliance.

PROFESSIONAL CERTIFICATIONS

Cybrary **Glendale, Arizona**
Offensive Penetration Testing Certificate *June 2024 – July 2024*
- Learned topics regarding fundamentals of penetration testing, such as Metasploit, SQLMap, Hashcat, Hydra, Nmap, package capture
- Practiced penetration testing methodologies, vulnerability assessment, and network security concepts in lab environments.

CompTIA Security+ (SY0-701) *In Progress: Expected Completion Feb 2026*
- Actively preparing for the industry-standard certification covering threat management, cryptography, and network security protocols.

SKILLS & ACTIVITIES

Security Tools: Palo Alto XSOAR, Arctic Wolf, Nessus, Rapid7, Elastic Stack (ELK), Wireshark, Nmap, Kali Linux.

Programming: Python (Automation/Scripting), Shell, Ruby, C++, C#, SQL, Git

Cloud/Platforms: GCP, Azure, Linux (Ubuntu/RHEL), MacOS

HackTheBox & TryHackMe: Compromised 20+ machines by exploiting vulnerabilities in applications and privilege escalation techniques.

LeetCode: Solved 150+ algorithmic challenges in Python/C++, applying optimized logic to enhance performance in security automation scripts.

Languages: Fluent in English and Spanish