

Gregory Dean

Boise, Idaho | gregdeancyber@proton.me | [LinkedIn](#) | [GitHub](#) | [Website](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in IT support, security monitoring, vulnerability assessment, web application testing, and cloud-based lab environments. Background includes supporting offensive security engagements, analyzing logs and network activity, building security-focused lab infrastructure, and documenting technical findings for remediation and operational improvement. Strong foundation in cybersecurity operations, defensive analysis, and structured security methodologies across both enterprise support and lab-based environments.

CORE SKILLS

Security Operations: Security monitoring, log analysis, incident triage, threat detection, vulnerability assessment, phishing analysis, remediation support

Tools: Splunk, ELK Stack, Wireshark, Zeek, Nmap, Nessus, Burp Suite, Dirbuster, Metasploit, Hydra, John the Ripper, Hashcat

Systems: Windows, Linux, Active Directory, TCP/IP, DNS, endpoint support, AWS, virtualization, system imaging, hardware diagnostics

Frameworks & Concepts: MITRE ATT&CK, OWASP Top 10, NIST CSF, NIST SP 800-53, CIS Controls, ISO 27001, CVSS, technical documentation

CERTIFICATIONS

(ESCP) Evolve Security Certified Professional Certification Evolve Security Academy	2025
Certificate in Cyber Security Evolve Security Academy	2025
Security+ CompTIA	Expected 2026

PROFESSIONAL EXPERIENCE

IT Technician - Soiltech Wireless | Boise, Idaho

March 2024 - December 2025

- Created and maintained SOPs, network diagrams, and asset documentation
- Imaged, configured, and diagnosed 50+ endpoint devices
- Supported patching, access control, and baseline system hardening
- Troubleshoot system and network issues to improve reliability and uptime

Temporary Penetration Tester - Drug Policy Alliance | New York, New York

June 2025 - July 2025

- Supported a team-based penetration test of a live client environment
- Led assigned testing tasks across recon, validation, and documentation
- Conducted internal and external assessments using Nmap, Nessus, Burp Suite, and Dirbuster
- Identified and documented 24 validated vulnerabilities with remediation guidance
- Performed CVSS-based triage to help prioritize remediation efforts
- Built a Python script using the HIBP API to check organizational email exposure

Cybersecurity Apprentice - Evolve Security Academy | Chicago, Illinois

January 2025 - July 2025

- Completed hands-on labs and capstone projects in offensive and defensive security
- Built AWS lab environments with segmented subnets and access controls
- Performed web application testing focused on OWASP Top 10 vulnerabilities
- Analyzed network traffic using Wireshark and Zeek to identify suspicious activity
- Created SIEM dashboards in Splunk and ELK to monitor indicators of compromise
- Conducted log analysis and mapped findings to MITRE ATT&CK techniques
- Applied NIST, CIS Controls, and ISO standards in security mapping exercises
- Used common security tools in structured lab and CTF-style environments

CYBERSECURITY PROJECTS

Cybersecurity Homelab - Active, Directory, Splunk/ELK, Kali Linux, Wireshark, Zeek | [GitHub Repository](#)

- Built a virtual enterprise-style lab for SIEM monitoring, log analysis, attack simulation, and defensive security testing, with documentation focused on detection workflows and incident investigation.

Email Breach Checker - Python, HIBP API, JavaScript | [GitHub Repository](#)

- Developed a Python tool to automate email breach checks and generate structured output for exposure analysis and remediation support