Connor Dedic

858-361-0166 | connordedicpro@gmail.com | github.com/ConnorDedic | linkedin.com/in/connor-dedic

Summary

Security engineer specializing in Windows malware development, cyber deception, and offensive tooling in C, Python and Go. Contributing researcher on an upcoming publication covering novel cyber deception techniques.

Work Experience

Cyber Deception Engineer January 2026 - May 2026
Space Dynamics Laboratory *Logan, UT*

- Cataloged, researched and developed cyber deception in preparation for presentations and an upcoming published paper
- Conducted forward-looking research to assess the feasibility and operational impact of novel cyber deception techniques
- Designed a taxonomy and methodology for applying cyber deception techniques across AI, ICS, AD, and bespoke systems

Information Security Operations Center Analyst August 2025 - December 2025
The Church of Jesus Christ of Latter-day Saints *Riverton, UT*

- Analyzing, triaging, and responding to cyber threats targeting worldwide infrastructure and global leaders
- Utilizing enterprise security tools including Splunk, Palo Alto Panorama, Microsoft Defender Online, Azure, BlueCat, BART and Crowdstrike to investigate phishing, malware, and other threat events
- Collaborating in a 24/7 SOC environment to protect critical systems and sensitive information from real-world adversaries across a global network

Course Architect for Cybersecurity Fundamentals & Security Assessment November 2024 - July 2025
Brigham Young University - Idaho *Rexburg, ID*

- Led 30+ students in learning the basics of cyber defensive operations and penetration testing
- Developed a defense simulation using Bash and 40+ virtual machines to allow students to simulate defending a live multi-phase cyberattack following standardized attacker methodology (MITRE ATT&CK) and practice threat hunting
- Deployed vSphere to manage 60+ cloud virtual machines for student labs including attack and defense infrastructure

Security Operations Center Analyst Tier 1 January 2025 - May 2025
Rexburg City *Rexburg, ID*

- Leveraged Security Onion to detect and report various cyber threats to ICS and other key infrastructure for 5 months
- Applied a structured threat hunt methodology to identify active attacks, triage findings, and report according to the playbook
- Analyzed hundreds of alerts, tracked attack patterns, and worked to streamline ticket queue eliminating false positives

Practical Experience

CTF Creator August 2025 - Present
BSides Utah *Remote*

- Created several Capture the Flag challenges for both BSidesSLC and BSidesRedRocks
- Challenge categories include PWN, web, cryptography, and reverse engineering with C, Python, Go, Docker, Bash, and Nginx

Society of Cybersecurity January 2024 - August 2025
Brigham Young University - Idaho *Rexburg, ID*

- Placed 3rd in the cybersecurity category at the HackUSU 2025 out of 600+ competitors in Logan, Utah
- Placed 5th at the 2024 Rocky Mountain Collegiate Cyber Defense Competition regional in Denver, Colorado
- Served as vice president and competition team captain of the BYU-Idaho Society of Cybersecurity
- Responsible for leading and training a team of 15+ students to prepare for competitions and other projects

Technical Projects January 2022 - Present
Security Engineering

- Developed a comprehensive Identity and Access Management (IAM) system by integrating a WordPress web service with Apereo CAS as the identity provider and Active Directory for centralized user authentication
- Frequently handled 15+ AWS services, including EC2, Lambda, RDS/DynamoDB, Cognito, EBS and Fargate
- Utilized tools such as Suricata, Git, AWS, Node.js, Security Onion, Splunk, ELK, Kibana, Sysmon and Docker
- Built networks with Palo Alto and Fortigate firewalls, Duo MFA, Radius, Squid, load balancing, Splunk and Cisco

Red Team Operations

- Studied and conducted Active Directory attack and defense techniques; proficient with open-source tools like Impacket, BloodHound, Plumhound, MiTM6, NetExec, Proxychains, Empire, Mimikatz, Sliver and PSExec in lab environments
- Created a homelab with a HP Proliant DL380P to practice securing a server as well as setting up offensive infrastructure
- Developed in Python, PowerShell, Bash, C, Golang, HTML, CSS and JavaScript individually and in teams
- Utilized tools such as Burp Suite, Metasploit, Sliver, Nessus, Recon-NG, Social Engineering Toolkit and PEASS

Education

Bachelor of Science - Cybersecurity January 2022 - July 2026
Brigham Young University - Idaho *Rexburg, ID*

- Key Courses: Systems Security 1 & 2, Security Assessment, Security Operations, AWS and Cloud Computing, Python 1 & 2, DevOps and IT Management, Advanced PowerShell, Networking 1 & 2, and Identity and Access Management
- Certifications: AWS Cloud Practitioner, Security+, PenTest+ and CySA+; Upcoming: PNPT