**CONNOR S. W. FITZGERALD**

(314) 478-4952 – connor.fitzgerald.1@outlook.com – the8bitwit.com

**PROFESSIONAL SUMMARY**

I’m a cybersecurity professional with 4 years of U.S. Air Force experience and a strong focus on hands-on, practical learning. Currently completing my Bachelor’s in Cybersecurity, I’ve developed skills across network defense, penetration testing, digital forensics, and incident response. I’m always looking for new ways to stay ahead of emerging threats. Beyond formal education, I actively train on hacking platforms, pursue certifications, and I’m the creator of Backdoors.ai—a gamified learning platform that helps people build real-world hacking skills through challenges and AI mentorship. My mission is to make cybersecurity more accessible, engaging, and genuinely rewarding for newcomers and enthusiasts alike. I’m passionate about not just growing in this field but contributing to it. Whether through challenge creation, mentorship, or building tools that help others learn faster, I’m committed to making an impact.

**EDUCATION**

**Keiser University, Sarasota, FL 2023-Present**

*Bachelor of Science in Cybersecurity*

My course work in Cyber Security included Security Operations, Risk Management, Network Defense, Threat Analysis, and Governance. My coursework has included ethical hacking, digital forensics, vulnerability assessment, incident response, and malware analysis; providing both technical depth and a strategic understanding of how to protect systems and data in real-world environments.

In addition to my academic work, I serve as the Capture the Flag (CTF) coach for Keiser University. In this role, I mentor fellow students in offensive security techniques, guide them through hands-on challenges, and help prepare them for competitions and careers in ethical hacking.

**Keiser University, Melbourne, FL 2022-2023** *Associate of Science in Information* Technology

My coursework in Information Technology included Network Design, Database Management, Systems Analysis, and Web Development. I also gained experience in IT Project Management, Software Engineering, Cloud Computing, and Information Systems Security, providing a comprehensive technical foundation. Successfully completed the degree with a 3.75 GPA.

**Community College of the Air Force, Montgomery, AL 2018-2021**

*Associate of Science Criminal Justice Course Work*

My Criminal Justice coursework covered areas such as Criminal Law, Criminology, Law Enforcement Procedures, and the U.S. Judicial System. I also studied Corrections, Juvenile Justice, Ethics in Criminal Justice, and Crime Prevention, providing a broad understanding of the legal and justice systems.

**WORK EXPERIENCE**

**Backdoors.AI, Tampa, FL**

**Founder and Lead-Developer** **2025-Present**

As the founder of Backdoors.ai, I’m building a hands-on cybersecurity training platform that teaches ethical hacking and core cybersecurity concepts through gamified challenges and real-world simulations. The platform blends technical realism with AI-powered mentorship to create a learning experience that’s practical, engaging, and beginner-friendly.

I lead product design, challenge development, and content strategy, while collaborating with developers to bring the platform’s vision to life. I also manage branding, user experience, and community engagement—continually refining the platform based on user feedback.

Backdoors.ai reflects my passion for cybersecurity and my commitment to making it more accessible. I believe learning this field should be both educational and fun, free from outdated methods and built around real skills that actually matter.

**Notable Accomplishments:**

* Waiting on user count.

**U.S. Air Force, 91st Security Operations Squadron, Minot AFB, ND**

**Cyber Security Liaison** **2020-2022**

As a Cyber Security Liaison, I managed a team of over 300 personnel, spanning various IT and Information Security functions. My responsibilities encompassed Microsoft 365 end-user support, Active Directory administration, Records Management, and IT asset budgeting, procurement, and deployment. I frequently took a hands-on approach to troubleshoot and resolve IT issues.

I conducted routine OPSEC (Operational Security) and INFOSEC (Information Security) training to ensure strict DoD compliance across eight diverse teams and over 12 unique programs.

**Notable Accomplishments:**

* Revamped the Records Management Program by digitizing over 10,000 records, ensuring proper storage and accountability, and helping over 50 programs run by the 91st Missile Security Operations Squadron maintain continuous DoD compliance.
* Streamlined the End User Agreement Request system, reducing average response time by 50% and significantly minimizing unexpected downtime for team members.
* Identified and recovered $100K worth of unaccounted IT equipment, enabling the acquisition of an additional 170 Dell laptops to boost the team's administrative capabilities, ultimately saving time, and enhancing productivity.

**Tactical Response Force Leader**  **2019-2020**

As a Tactical Response Force Leader, I conducted aerial security operations aboard the UH-1N rotary aircraft, safeguarding nuclear launch facilities within the DoD missile complex and reinforcing the Air Force's paramount mission of nuclear deterrence through over 500 hours of flight time.

Operating as a team leader, I led 15 highly trained security specialists on recapture and recovery missions within Minot AFB’s missile fields, conducting a wide range of tasks from vehicle interdictions to close quarter combat within the nuclear launch facilities.

**Notable Accomplishments:**

* Diligently carried out 1,000 hours of physical security, orchestrating a 15-member team in rapid response measures to potential hostile threats, ensuring the safety and protection of critical assets.
* Developed proficiency in performing and instructing highly specialized skills, including rappelling, fast roping, chemical breaching, close quarters combat, and weapon manipulation, elevating the team's tactical capabilities and preparedness.

**Convoy Response Force Member** **2018-2019**

As a member of a 52-person team I was responsible for the secure transportation of nuclear assets across the largest Department of Defense missile field, participating in over 100 critical missions. My role involved ensuring adherence to stringent safety protocols, supporting essential maintenance objectives, and contributing to the overall reliability of the missile stockpile. Through meticulous attention to detail and coordination, I helped safeguard national security while maintaining the highest operational standards in high-stakes environments.

**Notable Accomplishments:**

* Provided exemplary oversight to 12 direct subordinates by mentoring, training, and guiding them through over 300 hours of DoD-related courses, promoting their professional growth and enhancing their skill sets.

**AWARDS**

Placed Top 1% in National Cyber League CTF 2025

Placed Top 5% in National Cyber League CTF **2024**

Dean’s List **2023-2025**

Air Force Commendation Medal **2022**

Distinguished Graduate Award – Leadership Course **2021**

Staff Level Airman of The Year Award **2020**

Senior Airman Below the Zone **2019**

Aerial achievement Medal **2019**

Team Level Airman of The Quarter Award **2018**

**SKILLS**

I'm confident in public speaking and clear communication, with experience presenting to a wide range of audiences—from small teams to large groups. I work well both independently and on a team, and I’m comfortable adapting to different environments and people. I pay close attention to detail and take pride in being able to break down complex information in a way that makes sense. Whether I’m juggling multiple tasks or working under pressure, I stay focused on delivering quality results and doing the job right.

I’ve worked hands-on across a wide range of IT systems, from setting up and securing networks to troubleshooting hardware and managing enterprise environments. I’m experienced with configuring Cisco routers, switches, and firewalls, and have deployed VPNs, VLANs, and ACLs to enforce strong security practices. I’ve also managed Windows Server environments, working with Active Directory, DNS, DHCP, and Group Policy to control access and keep systems organized and secure.

On the hardware side, I’ve installed, repaired, and maintained desktops, laptops, servers, and network equipment—handling everything from failed power supplies and bad RAM to full system rebuilds. I’ve also done on-site walkthroughs to document and map IT assets for better network visibility.

In terms of tools and technologies, I’ve worked with Microsoft 365, Hyper-V, pfSense, and GPO management tools. I’ve used remote support software like VESD, inventory systems like ILS, and imaging tools such as Windows Deployment Services and Microsoft Configuration Manager. For automation and scripting, I’ve used PowerShell and basic Bash. I'm also familiar with managing cloud-based environments through platforms like AWS. I work with virtualization and container tools like VMware Workstation, VirtualBox, and Docker on a regular basis.

In cybersecurity, I’ve spent a lot of time getting hands-on with real tools and techniques. I primarily work in Kali Linux and have experience with vulnerability scanning, network exploitation, privilege escalation, and post-exploitation, all tested through platforms like Hack The Box, TryHackMe, Test-Out, Cengage, and my home lab.

While I focus heavily on red team tools and offensive techniques, I use that knowledge to strengthen my blue team skills. Understanding how attackers think helps me better identify weaknesses, anticipate exploits, and develop stronger defenses. Whether it’s writing detection rules, reviewing logs, or planning incident response steps, I approach each task with an attacker’s perspective in mind.

I’ve used a wide range of tools across different areas of cybersecurity. For offensive security, I’m familiar with Burp Suite, Nmap, Metasploit, Hydra, SQLmap, and Ghidra. On the defensive side, I’ve used Splunk, Wireshark, Security Onion, Redline, LogViewPlus, and Autopsy for forensics and threat hunting. For scanning and assessment, I’ve worked with Nessus, OpenVAS, Nikto, Yara, and Shodan. I reference Exploit DB regularly and apply the MITRE ATT&CK framework when analyzing threat actor’s behavior.

I incorporate scripting with Python and JavaScript for automation, payload development, and malware analysis.

I’ve led and participated in incident response tabletop exercises, focusing on identifying initial access, privilege escalation, and persistence. I’m always experimenting with ways to integrate AI into my workflow, whether to speed up analysis or guide learning.