REYNALDO RODRIGUEZ

Cybersecurity Student | Entry-Level Cybersecurity Analyst
786-306-6483 • ReynaldoRSoul@gmail.com • linkedin.com/in/reynaldorsoul • Miami, Florida

SUMMARY

Cybersecurity B.S. candidate (GPA 3.7, Aug. 2026) with hands-on experience in vulnerability analysis, red team testing, secure lab environments, and system troubleshooting. Led a senior capstone project focused on combining automated vulnerability scanning with manual testing to identify critical security gaps. Skilled in Splunk, Nessus, Wireshark, Docker, and Linux, with interest in entry-level cybersecurity, vulnerability management, security operations, and information security roles. Bilingual in English and Spanish.

EDUCATION

Florida International University Miami, FL *B.S. in Cybersecurity*
Expected Aug. 2026

GPA: 3.7 • Dean's List

CERTIFICATIONS

CompTIA Security+ *(Expected Aug. 2026)* **CompTIA Network+** *(Expected Aug. 2026)*

TECHNICAL SKILLS

Security Tools: Splunk (log ingestion & alerting), Wireshark, Nessus, Nmap, Metasploit, Burp Suite
OS & Platforms: Kali Linux, Ubuntu, Windows, Docker, Raspberry Pi, VirtualBox
Languages: Python, Bash, Java, C
Concepts: Networking, TCP/IP, DNS, VPN fundamentals, vulnerability scanning, log analysis, SIEM fundamentals, Linux administration, container networking, system troubleshooting, remote access security

PROJECTS

VulNerd — *Senior Capstone — Cloud Security Architect & Team Lead* Spring 2026 | FIU

- Led a 5-person senior capstone team as Cloud Security Architect, building the lab environment that supported an AI-powered tool for vulnerability analysis and compliance reporting (NIST 800-53, PCI-DSS)
- Deployed DVWA in Docker on a Raspberry Pi 5 with MariaDB, configured to Security Level Low to ensure all vulnerability classes were fully exploitable for team testing
- Secured lab access via Tailscale VPN — zero public exposure, team-only access enforced throughout the entire project lifecycle
- Ran multiple Nessus scan types (Basic Network, Credentialed, Web App, Advanced Dynamic) and supported manual red team testing across 8 attack modules including SQLi, XSS, and Command Injection
- Team demonstrated that roughly 40% of findings — including 3 of 4 Critical ones — were only caught through manual testing, highlighting the value of a layered approach over automation alone

SoulHomeLab — *Personal Home Server & Networking Lab* Ongoing

- Built and managed a Ubuntu-based home server running Docker containers (Plex, Sonarr, Nextcloud, Vaultwarden) managed through Portainer, with Adguard providing network-level DNS filtering
- Configured Cloudflare and Tailscale for secure remote access without exposing ports, and Duplicati for automated encrypted backups across all services
- Organized storage with separate mount paths for downloads, movies, and shows across multiple drives
- Monitored service availability with Uptime Kuma and debugged real networking issues including DNS conflicts, port collisions, and Docker container communication problems

WORK EXPERIENCE

T-Mobile *Mobile Expert* Nov. 2019 – Jul. 2022

- Identified and escalated suspicious account activity following security and identity verification procedures
- Educated customers on account security, MFA best practices, phishing awareness, and SIM-swap scam prevention
- Diagnosed device and network connectivity issues using systematic troubleshooting across iOS and Android platforms

AT&T *Sales Representative* Aug. 2019 – Oct. 2019

- Maintained customer records in CRM systems in compliance with data privacy procedures
- Explained complex technical information clearly to customers with varying levels of technical knowledge

MetroPCS *Sales Representative* Mar. 2017 – Aug. 2019

- Assisted customers with device setup, activation, and basic troubleshooting across Android and iOS
- Consistently met sales goals in a fast-paced retail environment