Adrian Christopher Fernandez Calso

(828) 974-6628 | adrianccalso@gmail.com | Charlotte, NC | LinkedIn

SUMMARY

Driven and detail-oriented security analyst with hands-on experience from homelab projects, bootcamp training, and industry-recognized certifications, including the Security+, Network+, and ITIL4. Strong foundation in threat detection, monitoring, and response, with practical exposure to SIEM platforms like Elastic SIEM, endpoint security tools, and Snort IDS. Comfortable working across Linux and Windows environments, combining technical skills with an investigative mindset and a focus on refining detection logic and uncovering subtle threats. Known for a proactive, self-taught approach to cybersecurity, strong problem-solving abilities, and a curious mindset — eager to sharpen both tools and instincts within fast-paced, high-impact security teams.

EDUCATION

B.S Cybersecurity & Information Assurance | Western Governors University 9/2024 – 12/2025

- *Relevant Coursework:* IT Applications, Legal Issues in Information Security, Networks, Emerging Technologies in Cybersecurity, Network and Security: Applications, Business of IT: Applications, Digital Forensics in Cybersecurity
- Active member of the WGU Cybersecurity Club

Cybersecurity Bootcamp | North Carolina State University 7/2023

- Comprehensive 10 month-long program covering the fundamentals of networking and cybersecurity through live classes with labs and simulations from industry-leading professionals.
- *Capstone: Security Operations Center Homelab*
  - Designed a security operation center virtualized in Proxmox, hosting an Elastic/Logstash/Kibana (ELK) SIEM Stack with Snort intrusion detection system (IDS), Docker, PFSense firewalls, and CIS Benchmark hardened/non-hardened Linux/Windows virtual machines.
  - Performed penetration tests using Nmap and Metasploit, followed by endpoint and log analysis with their corresponding SIEM events mapped to the MITRE ATT&CK Framework.
  - Implemented DLP solutions via MyDLP, database encryption, group policy, and firewalls.
  - Showcased foundational knowledge in Linux and Windows security, TCP/IP, Active Directory, DNS, and DHCP.

PROFESSIONAL DEVELOPMENT

Member of (ISC)2, Charlotte Metro Chapter, Charlotte, NC 4/2024 – Present

Black Hills Information Security Training 1/2025 – 3/2025

- Performed log analysis, threat hunting, and incident response; utilized tools such as Wireshark, Sysmon, and Zeek to detect and investigate real-world threats.
- Applied the MITRE ATT&CK framework to map adversary tactics and techniques, develop detection logic, and simulate threats using Atomic Red Team.
- *Deployed honeypots, honeytokens, and deceptive artifacts to identify and disrupt attacker behavior; integrated deception-based threat intel into alerting workflows to improve detection and response capabilities.*

Recorded Future PREDICT 2023 Conference, Washington D.C. 10/2023

- Placed 4th in threat-hunting style Capture the Flag using Recorded Future's AI threat intelligence platform.

Joint University Cybersecurity Conference, Washington D.C. 9/2023

- Learned about the current state and future of cybersecurity in the private and public sector through Duke, Georgetown, George Mason, and the FBI Association of Intelligence Analysts.

CERTIFICATIONS & TECHNICAL SKILLS

Certifications:	(ISC)2: CC | CompTIA A+, Network+, Security+
Systems:	Windows: 7/10/11, Server 2019 | Linux: Ubuntu, Debian/Debian-based
Languages:	Python, Powershell, Bash, JavaScript
Tools:	Wireshark, Nmap, Metasploit, Elastic SIEM, VirtualBox, Active Directory, MITRE ATT&CK Framework, PFSense, Zeek