ANTONIO BELTRAN-MILLER

Clarkston, MI • 248-892-3676 • antoniobeltranmiller@gmail.com
LinkedIn: linkedin.com/in/antoniobeltran-miller • GitHub: github.com/CyberShellCode

NOTABLE ACHIEVEMENT

Critical Vulnerability Discovery: Discovered a supply chain attack vulnerability in a public repository's npm configuration that could enable man-in-the-middle attacks leading to remote code execution. Currently following responsible disclosure process.

PROFESSIONAL SUMMARY

Skilled cybersecurity professional with a proven track record in threat detection, incident response, and vulnerability assessment, specializing in enterprise-grade security monitoring environments. Demonstrated expertise in cloud security architecture, penetration testing, and identity management systems with active contributions to the security research community through hands-on lab work and bug bounty programs.

PROFESSIONAL EXPERIENCE

Independent Cybersecurity Consultant — Jan 2023 – Present

- Conducted cybersecurity assessments and implemented foundational security controls, including firewall deployment and network segmentation
- Performed security gap analyses and delivered prioritized remediation roadmaps based on risk assessment findings
- Established security monitoring and alerting capabilities for previously unprotected network environments

IT Support Specialist | ALM Freight (Amazon Delivery Service Partner) — Sep 2021 - May 2024

- Performed system hardening and patch management across 150+ endpoints, reducing vulnerability exposure by 35%
- Maintained security compliance reporting achieving 95% patch compliance rate
- Managed Active Directory access controls and group policies enforcing least-privilege principles
- Streamlined user provisioning workflows reducing resolution time by 50%

KEY PROJECTS

- **Enterprise SOC Home Lab:** Deployed a comprehensive security environment with pfSense firewall, Active Directory, Sysmon endpoints, Splunk SIEM, and custom detection rules for advanced persistent threats
- **T-Pot Honeypot Analysis:** Deployed multi-honeypot stack, analyzed attack patterns over two weeks, identified 12 new attack vectors and improved detection capabilities by 25%
- **Malware Analysis Environment:** Built isolated Flare VM sandbox for dynamic analysis, documented malware behavior, and created detection signatures

TECHNICAL SKILLS

Security: SIEM (Splunk), Microsoft Defender, Nessus, Burp Suite, Nmap, CrowdSec, FortiGate Firewall, Incident Response, Threat Hunting, Vulnerability Assessment, Penetration Testing

Systems: Active Directory, Sysmon, PowerShell, Bash, Windows/Linux Administration, AWS Security

Programming: Python, PowerShell, Bash, SQL, Solidity

EDUCATION & CERTIFICATIONS

Bachelor's degree in cybersecurity and information assurance (In progress) — Expected Fall 2026

Western Governors University

Current Certifications:

- **CompTIA Security+ (In Progress - Expected September 2025)**
- **AWS Security Best Practices Series (5 certificates)**
- **Fortinet Certified Associate (FCA) in Cybersecurity**
- **SailPoint Identity Security Leader**
- **Google Cybersecurity Professional Certificate**
- **LetsDefend SOC Analyst Learning Path**

CONTINUOUS LEARNING

- **Active in cybersecurity CTFs (HackTheBox,TryHackMe, PicoCTF)**
- **Completed PortSwigger Web Security Academy labs (OWASP Top 10)**
- **Security research contributor**
- **Ongoing professional development through hands-on labs**