ANTONIO BELTRAN-MILLER

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

PROFESSIONAL SUMMARY

Security analyst specializing in SIEM operations, threat intelligence, and automation with offensive security research capabilities. Built production-grade tools for vulnerability testing; deployed multi-honeypot infrastructure analyzing 424,000+ attacks; engineered AI-assisted incident triage automating manual enrichment workflows. Active contributor across Web2/Web3 bug bounty platforms with multiple confirmed vulnerabilities and responsible disclosures.
→ Detailed project documentation, screenshots, and technical writeups at antoniobeltranmiller.com

TECHNICAL SKILLS

Security: Splunk, ELK, Microsoft Defender, FortiGate, CrowdSec, Nessus, Burp Suite, Incident Response, Threat Hunting, Detection Engineering, Honeypots, IOC/IOA Enrichment, Suricata
Systems: Active Directory, Sysmon, Windows/Linux Administration, PowerShell, Bash, Docker, AWS Security
Programming: Python, PowerShell, Bash, SQL, Solidity

PROFESSIONAL EXPERIENCE

Security Researcher & Vulnerability Analyst — Self-Directed
Jan 2023 – Present
Reported 6+ confirmed vulnerabilities across Bugcrowd/Cantina (Web2 & smart contracts) including critical MITM attack vector enabling RCE via insecure npm registry configuration (P4-Low escalated to P2-High)
Deployed T-Pot multi-honeypot across 8 profiles; analyzed 424,000+ attacks over the period of a month, including URGENT/11, Citrix Workspace exploitation, and VoIP toll fraud. Documented attack patterns, submitted IOCs to AbuseIPDB, and coordinated with hosting provider abuse teams (GoDaddy, others) to disrupt C2 infrastructure
IT Support Specialist — ALM Freight
Sep 2021 – May 2024
Performed system hardening and patch management across 150+ Windows/Linux endpoints; maintained security compliance reporting and vulnerability tracking
Managed Active Directory security baselines enforcing least-privilege access; streamlined user provisioning and incident response workflows
Implemented enterprise GPOs for security configuration, endpoint protection, and access control

KEY PROJECTS

Full technical documentation, attack simulations, and analysis available at antoniobeltranmiller.com/projects

SOC Automation & AI-Enhanced Triage

Built next-generation SOC automation infrastructure merging AI with traditional security operations. Engineered automated incident response pipeline using Splunk, n8n, and GPT-4, incorporating real-time threat intelligence enrichment, MITRE ATT&CK; mapping, and instant Slack alerting for rapid response. Achieved high-fidelity detection across 10 automated rules while maintaining minimal false positive rates.

T-Pot Threat Intelligence Platform

Deployed distributed honeypots capturing 424,000+ attacks; documented exploitation of URGENT/11, Citrix Workspace (CVE-2020-11900), VoIP toll fraud from compromised GoDaddy infrastructure, and commercial scanner reconnaissance. Published detailed analysis and IOCs; coordinated with hosting providers.

Malware Analysis Environment

Analyzed RATs and rootkits in FlareVM sandbox; identified persistence mechanisms (scheduled tasks, registry modifications) using Process Hacker, Hollows Hunter, Regshot, Autoruns, Procmon, and Wireshark. Documented IOCs and created detection signatures.

Blind XSS Detection Platform

Production-ready XSS hunter with SSL dashboard, real-time capture monitoring, and automated payload generation. Zero-to-deployment in 60 seconds via automated installation bash script.

EDUCATION & CERTIFICATIONS

Bachelor's degree in Cybersecurity and Information Assurance (In Progress)
Western Governors University | Expected late 2026
Current Certifications:
CompTIA Security+ (Certified October 2025)
AWS Security Best Practices Series (4 certificates)
Fortinet Certified Associate (FCA) in Cybersecurity & FortiGate 7.6 Operator
SailPoint Identity Security Leader
Google Cybersecurity Professional Certificate
LetsDefend SOC Analyst Learning Path

CONTINUOUS LEARNING

Active in cybersecurity CTFs (HackTheBox, TryHackMe, PicoCTF); PortSwigger Web Security Academy (OWASP Top 10)
Bug bounty contributor (Bugcrowd, Cantina); publishes security research at antoniobeltranmiller.com/blog
Ongoing professional development through hands-on vulnerability research and lab environments

NOTABLE ACHIEVEMENT

Paid Bug Bounty — HIGH-Severity RCE
Discovered and responsibly disclosed vulnerability in public repository where insecure HTTP method configuration enabled remote code execution; received monetary bounty through Bugcrowd platform.

→ View detailed case studies, attack simulations, and technical writeups: antoniobeltranmiller.com