# MATHEW MONTALVO

San Sebastian, Puerto Rico | 787-943-4338 | mathew.montalvoruiz@gmail.com
linkedin.com/in/mathew-montalvo-7889a0243 | github.com/mmontalvo-sec | mmontalvo-sec.github.io

## PROFESSIONAL SUMMARY

Security operations-focused IT technician with hands-on experience triaging SIEM/IDS alerts, reviewing vulnerability findings, investigating authentication and endpoint events, and documenting incident response steps. Built and operated a SOC lab using Wazuh SIEM, Snort IDS, Palo Alto firewall segmentation, Nessus/OpenVAS, Kali Linux, Active Directory, and Ubuntu hardening. CompTIA A+, Network+, and ITF+ certified; Security+ in progress.

## TECHNICAL SKILLS

**Security Operations:** Alert triage, log analysis, threat detection, security monitoring, incident documentation, vulnerability assessment, endpoint monitoring, malware remediation, hardening, network segmentation
**Security Tools:** Wazuh SIEM, Snort IDS, Nessus, OpenVAS/GVM, Kali Linux, Nmap, Wireshark, Fail2Ban, UFW, tcpdump
**Networking:** TCP/IP, DNS, DHCP, VLANs, routing, NAT, VPN, Palo Alto firewall zones, Cisco switching, inter-VLAN routing
**Systems:** Windows Server, Active Directory, Group Policy, Windows 10/11, Ubuntu Server, NGINX, Docker, PowerShell, Bash, SSH, RDP

## SECURITY PROJECT EXPERIENCE

**SOC Lab Environment** | *Wazuh SIEM* | *Snort IDS* | *Palo Alto* | *Nessus* | *OpenVAS* | *Kali* | *Active Directory*

- Designed and deployed a SOC lab with Wazuh SIEM, Snort IDS, Palo Alto firewall segmentation, Cisco switching, Active Directory, and Windows Server.
- Configured AD, DNS, DHCP, domain-joined clients, VLANs, firewall zones, and controlled inter-VLAN communication for realistic monitoring coverage.
- Generated and investigated SIEM/IDS alerts from authentication events, endpoint behavior, Nmap scans, ICMP traffic, shared-folder access, and vulnerability scans, distinguishing true positives from false positives.
- Reviewed Nessus and OpenVAS/GVM findings against Windows and Linux targets; documented severity, likely impact, remediation steps, and validation notes.
- Practiced incident response workflows including alert triage, evidence collection, containment planning, remediation, and post-incident documentation.
- Hardened an Ubuntu NGINX server with UFW rules, SSH key access, Fail2Ban, security headers, and least-exposure configuration.

## PROFESSIONAL EXPERIENCE

**Independent IT Technician** | Tech West PC Repair | San Sebastian, PR **2023 – Present**

- Diagnose and resolve Windows failures, hardware faults, malware infections, printer issues, and network connectivity problems for residential and small-business clients with 90%+ same-day resolution.
- Conduct malware remediation using endpoint isolation, scan-based removal, startup review, clean-system validation, and preventive recommendations.
- Translate incident findings and remediation steps for non-technical clients while maintaining clear documentation and follow-up notes.
- Perform SSD upgrades, RAM testing, BIOS/UEFI updates, OS installation, system imaging, backups, and post-repair validation.

**Practicum Intern** | ITAuditors PR | Puerto Rico **2026 | 180 Hours**

- Assisted with mail server cybersecurity hardening through configuration review, attack-surface reduction, and technical documentation.
- Participated in field deployments across 5 client environments: structured cabling, rack organization, patch panels, connectivity testing, MikroTik and Grandstream equipment.

## ADDITIONAL INFRASTRUCTURE LAB

**Home Cloud Infrastructure** | *Ubuntu Server* | *Docker* | *Nextcloud* | *Pi-hole* | *Portainer* | *Tailscale*

- Deployed containerized services on Ubuntu Server and configured Tailscale private remote access without exposing public management interfaces.

## EDUCATION & CERTIFICATIONS

**B.S. Computer and Network Technology, Minor in Network Security** | GPA: 3.73 | **Graduated June 2026**
Inter American University of Puerto Rico, Aguadilla Campus | Highest GPA in Concentration

**Certifications:** CompTIA A+ | CompTIA Network+ | CompTIA ITF+ | TestOut PC Pro | TestOut Ethical Hacker | TestOut IT Fundamentals Pro | CompTIA Security+ (In Progress)