CARLOS CABRERA

Information Security Specialist · Cyber Incident Response

carlos@cabrerapr.com | Puerto Rico | Bilingual (English / Spanish)

PROFESSIONAL SUMMARY

Information Security Specialist with extensive experience across cybersecurity and information-systems management & administration. Trusted to secure clients in the industrial, legal, medical, educational, and banking industries throughout Puerto Rico and the United States — finding, documenting, analyzing, and delivering technical solutions while building secure, trusted business relationships. I help clients respond to incidents by discovering, reinforcing, and eliminating security risk, and deliver clear, actionable remediation plans. Currently seeking a challenging, hands-on cybersecurity role to complement my career path.

TECHNICAL SKILLS

- **Programming:** Bash, Python, PowerShell, PHP, HTML
- **Operating Systems:** Windows, Linux, Unix, FreeBSD
- **Firewalls:** Palo Alto, FortiGate (Fortinet), Cisco Meraki, pfSense
- **Endpoint / AntiVirus:** McAfee ePO, Sophos Central, Palo Alto TRAPS, Microsoft Defender, ESET
- **SIEM & Logging:** Elastic, Graylog, NX-Log, Tenable.io, Security Center, ProofPoint, KnowBe4, Enzoic
- **Databases:** TSQL, MySQL, SQLite, Elastic
- **Web Servers:** IIS, Apache, NGINX, Lighttpd
- **Cloud:** Microsoft Azure, AWS, DigitalOcean
- **Windows Infrastructure:** Active Directory, System Center, WSUS
- **Virtualization:** VMware ESXi, Proxmox, Hyper-V, Citrix, Xen
- **Backup & DR:** Veeam, Iperius, Druva, EaseUS
- **Administration:** RSAT, SpiceWorks, Dameware, SplashTop, AnyDesk

WORK EXPERIENCE

Evertec — San Juan, PR (Hybrid) | Jun 2024 – Present

Cyber Incident Response Specialist

- Receive and investigate incident reports from internal stakeholders; conduct thorough root-cause analysis.
- Develop and implement containment, eradication, and recovery strategies across cross-functional teams.
- Threat hunting with threat intelligence and advanced analytics to proactively identify emerging threats and attack vectors.
- Conduct regular vulnerability assessments and penetration testing to identify weaknesses.

- Ensure adherence to industry standards and regulatory requirements (NIST, FINRA); maintain accurate, detailed incident records.

TeleMedik — Guaynabo, PR | Jun 2021 – Jul 2024

Information Security Specialist

- Maintained the organization's information-security framework — policies, procedures, standards, and guidelines — with the IT Director.
- Led development and updates of the information-security strategy; reported gaps, strategies, and results to the Compliance Committee.
- Ensured administrative, physical, and technical safeguards protected information assets from internal and external threats; tested them regularly.
- Owned the security-incident and vulnerability-management processes end to end; performed ongoing security monitoring and annual audits.
- Ensured confidentiality and compliance with state and federal healthcare regulations, including HIPAA.

Cortelco Systems Puerto Rico, Inc. — Caguas, PR | Jul 2018 – Jun 2021

Information Security Analyst II

- Delivered managed security services (MSP) across industries: SOC/NOC development, provisioning, and log analytics.
- Firewall management — rule creation, hardening, reporting, and Python API development for custom reports.
- McAfee ePO, EndPoint, and SIEM management; ProofPoint Secure Email Gateway, phishing, and malware analysis.
- Built Graylog and NX-Log collectors and regex-driven dashboards to correlate events and identify threats.
- Vulnerability scanning via Tenable.io and Security Center; phishing-awareness training with KnowBe4.
- Performed scheduled penetration testing and delivered remediation reports on misconfigurations, risk, and data exposure.
- *Tools:* McAfee ePO, Tenable, Enzoic, Palo Alto, ProofPoint, Office 365, KnowBe4.

Computer Pro PR — San Juan, PR | Jun 2017 – Jun 2018

Information Security Technician

- Assisted the security lead and team with access provisioning, log analysis, and network security.
- Reviewed IDS logs for intrusions — account brute-forcing, email phishing, malware spread, and more.
- Provided proactive malware analysis through sandboxing to block and attribute threats.
- Managed the MobileIron MDM platform, building secure device profiles per company security metrics.
- Analyzed legacy software to document usage and reinstallation procedures.

Umeco Puerto Rico — San Juan, PR | Feb 2014 – Jun 2017

Director of IT

- Owned all aspects of systems administration and onsite security: servers, applications, routers, switches, firewalls, and databases.
- Handled implementation, configuration, maintenance, troubleshooting, security, and usage monitoring; developed specialized system procedures.
- Built CRM tooling with SQL data exported for customer purchase tracking and sales generation.
- Designed and implemented a WordPress website with a web store to boost sales and social presence.
- Managed 10+ servers, 6 multifunction printers, and 35+ endpoints for 50+ employees.

EDUCATION & CERTIFICATIONS

Bachelor of Business Administration, Information Systems — SUAGM, Cupey, PR (2020)

- CompTIA Security+ (ce) — **verified**
- MITRE ATT&CK Fundamentals — MAD20 — **verified**
- Recorded Future Certified Analyst (2025)
- CompTIA PenTest+ (ce) (2021, expired)
- Tenable Certified Sales Associate (TCSA) (2021)
- Palo Alto Networks PSE: Endpoint Associate
- CompTIA A+ **(2004 — good for life)**