# Marcos De La Rosa

El Paso, TX | 915-249-0414 | mdelarosa.cyber@gmail.com | [LinkedIn](http://www.linkedin.com/in/marcos-de-la-rosa)

## Professional Summary

Cybersecurity professional transitioning from a leadership role at Apple Inc. to security operations, bringing expertise in incident response, vulnerability management, log analysis, and network security. Skilled in SIEM monitoring (Splunk, Elastic Stack), Linux administration, security compliance, and cloud security. Experienced in threat intelligence, security automation, and risk mitigation. Passionate about cyber defense, compliance, and continuous professional growth and development. Seeking a Cybersecurity Analyst role to leverage technical expertise, investigative skills, and security operations knowledge in a higher education environment.

## Technical Skills

* Security Operations & Incident Response: SIEM monitoring (Splunk, Elastic Stack), log analysis, phishing investigations, threat hunting.
* Networking & Security: IDS/IPS, firewalls, VPNs, DNS security, system hardening, network defense.
* Vulnerability Management: Tenable Nessus, security patching, risk assessment, remediation strategies.
* Authentication & Identity Management: Active Directory, MFA, SSO, certificate management.
* Threat Intelligence & Forensics: OpenCTI, TheHive, YARA, malware analysis, phishing assessment, OSINT tools.
* Endpoint & Cloud Security: MDM, EDR, AWS Security, Azure Security, Sentinel, Defender for Endpoint.
* Programming & Scripting: Python, Bash, PowerShell, SQL, KQL.
* Compliance & Policy: NIST, ISO 27001, UT System security standards.

## Professional Experience

### Apple Inc., El Paso, TX

**Senior Manager** (May 2020 – May 2024)

* Led technical incident response, ensuring rapid mitigation and minimal downtime.
* Implemented security awareness training, reducing risk exposure and policy violations.
* Trained teams on security best practices, improving compliance and reducing operational risk.
* Conducted security awareness training, improving risk mitigation.

**Manager** (Jan. 2014 – May 2020)

* Supervised technical support operations, enforcing security protocols and compliance policies.
* Reduced downtime by 50% through improved incident response strategies.
* Assisted in cybersecurity investigations, documenting potential security violations.

## Certifications

* CompTIA Security+
* CompTIA Network+
* CompTIA Project+
* CompTIA A+
* Google Cybersecurity Certificate
* Linux Essentials
* ITIL 4 Foundation

## Education

**B.S. Cybersecurity & Information Assurance** (Anticipated Nov. 2025)  
Western Governors University

B.S. Graphic Design  
Art Institute of Pittsburgh

## Cybersecurity Projects & Training

**TryHackMe Training (SOC Level 1 Path in progress)**

* Conducted threat analysis, phishing investigations, and SIEM monitoring (Splunk, Elastic Stack).
* Practiced incident triage workflows, log correlation, and network security analysis.

**Home Security Lab**

* Configured IDS for network monitoring and real-time threat detection.
* Investigated phishing emails using Talos, PhishTool, and urlscan.io.
* Performed vulnerability scans using Nessus and documented remediation strategies.

**Azure Honeypot Security Lab**

* Deployed an Azure-based honeypot to log attacker behavior and analyze failed login attempts.
* Set up Microsoft Sentinel SIEM for event correlation and threat monitoring.
* Used KQL queries to analyze failed logins and attacker IPs for geographic enrichment.

## Additional Training & Interests

* Active participant in cybersecurity forums, CTF challenges, and online security labs.
* Hands-on experience with forensic tools (Autopsy, FTK Imager, Volatility, Wireshark).