ERRIK GUZMAN

Chino, Ca. • 909-437-9464 • errik.guzman@gmail.com • linkedin.com/in/errik-guzman/ • github.com/MrR3bu5

SECURITY ENGINEER — DETECTION & INCIDENT RESPONSE

Security-focused IT professional with 10+ years of enterprise and public-sector infrastructure experience, specializing in detection, incident response readiness, and operational security practices. Integrates practical security controls into production environments while balancing uptime, governance, and user impact. Maintain a hands-on cybersecurity lab focused on threat detection, log analysis, and purple-team concepts within virtualized, segmented environments. Known for strong operational discipline, clear documentation, and translating infrastructure experience into defensive security outcomes.

CORE SKILLS

Detection & Response

Incident Response • Threat Hunting • Log Analysis • Security Monitoring • MITRE ATT&CK • SIEM Concepts • Endpoint Detection & Response (EDR/XDR)

Security Operations & Infrastructure

Identity & Access Management (IAM) • Endpoint Security • Windows Server Hardening • Group Policy • Network Segmentation • VLAN Architecture • Firewall Policy Administration • VPN Support • Proxmox Virtualization • ServiceNow

Security & Governance Foundations

NIST CSF • NIST 800-61 Incident Response • CIS Critical Security Controls • ISO/IEC 27001 Concepts

Offensive Awareness (Lab-Based)

Kali Linux • Nmap • Burp Suite • Metasploit • OpenVAS • BloodHound/SharpHound • Nessus Essentials

Scripting & Utilities

PowerShell • Bash • SQL • Python • C#

PROFESSIONAL EXPERIENCE

Principal IT Analyst - City of Ontario | Nov 2024 – Present

Lead enterprise IT operations supporting citywide infrastructure and end-user services across Police, Fire, Utilities, and core municipal departments, ensuring secure and reliable service delivery in a regulated public-sector environment.

- Partner with security and infrastructure teams to strengthen identity, endpoint security, and privileged access controls
- Mentor technical staff, promoting operational discipline and security-first decision making
- Develop and standardize SOPs, policies, and workflows to improve consistency and audit readiness
- Contributed to MFA identity-verification policy and supported Okta Desktop MFA rollout
- Led Windows 11 upgrade and asset audit initiatives, improving CMDB accuracy in ServiceNow
- Supported infrastructure and identity integration during Tiburon CAD → Hexagon CAD/MPSLaw migration aligned with DOJ requirements

Parco, Inc. - Ontario, CA | Jan 2010 - Nov 2024

Progressed through roles: IT Technical Specialist → Sr. Technical Specialist → Systems Administrator

Systems Administrator | Aug 2021 - Nov 2024

Supported and secured multi-site enterprise infrastructure across CA, TX, and LA environments, aligning systems with global security standards during organizational acquisition and modernization efforts.

- Reduced endpoint vulnerabilities through phased OS upgrades and improved patching practices
- Designed secure site-to-site VPN architecture (IPsec/TLS) connecting U.S. and international operations
- Built Nutanix virtualization cluster consolidating legacy servers and improving up time
- Upgraded network to segmented Cisco architecture supporting secure traffic separation
- Implemented role-based access controls aligned with least privilege and ISO 27001 guidance
- Applied CIS-aligned workstation hardening baselines to improve endpoint resilience
- Automated reporting workflows using C#, SQL, and WPF, reducing manual processing time by ~30%

PROJECTS & LABS

Detection & Threat Hunting Home Lab

Design and maintain a segmented Proxmox-based security lab focused on defensive security concepts, log analysis, and incident response workflows.

- Practice threat detection concepts using SIEM and endpoint telemetry
- Simulate adversary behavior to understand detection gaps and response workflows
- Build enterprise-style network segmentation to mirror production security zones
- Document architecture, troubleshooting processes, and lessons learned to reinforce operational maturity

EDUCATION

University of Phoenix

- MS, Information Systems - GPA 3.98
- BS, Information Technology - GPA 3.9

CERTIFICATIONS

- TryHackMe - Cyber Security 101 (SEC1) - Feb 2026
- Security+ (SY0-701) CompTIA - Aug 2025
- Certified in Cybersecurity (CC) ISC2 - Dec 2023
- Cybersecurity First Responder - Cybersecurity Defense Initiative - Aug 2025
- ISO 27001 Lead Auditor - Sep 2025
- Cyber Security Governance, Risk & Compliance - Sep 2025
- Google Cybersecurity Certificate - Oct 2023

EXTENDED LEARNING

- TryHackMe: https://tryhackme.com/p/MrR3bu5
- HackTheBox: https://app.hackthebox.com/profile/1795061
- Cybrary: https://app.cybrary.it/browse/eguzman