

# ERRIK GUZMAN

Chino, CA • 909-437-9464 • errik.guzman@gmail.com • [linkedin.com/in/errik-guzman](https://linkedin.com/in/errik-guzman) • [mrr3bu5.github.io](https://mrr3bu5.github.io)

## SECURITY ENGINEER

I am a security focused IT leader with more than ten years supporting enterprise infrastructure and public sector environments. I focus on security engineering, detection, and incident response. My work sits between operations and defense, where stability, visibility, and fast response drive outcomes. I build and run a hands on cybersecurity lab that mirrors production systems to test detections, study attacker behavior, and improve response workflows across Windows and Linux environments.

## CORE SKILLS

### Detection and Response

Incident Response, Threat Hunting, Log Analysis, Security Monitoring, MITRE ATT&CK, SIEM Concepts, EDR and XDR

### Security Operations and Infrastructure

Identity and Access Management, Endpoint Security, Windows Server Hardening, Group Policy, Network Segmentation, Firewall Administration, Proxmox Virtualization, ServiceNow

### Security Governance Foundations

NIST CSF, NIST 800-61, CIS Critical Security Controls, ISO 27001 Concepts

### Offensive Awareness

Kali Linux, Nmap, Burp Suite, Metasploit, OpenVAS, BloodHound, Nessus Essentials

### Scripting

PowerShell, Bash, Python, SQL, C#

## PROFESSIONAL EXPERIENCE

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

- Lead enterprise IT operations across end user support, service desk, and production systems. Maintain availability, operational stability, and secure service delivery.
- Work with security and infrastructure teams to improve identity governance, endpoint protection, and privileged access processes.
- Coach and develop technical staff. Reinforce operational discipline, incident preparedness, and security focused decision making.
- Create and maintain SOPs, policies, and documented workflows to strengthen consistency and audit readiness.
- Supported MFA identity verification policy and Okta Desktop MFA rollout.
- Led Windows 11 upgrade and asset audit initiatives that improved CMDB accuracy.
- Assisted infrastructure and identity integration during CAD and MPSLaw migration aligned with DOJ requirements.

## **Parco, Inc. | Ontario, CA | Jan 2010 – Nov 2024**

Progressed through multiple technical roles supporting infrastructure, systems, and operations.

### **Systems Administrator | Aug 2021 – Nov 2024**

- Managed Windows and Linux systems that supported daily production operations.
- Applied and maintained security controls across endpoints, servers, and network infrastructure.
- Assisted with incident response through system recovery, log analysis, and root cause review.
- Strengthened reliability and security through patching, access governance, and configuration hardening.
- Acted as an escalation resource for complex operational and security incidents.
- Designed secure site to site VPN architecture connecting domestic and international operations.
- Built Nutanix virtualization cluster consolidating legacy servers.
- Automated reporting workflows using C#, SQL, and WPF.

## **PROJECTS AND LABS**

### Detection Engineering and Threat Hunting Lab

- Run a continuous security lab focused on detection engineering, threat hunting, and incident response.
- Develop and tune SIEM detections aligned to attacker behavior.
- Execute purple team testing to validate alert coverage and reduce false positives.
- Simulate intrusion scenarios across segmented Proxmox environments.
- Document architecture decisions, troubleshooting, and lessons learned.

## **EDUCATION**

- |   |                 |
|---|-----------------|
| • Master of Science: Information Systems, University of Phoenix, GPA 3.98     | <b>Dec 2019</b> |
| • Bachelor of Science: Information Technology, University of Phoenix, GPA 3.9 | <b>Oct 2017</b> |

## **CERTIFICATIONS**

- |  |                 |
|--|-----------------|
| • Cyber Security 101 (SEC1), TryHackMe                         | Feb 2026        |
| • ISO 27001 Lead Auditor, GRC Mastery                          | Sept 2025       |
| • Cyber Security Governance, Risk, and Compliance, GRC Mastery | Sept 2025       |
| • CompTIA Security+ (SY0-701), CompTIA                         | Aug 2025        |
| • Cybersecurity First Responder                                | Aug 2025        |
| • ISC2 Certified in Cybersecurity (CC), ISC2                   | Dec 2023        |
| • Google Cybersecurity Certificate, Coursera                   | <b>Oct 2023</b> |

## **EXTENDED LEARNING**

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