Jose F. Romero

JFRsec | Cybersecurity Analyst

Defensive Operations, Risk Assessment, and Security Lab Engineering

- jfromero@jfrsec.com
- (626) 671-9774
- Pasadena, CA
- Bilingual (English & Spanish)
- Portfolio: jfrsec.com
- GitHub: github.com/askpeps-jfr

EDUCATION

Bachelor of Science in Information Technology

ITT Technical Institute – West Covina, CA

CERTIFICATIONS

- Google Cybersecurity Professional Certificate | In progress
- Google AI Professional Certificate | Google (Completed May 2026)
- IBM CompTIA A+ Certification Preparation Specialization | IBM (Completed March 2025)
- Google IT Support Professional Certificate | In progress
- Foundations of Ethical Hacking, Cybercrime & SQL Injection | Simplilearn Skillup

LANGUAGES

- **English**
  Native or Bilingual Proficiency
- **Spanish**
  Native or Bilingual Proficiency

PROFESSIONAL SUMMARY

Cybersecurity Analyst and IT Systems Specialist with a B.S. in Information Technology and 20+ years of experience supporting enterprise infrastructure, multi-site networks, and large-scale endpoint deployments. Brings an operations-focused perspective to defensive security, threat modeling, security assessments, and hands-on lab engineering. Founded JFRsec and built its interactive security lab and technical portfolio at jfrsec.com.

TECHNICAL SKILLS & PLATFORMS

- **Security & Risk Frameworks:** NIST CSF, NIST SP 800-30, PASTA, STRIDE, OWASP ASVS, Attack Trees, Risk Matrices.
- **Defensive Operations & Triage:** IOC Extraction, SIEM Alert Triage, PCAP Analysis (Wireshark, tcpdump), Linux Log Triage (auth.log, grep, awk).
- **Systems & Virtualization:** Active Directory (GPO, Kerberos, SMB Signing), Linux (Debian, Ubuntu), Windows, macOS, KVM/QEMU, VMware, Nutanix, Isolated VLAN 53 Routing.
- **Database & Querying:** SQL (Log filtering, user privilege auditing, injection mitigation via prepared statements).
- **ITSM & Enterprise Tools:** ServiceNow (PDI), Kaseya VSA/BMS, ManageEngine ServiceDesk Plus, Dell KACE, Okta IAM, Duo 2FA, ThreatLocker.
- **AI & Agentic Workflows:** Autonomous Agent Workflows (Claude Code CLI, Gemini, OpenAI), Context-Aware Prompt Pipelines, Automated Incident Documentation, Technical Triage Scripting.

FEATURED CYBERSECURITY PROJECTS & SANDBOX OPS

Interactive cybersecurity sandboxes, terminal replays, triage playbooks, and the complete project catalog are available at **jfrsec.com** and **github.com/askpeps-jfr**.

Security Virtualization Range & Sandbox (Bare-Metal KVM/QEMU):

Built an isolated bare-metal KVM/QEMU security range on Ubuntu with VLAN 53 routing and internet isolation. Hardened Windows Server 2022, macOS Sonoma, and Kali Linux nodes using Active Directory GPO baselines, SMB signing, and Kerberos controls.

Botium Toys – NIST CSF Security Assessment & Compliance Audit:

Conducted a security audit for an e-commerce platform mapped to NIST CSF functions: Identify, Protect, Detect, Respond, and Recover. Identified unencrypted database PII at rest and a flat network architecture, then developed an executive risk-mitigation plan.

Jose F. Romero

CYBERSECURITY ANALYST

PROFESSIONAL EXPERIENCE

Technical Caregiver (IHSS / Hospice) and Independent Security Lab Engineer

Pasadena, CA

May 2023 – Present

- Provide dedicated in-home healthcare and hospice caregiving support for family via IHSS.
- Architected Linux KVM/QEMU security ranges, deployed Active Directory baselines, and implemented isolated VLAN boundaries to maintain hands-on security engineering skills.
- Publish open-source security tools, triage playbooks, and interactive labs through GitHub and jfrsec.com.
- Build IT service, incident, and change-management workflows in a ServiceNow Personal Developer Instance.

Helpdesk Support & Systems Analyst | Manning Kass

Los Angeles, CA

January 2023 – April 2023

- Delivered Tier II/III support across 7 sites and 1,000+ users, resolving 15–25 daily tickets through Kaseya BMS/VSA and deploying critical endpoint patches.
- Supported VMware-to-Nutanix migration and enforced access controls with Duo 2FA, LastPass, and ThreatLocker.

IT Technical Support Analyst (Contractor) | Los Angeles County DPSS

El Monte, CA

March 2021 – June 2021

- Administered deployments, maintenance, and ticket resolution across 5 regional sites serving 1,000+ personnel.
- Configured and secured endpoint systems and trained staff on remote-work platforms and telework protocols.

Helpdesk Support Agent (Contractor) | Ontellus

San Dimas, CA

June 2020 – August 2020

- Supported 500+ users across 2 facilities, resolving up to 20 daily tickets in ManageEngine ServiceDesk Plus while meeting SLAs.
- Configured and secured Android devices and Windows 10 laptops and resolved network, peripheral, and workstation issues.

Helpdesk Support Analyst (Contractor) | Public Storage Corporate

Glendale, CA

January 2020 – April 2020

- Imaged, provisioned, and deployed 300+ enterprise laptops within two weeks during the initial COVID-19 evacuation, enabling remote business continuity for corporate headquarters.
- Partnered with security and systems administrators to deploy Okta SSO and SonicWall VPN access for 300+ corporate users.
- Guided nontechnical staff through secure remote workflows, authentication policies, and home-network practices.
- Migrated 1,000+ distributed desktops to Windows 10 Pro with a 90% first-pass success rate using PsExec and remote tools.

IT Technician | Carroll, Guido & Groffman

West Hollywood, CA

September 2013 – September 2018

- Managed IT infrastructure, endpoint security, and connectivity across 2 offices supporting 40+ legal staff.
- Patched and audited Windows systems and reduced downtime through proactive hardware, print-server, and network troubleshooting.