ESTEBAN ROSALES M.

SECURITY ENGINEER | CYBERSECURITY & IT INFRASTRUCTURE

Remote (UTC−6) · Costa Rica · +506 6333 5814 · estebanrosalesmora@gmail.com · linkedin.com/in/esteban-rosales · Spanish (native) / English (B2)

PROFILE

Security engineer with 3+ years defending production infrastructure in healthcare and public-sector environments, where downtime and data exposure carry regulatory and human cost. I own the defensive layer end to end: Wazuh SIEM detection, NIST-aligned incident response, Ansible-driven hardening across Windows and Linux fleets, and network segmentation. Remote-ready and used to async work with distributed stakeholders.

CORE TECHNICAL SKILLS

Security Operations Wazuh SIEM engineering, log analysis and alert triage, threat detection, incident response (NIST 800-61), forensics support, malware analysis (static & dynamic).
Infrastructure Windows Server & Linux, Active Directory / GPO, virtualization (Proxmox VE, VMware vSphere), backup & DR (vzdump, NFS), patch management.
Networking Firewall rule design, VLAN segmentation, VPN, DNS, DHCP, monitoring, zero-trust access principles.
Automation & IaC Ansible (hardening playbooks, configuration baselines), Bash and PowerShell scripting, internal tooling development.
Offensive Security Internal penetration testing; vulnerability assessment and risk-based remediation prioritization.
Governance & Compliance NIST CSF, security policy authoring, awareness programs, audit support, reporting to non-technical stakeholders.

PROFESSIONAL EXPERIENCE

Hospital Clínica Bíblica · IT Security & Systems Specialist

Jul 2023 – Present · Liberia, Guanacaste, Costa Rica

- **Own security and infrastructure operations** across 10+ production servers and 100+ endpoints in a 24/7 healthcare environment, and author the security policies audited against NIST CSF and national data-protection law.
- **Deployed and tuned Wazuh SIEM** for centralized log collection and detection across the server fleet, cutting mean time to detect suspicious activity from days to minutes and reducing alert noise by 60%.
- **Design and enforce access-control, firewall and endpoint hardening policies** measurably shrinking the external attack surface and closing 40+ high-severity findings from internal audits.
- **Detect, contain and remediate security incidents** before escalation — handling ~15 investigations per month and documenting root cause and corrective action for each.
- **Built the organization's security awareness program** designing and delivering training to 120+ staff, plus phishing simulations to measure real exposure and target follow-up training.
- **Ran a credential-hardening campaign,** cracking weak passwords internally to demonstrate real exposure to leadership and users; accounts with crackable passwords fell from 55% to 5.8% (7 of 120).
- **Delivered an internal quoting application** with live price synchronization, replacing manual client pricing across the hospital's operational areas.

Municipalidad de Carrillo · Security Analyst

Jan 2023 – May 2023 · Guanacaste, Costa Rica

- **Ran risk and vulnerability assessments** across on-premises infrastructure, identifying 10+ findings and sequencing remediation by exploitability and business impact.
- **Designed and implemented the incident response plan** aligned to the NIST framework — the institution's first documented IR process, covering detection, containment, eradication and lessons learned.
- **Automated system hardening with Ansible** in a VMware environment, replacing manual per-host configuration and reducing baseline deployment time by over 90%.
- **Conducted internal penetration tests** and translated the findings into prioritized, plain-language technical reports for municipal leadership.
- **Responded to live security incidents** and supported forensic investigation and evidence preservation.

HOME LAB & PROJECTS

- **Wild Boar — security operations platform (in development)** — personal project consolidating incident, risk and audit tracking in one place, with a log explorer, automated detections and executive PDF reporting.
- **Proxmox VE cluster with Windows Server NFS backup target** — self-hosted virtualization lab; vzdump jobs to an NFS datastore on Windows Server, incl. UID/GID mapping, stale-mount recovery and throughput tuning.
- **Wazuh detection lab** — custom rules and decoders validated against simulated attack traffic before production rollout.
- **Windows incident-response tooling** — PowerShell triage workflows using native tooling: event logs, persistence, process/network artifacts, timeline reconstruction.

CERTIFICATIONS

- **Certified in Cybersecurity (CC)** — ISC2
- **Jr Penetration Tester** — TryHackMe
- **Systems Auditing: Detecting Cybersecurity Flaws**

EDUCATION

- **B.S. in Business Informatics** — University of Costa Rica · 2019–2022
- **English Language Program (B2)** — Instituto Estelar · 2024–2025