ROBERT PEREZ-PEREDA

r.perezpereda01@gmail.com | GitHub | LinkedIn | Blog

EDUCATION

Bachelor of Science in Cybersecurity and Information Assurance *December 2026*
Western Governors University | Online
Relevant Coursework: Network Security • Scripting & Programming • Vulnerability Analysis • Digital Forensics • Information Systems Security • Linux Foundations • Python for IT Automation (in progress)

CERTIFICATIONS/SKILLS

Certifications: CompTIA A+, Network+, Security+, Project+, ITIL 4 Foundation, LPI Linux Essentials | CySA+ in progress
Tools: Splunk, Microsoft Sentinel, KQL, Wireshark, Nmap, Metasploit, Burp Suite, PowerShell, Python, Bash, Tenable Nessus, Kibana, Elasticsearch, BloodHound, Slack, ClickUp
Networking: TCP/IP, Ports & protocols, Firewalls, VPN, DNS, IDS/IPS
Systems: Windows, Linux, Active Directory (Kerberos, domain enumeration, lateral movement), VirtualBox
Blue Team: SOC operations, alert triage, incident response, threat detection, threat hunting, SIEM log analysis, C2 detection, LOLBin identification, phishing analysis, IOC extraction, vulnerability assessment, RBAC testing, security documentation

WORK EXPERIENCE

Topflight Apps | Remote *May 2026 - Present*
QA Engineer

- Performed **security-focused QA testing** on two live platforms, including a mobile AI health app and a multi-tenant clinic web application, identifying **authentication bypasses**, **RBAC failures**, and **API access control vulnerabilities**
- Tested **AI safety and security behavior** including **prompt injection**, **cross-user data isolation**, and **access scope enforcement** on a production AI assistant, documenting findings with structured **severity triage**
- Conducted **regression and functional testing** across **authentication**, **session management**, and **role-based access control** flows, filing detailed bug reports and tracking remediation status across multiple concurrent projects
- Participated in **weekly team standups** to present **QA findings**, discuss **security issues**, and align on bug remediation priorities across cross-functional remote teams

RWS Group | Remote *June 2024 - May 2026*
AI Data Quality Auditor

- Maintained greater than **98% accuracy** across **200-500 weekly reviews** under strict deadlines, building structured documentation and analytical habits directly transferable to security operations
- Identified and flagged **5+ issues per batch** before downstream impact, demonstrating the pattern recognition and attention to detail required in alert triage and vulnerability assessment

PROJECTS

Pulse | Windows Threat Detection Platform | GitHub *April 2026*

- Built a self-hosted SOC-style platform with **25 MITRE ATT&CK-mapped detection rules** covering brute force, credential dumping, lateral movement, persistence, and defense evasion, validated by **652 automated tests**
- Developed a lightweight Windows agent shipping findings over HTTPS to a live **SOC dashboard** with alert triage workflow, multi-tenant isolation, and real-time threat monitoring

LABS & TRAINING

Splunk 2 (BOTSv2) | Advanced SOC Investigation | GitHub *March 2026*

- Investigated four attack scenarios in a simulated SOC environment: **insider threat**, **SQL injection and XSS**, **USB-delivered ransomware**, and a **nation-state APT** using PowerShell C2; decoded payloads with CyberChef and mapped findings to **MITRE ATT&CK** and the Diamond Model

Microsoft Sentinel Lab | Cloud SIEM & Threat Detection | Blog *April 2026*

- Deployed a Microsoft Sentinel workspace, connected Azure AD and threat intelligence sources, and wrote **KQL detection queries** to identify failed sign-in patterns and matches against known malicious IPs

Active Directory Lab | Full Domain Compromise | GitHub *February 2026*

- Built a Windows domain environment from scratch and attacked it end-to-end, simulating a company breach from first access to **full domain compromise**; documented the attack across 5 phases in a structured security report