Erick Cisneros Ruballos

erick.cisneros2@proton.me
https://github.com/erickcisneros1
https://www.linkedin.com/in/erickcr1/
erickcisneros.com

EXPERIENCE

Company: Log(N) Pacific 2/9/2025 - Present

Title: Cyber Security Support Analyst (Vulnerability Management & SecOps Intern)

Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations, contributing to a 100% reduction in critical, 90% in high, and 76% in medium vulnerabilities for the server team.
- Performed vulnerability assessments and risk prioritization using Tenable across Windows and Linux environments.
- Executed secure configurations and compliance audits (DISA STIG) with Tenable to meet industry standards.
- Automated remediation processes and STIG implementations using PowerShell to address critical vulnerabilities.
- Deep understanding of the "soft" side of Vulnerability Management: rapport, trust, transparency, and business need.

Security Operations:

- Performed threat hunting with EDR, detecting IoCs from brute force attacks, data exfiltration, and ransomware.
- Designed, tested, and published advanced threat hunting scenarios for incident response tabletop exercises.
- Developed custom detection rules in Microsoft Defender for Endpoint to automate isolation and investigation of compromised systems.
- Reduced brute force incidents by 100% by implementing inbound NSG/Firewall rules to limit Internet exposure.
- Created Microsoft Sentinel dashboards to monitor logon failures and malicious traffic using threat intelligence.
- Experienced with KQL (similar to SQL/SPL) which I used to query logs within the SIEM and EDR platform.

Company: Apple 08/2021 - Present

Title: Technical Expert | Technical Specialist | Sales Specialist

- Consistently achieved a **100% repair success rate**, delivering high-quality, first-time resolutions for Apple hardware and software issues in alignment with Genius Bar standards.
- Maintained one of the **highest NPS scores in the region**, reflecting exceptional customer satisfaction and trust throughout the service experience.
- Supported team development by mentoring peers on diagnostic techniques and Apple repair procedures, improving overall team capability and service consistency.

  Drove sales and customer loyalty by recommending tailored products and service solutions based on individual customer needs, resulting in increased attachment rates.

Company: Computuners 10/2020 – 03/2021

Title: Repair Technician

- Executed computer repair, hardware upgrades, and custom PC builds, ensuring optimal system performance and enhanced user experiences.
- Use extensive knowledge of hardware and software components to identify where technical issues may originate from and educate others on the team.
- Assisted clients with selecting the right technology by offering new and refurbished PCs, emphasizing both performance value and budget-conscious choices.

PROJECTS

Vulnerability Management and Threat Hunting Projects

Source: https://github.com/erickcisneros1

Platforms and Technology Used: Tenable.io, SIEM (Microsoft Sentinel), EDR (Defender for Endpoint), Azure VMs, KQL

CERTIFICATIONS

CompTIA Security+
ICS2- CC Entry-Level Cybersecurity
Coursera- Google Cyber Security
Oracle - Oracle Cloud Infrastructure 2025 Foundations Associate
Oracle - Oracle Cloud Infrastructure 2025 Certified AI Foundations Associate

EDUCATION

Bachelor of Science in Computer Science and Information Security — John Jay College of Criminal Justice, 2021
Associate of Science in Computer Information Systems — Rockland Community College, 2018

LANGUAGES

English (Native)
Spanish (Native)
French (Elementary)

ADDITIONAL SKILLS AND TECHNOLOGIES

Endpoint Detection and Response, CVE/CWE Management, CVSS Scoring, OWASP Top 10, Risk Prioritization, Vulnerability Remediation, PowerShell Scripting, BASH Scripting, Firewall/NSG Configuration, NIST 800-37: Risk Management Framework, NIST 800-53: Security and Privacy Controls, NIST 800-61: Computer Security Incident Handling Guide, NIST 800-40: Guide to Enterprise Patch Management Planning, NIST Cybersecurity Framework, PCI-DSS, GDPR, HIPAA

References available upon request.