Yasmani Castaneda

Las Vegas, NV | 7029943339 | yasmanicastaneda@proton.me

Professional Summary

Cybersecurity Engineer with hands-on experience implementing and automating detection and response workflows, tuning SIEMs, and performing vulnerability assessments. Proven track record deploying endpoint-forensics automation (CrowdStrike / Falcon), integrating third-party security APIs, and driving incident response investigations to containment and remediation. Familiar with NIST and industry best practices.

Skills

- IDS/IPS (Palo Alto)
- SIEM (Exabeam)
- Incident response, forensic collection, log analysis, threat hunting
- Programming & Automation: Python, PowerShell, REST APIs
- Vulnerability Scanner (Qualys)
- Endpoint Protection: CrowdStrike Falcon, Carbon Black, FalconRTR

Experience

Cybersecurity Engineer [CONTRACTOR] — *Link Technologies, Las Vegas, United States* (May 2025 – Present)

- Monitors security alerts and logs from various security tools and platforms, responding promptly to potential threats.
- Contribute to development and implementation of security policies and playbooks; align controls with NIST/ISO frameworks and compliance requirements.
- Collaborated with engineering, compliance, and infrastructure teams to remediate vulnerabilities and implement secure configurations.

Cybersecurity Analyst [FULL TIME] — *Credit One Bank, Las Vegas, United States* (Jun 2024 – May 2025)

- Worked as part of the SOC team, monitoring and analyzing security events, escalating incidents, and coordinating response activities.
- Administered and tuned firewalls, IDS/IPS and EDR solutions (Carbon Black, CrowdStrike); integrating logs into the SIEM for centralized detection.
- Participated in incident response playbooks, captured forensic artifacts (KAPE via FalconRTR), documented lessons learned and updated runbooks.
- Developed and deployed Python/PowerShell automation to ingest security telemetry, run detections, and generate SOC reports.
- Collaborated with cross-functional teams (network, compliance, IT) to resolve incidents and strengthen overall security posture.
- Ensured monitoring, incident response, and security controls complied with PCI DSS requirements and financial industry regulations, safeguarding sensitive payment card data.

IT End User Support [FULL TIME] — *Motional, Las Vegas, United States* (Mar 2023 – Jun 2024)

- Deploy, configure, and troubleshoot Windows, macOS, and Linux workstations, ensuring secure baseline images and endpoint hardening.
- Maintain and update IT system/process documentation, runbooks, and escalation procedures.
- Implement and enforce network security controls (VPN, DNS filtering, segmentation) and coordinate device onboarding with NAC/MDM.

IT System Technician [FULL TIME] — *Stimulus Technologies, Las Vegas, United States* (Jul 2022 – Mar 2023)

- Conduct second level support, analysis, and resolution of IT related events (breaches, outages, network issues).
- Administered Barracuda email security gateway and implemented quarantine response processes to reduce phishing risk.
- Performed AD administration and hardened user accounts (least privilege, MFA rollout support); investigated workstation incidents.

Freelance Web Developer — *Self-Employed, Las Vegas, United States* (Apr 2021 – Jul 2022)

- Designed and deployed responsive websites while applying secure coding practices such as input validation, parameterized queries, and sanitized data handling to mitigate XSS and SQL injection risks.
- Implemented role-based access controls (RBAC) and secure authentication workflows, including multi-factor authentication integrations, to protect client applications and user data.
- Conducted code reviews and vulnerability scans (e.g., OWASP ZAP) to identify and remediate security weaknesses, ensuring compliance with OWASP Top 10 and industry best practices.

Education

Bachelors in Cybersecurity and Information Assurance — Western Governors University, Salt Lake City (Jun 2021 – Nov 2023)
Fullstack Web Developer — Lambda Coding Bootcamp, Las Vegas (Sep 2019 – Feb 2020)

Certifications

- CompTIA A+ (Oct 2029)
- CompTIA Network+ (Oct 2029)
- CompTIA Pentest+ (Nov 2026)
- CompTIA Cybersecurity Analyst (CySA+) (Oct 2029)
- CompTIA Security+ (Oct 2029)
- Blue Team Level 1 (BTL1), Security Blue Team (No Expiration)

Projects

KAPE Automation — PowerShell, CrowdStrike FalconRTR, KAPE

- Developed a PowerShell automation that used the CrowdStrike FalconRTR API to remotely deploy and run KAPE across EDR-managed endpoints, automatically collect forensic artifacts, and package standardized incident reports for DFIR handoff.

Carbon Black Monthly Report — Python, Carbon Black API

- Built a Python integration that queried the Carbon Black API to generate a monthly approval/denial dashboard; automated reporting increased visibility and removed manual data pulls.

Phishlabs Case Retriever — Python, Flask, Gunicorn, NGINX, Linux

- Created an internal web service that fetched Phishlabs case details via API by case number; deployed as a resilient Linux service to speed up phishing triage.

SOC Daily Checklist Automation — Python, SIEM & vendor APIs, Excel

- Automated daily SOC operational checks and consolidated results into emailed Excel reports, reducing repetitive analyst tasks and improving team situational awareness.

National Cyber League (NCL) — Participant (2023, 2024)

- Ranked 848 / 7,934 (Top 11%). Completed penetration testing challenges in OSINT, cryptography, log & network analysis, forensics, exploitation, and web application security.

Automated Software Approval / Adult Safelist Workflow — Google Apps Script, JavaScript, Google Forms, Google Sheets, Gmail API

- Built automation for software-request approvals with Google Apps Script for Clark County School District (CCSD), eliminating manual data entry and improving traceability.