Elena M. Vasquez | Senior Cybersecurity Engineer | Cloud Security & Threat Detection

475 Brannan Street, Suite 300, San Francisco, California, United States, 94107
(415) 555-0198 • elena.vasquez@example.com • https://elenavasquez.dev
@elena-vasquez-sec • @elenavasquez • @elena-vasquez

Basics

- Cybersecurity engineer with 8+ years of experience securing cloud-native applications, enterprise networks, and high-traffic SaaS platforms.
- Specialized in threat detection, incident response, vulnerability management, and secure architecture across AWS and Azure environments.
- Adept at building automation with Python, Terraform, and SIEM tooling to reduce response time and strengthen security posture.
- Collaborates with engineering, compliance, and product teams to translate risk requirements into practical controls and measurable outcomes.

Education

Georgia Institute of Technology **https://www.gatech.edu**
Master, Cybersecurity, Score: 3.9 *Aug 2013–May 2015*

- Completed graduate coursework in secure systems, network defense, and applied cryptography.
- Built a cloud incident response lab and evaluated detection coverage for common attack paths.
- Collaborated on a capstone project focused on identity-based threat detection in hybrid environments.

Courses: Advanced Network Security, Applied Cryptography, Cloud Security Architecture, Incident Response and Forensics, Secure Software Development, Risk Management and Compliance

University of Illinois Urbana-Champaign **https://illinois.edu**
Bachelor, Computer Science, Score: 3.8 *Aug 2009–May 2013*

- Developed a strong foundation in operating systems, networking, and software engineering.
- Completed coursework projects in network protocol analysis and secure application development.
- Served as a teaching assistant for an introductory computer security course.

Courses: Data Structures, Operating Systems, Computer Networks, Database Systems, Algorithms, Software Engineering

Work

Northstar Cloud Systems **https://www.northstarcloud.io**
Staff Cybersecurity Engineer *Jan 2021–Present*

- Lead threat detection and incident response for a multi-tenant cloud platform serving enterprise customers.
- Designed detection-as-code pipelines and tuned SIEM/EDR alerts to cut mean time to investigate by 35%.
- Partnered with platform engineering to implement zero trust controls, least-privilege IAM, and secure-by-default services.
- Coordinated tabletop exercises and post-incident reviews with legal, compliance, and product stakeholders.
- Mentored security engineers and established reusable playbooks for cloud forensics and containment.

Keywords: Threat Detection, Incident Response, AWS Security, SIEM, Zero Trust

Apex Financial Technologies **https://www.apexfintech.com**
Senior Security Engineer *Mar 2017–Dec 2020*

- Owned vulnerability management and secure SDLC programs for payment and lending applications.
- Led PCI DSS remediation efforts across distributed teams and reduced critical findings by 42% year over year.
- Built Python and Splunk automations to correlate vulnerability data with asset ownership and patch status.
- Performed threat modeling, security reviews, and penetration test coordination for new product launches.

Keywords: Vulnerability Management, PCI DSS, Python, Splunk, Penetration Testing

BlueRiver Health Systems **https://www.blueriverhealth.org**

Security Analyst *Jun 2015–Feb 2017*

- Monitored and triaged security events in a 24x7 SOC supporting clinical and corporate environments.
- Investigated phishing, malware, and unauthorized access incidents and documented response actions.
- Improved endpoint detection coverage and reduced false positives through rule tuning and asset baselining.
- Assisted with HIPAA security assessments and NIST CSF gap analysis across infrastructure teams.

Keywords: SOC Operations, NIST CSF, Endpoint Security, Log Analysis, Phishing Response

Languages

English: Native or Bilingual Proficiency **Keywords**: Native speaker, Technical writing

Spanish: Full Professional Proficiency **Keywords**: Professional working, Cross-team liaison

Skills

Cloud Security: Expert **Keywords**: AWS, Azure, GCP, Terraform, IAM

Threat Detection and Response: Expert **Keywords**: SIEM, EDR, SOAR, Splunk, CrowdStrike

Application Security: Advanced **Keywords**: OWASP Top 10, SAST, DAST, Threat Modeling, Secure SDLC

Network Security: Advanced **Keywords**: Firewalls, IDS/IPS, VPN, Zero Trust, Wireshark

Programming and Automation: Advanced **Keywords**: Python, Bash, PowerShell, Go, Ansible

Governance Risk and Compliance: Advanced **Keywords**: SOC 2, ISO 27001, NIST CSF, PCI DSS, HIPAA

Awards

Outstanding Security Engineer Award

Northstar Cloud Systems *Nov 2023*

Recognized for leading the response to a high-severity cloud incident and improving detection coverage across critical services.

Capture the Flag Champion

BSides San Francisco *Sep 2019*

Placed first in a team-based enterprise security competition focused on cloud exploitation, forensics, and incident response.

Certificates

Certified Information Systems Security Professional (CISSP) **https://www.isc2.org/certifications/cissp**

ISC2 *Jun 2018*

AWS Certified Security - Specialty **https://aws.amazon.com/certification/certified-security-specialty/**

Amazon Web Services *Feb 2022*

Offensive Security Certified Professional (OSCP) **https://www.offsec.com/courses/pen-200/**

Offensive Security *Oct 2016*

GIAC Certified Incident Handler (GCIH) **https://www.giac.org/certifications/certified-incident-handler-gcih/**

SANS Institute *Mar 2020*

Publications

IEEE Security & Privacy **https://ieeexplore.ieee.org/document/9876543**

Detecting Lateral Movement in Cloud Environments *Aug 2022*

- Presents a practical detection model for identifying lateral movement across hybrid cloud workloads.
- Combines identity telemetry, network flow logs, and endpoint signals to reduce false positives.
- Includes open-source detection rules and evaluation results from a simulated enterprise environment.

Projects

PhishGuard **https://github.com/elenavasquez/phishguard**

Open-source phishing triage platform for SOC teams *Jan 2020–Jun 2021*

- Automates phishing report ingestion, enrichment, and analyst triage workflows.
- Integrates with email security APIs and ticketing systems to reduce manual effort.
- Provides dashboards for tracking recurring sender patterns and campaign trends.

Keywords: Phishing, Python, SOAR, Email Security

Cloud IAM Posture Scanner **https://github.com/elenavasquez/iam-posture-scanner**

Automated scanner for identifying risky IAM permissions in AWS *Mar 2022–Nov 2022*

- Inventories IAM roles, policies, and trust relationships across multiple AWS accounts.
- Flags excessive permissions, unused credentials, and risky cross-account access paths.
- Generates remediation guidance and exports findings to security dashboards.

Keywords: AWS, IAM, Python, Security Automation

Interests

Security Research: CTF competitions, Malware analysis, Cloud forensics

Outdoors: Trail running, Rock climbing, Backpacking

Volunteer

Bay Area Women in Cybersecurity **https://www.bawic.org**

Mentor and Workshop Instructor *Sep 2019–Present*

- Mentor early-career security professionals on cloud security fundamentals and career development.
- Deliver hands-on workshops covering detection engineering, log analysis, and incident response.
- Help organize community meetups and an annual conference track for local practitioners.