Reina Castillo Junior Cloud Security Engineer

San Francisco, CA · reina.castillo@gmail.com · +1 415-555-0162 · linkedin.com/in/reinacastillo

PROFILE SUMMARY

- **Junior Cloud Security Engineer** with **3 years** in security, now hardening the **AWS accounts** behind a **business banking platform** after **18 months in a SOC**, focused on **posture fixes and cloud alerts**.
- Works daily in **AWS** (IAM, Organizations, CloudTrail), **Wiz** for posture, **Terraform** with Checkov in GitHub Actions, **GuardDuty** and Splunk for alerts, and writes **Python** for small Lambda fixes.
- Building depth in **IAM policy review**, **S3 and KMS hardening** and **CloudTrail investigations**, checking every fix against the **CIS AWS Foundations Benchmark** so a closed finding stays closed.
- Works with **platform engineers**, the **compliance team** and the **senior cloud security engineer** on reviews, and pairs with **product teams** on the Terraform change whenever a Wiz finding lands in their queue.
- Keeps the **posture runbook** and the **GuardDuty triage notes** up to date, answers questions in the **#security-help** channel, holds **AWS Solutions Architect Associate** and is studying for **AWS Security Specialty**.

TECHNICAL SKILLS

Cloud Platforms & Frameworks:	AWS, AWS Organizations, CIS AWS Foundations Benchmark, SOC 2 (basics)
Identity & Access:	AWS IAM, IAM Identity Center, IAM Access Analyzer, Okta
CSPM & CNAPP:	Wiz, AWS Security Hub, AWS Config
Containers & Kubernetes:	Amazon ECS, Docker, Trivy (image scans)
IaC & Policy-as-Code:	Terraform, Checkov, GitHub Actions
Network & Encryption:	AWS KMS, AWS Secrets Manager, security groups, AWS WAF (basics)
Detection, Logging & Scripting:	Amazon GuardDuty, AWS CloudTrail, Splunk (SPL), Python, Bash

EDUCATION

San José State University — **B.S. in Business Administration, Management Information Systems** — San Jose, CA · Aug 2019 to May 2023

Amazon Web Services — **AWS Certified Solutions Architect Associate** — San Francisco, CA · Jun 2024

WORK EXPERIENCE

Mercury — **Junior Cloud Security Engineer** — San Francisco, CA · Feb 2025 to Present

- Worked through the **Wiz** backlog for 140 AWS accounts with service owners, fixing public bucket policies and open security groups, and cut open critical findings from **212 to 31** in 9 months.
- Reviewed IAM roles with **IAM Access Analyzer** and last-accessed data, then rewrote the 40 broadest policies to least privilege, removing **1,180 unused permissions** without breaking a single deploy.
- Triaged **Amazon GuardDuty** and CloudTrail alerts in **Splunk**, adding detections for console logins without MFA and access keys used from new countries, which cut false positives by **64%**.
- Added **Checkov** to the **Terraform** pull request checks in GitHub Actions for 30 repos, so engineers fixed **83%** of new misconfigurations themselves before anyone had to open a ticket.
- Turned on default **AWS KMS** encryption and Block Public Access for every S3 bucket, and moved **70 hardcoded API keys** into AWS Secrets Manager with rotation every 90 days.

Splunk — **Security Analyst (SOC)** — San Francisco, CA · Jul 2023 to Jan 2025

- Triaged alerts in **Splunk Enterprise Security** for the corporate SOC, checking VPC Flow Logs and firewall logs on cloud cases, and escalated **26 confirmed incidents** to incident response.
- Scanned container images in the internal build pipeline with **Trivy**, opened tickets for critical CVEs in shared base images, and got **88%** of them patched inside the 30-day window.
- Joined security reviews for 3 new AWS environments in a lab migration, checking VPC layouts and security groups, and removed **17 rules** that allowed SSH from anywhere on the internet.