Maya Torres

Cloud Security Engineer

maya.torres@cloudsecpro.dev • +1 (512) 555-0148 • Austin, TX (Remote) • linkedin.com/in/mayatorres-sec • github.com/mtorres-sec

Summary

Cloud security engineer with 8+ years hardening multi-cloud environments (AWS, Azure, GCP) for regulated fintech and SaaS organizations. Builds automated compliance pipelines mapped to SOC 2, ISO 27001, and PCI-DSS, and embeds security-as-code into CI/CD so misconfigurations are caught before they reach production. Known for turning audit findings into permanent guardrails instead of one-off fixes.

Core Competencies

Cloud Platforms & Identity
AWS (IAM, Organizations, KMS, GuardDuty, Security Hub, Control Tower), Nimbus Entra ID, GCP IAM, SAML/OIDC SSO

Compliance & Frameworks
SOC 2 Type II, ISO/IEC 27001, NIST 800-53, PCI-DSS, CIS Benchmarks

Security Tooling & SIEM
Wiz, Prisma Cloud, AWS Security Hub, Splunk, Datadog Cloud SIEM, Qualys, Tenable.io, Snyk, Trivy, Falco

DevSecOps & IaC
Terraform, CloudFormation, OPA/Gatekeeper, Checkov, tfsec, GitHub Actions, Jenkins, Kubernetes, Docker, Python, Go, HashiCorp Vault

Professional Experience

Senior Cloud Security Engineer **Mar 2022 – Present**
Nexa Cloud Solutions — Austin, TX (Remote)

- Led SOC 2 Type II and ISO 27001 certification programs across 40+ AWS accounts under an AWS Organizations landing zone, achieving zero material findings for three consecutive audit cycles.
- Architected a CSPM program using Wiz and AWS Security Hub, reducing critical misconfigurations by 78% and mean time-to-remediation from 12 days to 36 hours.
- Built policy-as-code guardrails (OPA/Gatekeeper, Checkov, tfsec) into Terraform CI/CD pipelines, blocking non-compliant infrastructure changes pre-merge across 25 engineering teams.
- Directed incident response for cloud-native security events, including containment of a compromised IAM role that limited blast radius from account-wide to a single VPC.

Cloud Security Engineer **Jul 2019 – Feb 2022**
Synapse Financial Group — Denver, CO

- Migrated legacy on-premises workloads to a multi-account AWS environment while maintaining PCI-DSS Level 1 compliance for card-processing systems.
- Deployed GuardDuty, Macie, and centralized CloudTrail logging across all accounts, cutting detection-to-alert time from 6 hours to under 10 minutes.
- Implemented least-privilege IAM via Access Analyzer and automated permission right-sizing, removing 1,900+ unused or over-scoped permissions.
- Partnered with external auditors on annual SOC 2 and PCI-DSS assessments, reducing audit prep time by 60% through evidence automation.

DevSecOps Engineer **Jun 2017 – Jun 2019**
Vertex Systems — Chicago, IL

- Embedded security scanning (Snyk, Trivy, Checkmarx) into Jenkins and GitHub Actions pipelines for 15+ microservices, cutting shipped critical vulnerabilities by 65%.
- Hardened Kubernetes clusters with Falco, network policies, and Pod Security Standards ahead of the company's first SOC 2 audit.
- Rolled out HashiCorp Vault for secrets management, eliminating hardcoded credentials across 200+ repositories.

Certifications

AWS Certified Security – Specialty • CISSP • CKS – Certified Kubernetes Security Specialist • CCSP • Terraform Associate (HashiCorp)

Education

B.S. in Computer Science **2013 – 2017**
Apex Institute of Technology — Boston, MA
Relevant coursework: Network Security, Applied Cryptography, Distributed Systems