Carlos R Gomez

Manager, Security Engineering

+1.323.620.2277
crgomez167@gmail.com
https://crgomez.com

PROFILE

Security Engineering Leader with advanced training in AI/ML and data-driven leadership. Over 11 years of experience in insider threat detection (ITD) and incident response (IR) with quantitative decision-making frameworks to drive strategic security initiatives across multidisciplinary business units.

Developed and scaled both ITD & IR programs across Amazon Devices Subsidiaries & Acquisitions (Amazon Alexa, Blink, Eero, Ring, Key, & Zoox) through data-driven risk mitigation and advanced detection capabilities.

EDUCATION

AS Behavioral & Social Science
Los Angeles Southwest College

BS Information Systems Security
Azusa Pacific University

MS Homeland Security InfoSec & Forensics
Penn State University

Professional Development

Leading in a Data-Driven World: Developing Quantitative Intuition
Columbia Business School Executive Edu.

Demystifying AI, Crash Course in AI & The Mindful Manager: Navigating Workplace Conflict
Stanford Continues Studies

TECHNICAL SKILLS

Security Engineering
Threat Hunting, Incident Response, Digital Forensics, SOAR, SIEM Platforms

AI/ML & Data Science
Business Intelligence, Risk Modeling, Predictive Analytics
Machine Learning, Anomaly Detection, Quantitative Analysis, Statistical Modeling

Leadership & Strategy
Conflict Resolution, Operational Planning, Talent Management, Resource Budgeting

EXPERIENCE

Devices Subsidiaries & Acquisitions - Manager, Insider Threat Program
Amazon I 2022 - Present

- Led cross-functional team of analysts, data scientists, and security engineers to develop enterprise-scale insider threat detection capabilities across Amazon's hardware subsidiaries (Ring, Blink, Eero) and autonomous vehicle division (Zoox). Architected centralized security analytics platform processing CloudTrail telemetry from ~4k+ AWS accounts, engineering 50+ custom threat indicators and automated correlation algorithms for real-time risk assessment.
- Developed dynamic program strategy, & program charter allowing for adaptive & technical challenges across business units, leading towards operational effectiveness, and program positioning within Amazon Enterprise Protection Program. Dynamic program modeling allowed us to anticipate business directives, while allowing us to stay on road mapping course.
- Led security initiative focused on implementing orchestration middleware security controls across Amazon's hardware subsidiaries, mitigating services from interfacing directly with Ring's ~40M Monthly Active Users through its data source owners (DSO). Designed comprehensive data governance controls for video processing, deletion, retention, and legal hold services while retaining Authentication, Authorization, and Audit capabilities throughout the data lifecycle. Successfully scaled security model to Blink and drove organization-wide adoption across multiple Amazon development teams.

RBKS - Security Engineer III, Lead Insider Threat Program
Amazon I 2020 - 2022

- Conducted case-studies highlighting security & privacy risks around potential for internalized threat actors, gaining stakeholder sponsorship (Ring CTO, COO, CISO) to develop Ring's Insider Threat Program under Defensive Security.
- Led security optimization initiatives that reduced mean time-to-detect (MTTD) and mean time-to-respond (MTTR) through implementation of a comprehensive Threat Lifecycle Management Framework and automated SOAR pipeline. Streamlined AWS CloudWatch log onboarding process, reducing deployment time from 3-4 weeks to 30 minutes and significantly decreasing operational overhead for development teams
- Architected and championed implementation of Two Person Authorization (2PA) security controls across Ring's platform, mitigating internal threat vectors for account takeover attacks. This critical security enhancement protected 35.8 million customer accounts (49.49% of user base) lacking multi-factor authentication, significantly reducing insider threat exposure and strengthening the overall security posture.

Ring – Security Engineer II, Incident Response
Amazon I 2018 - 2020

- Authored Ring's Incident Response Protocols/Procedures; built on F3EAD framework and NIST Computer Security Incident Response Guide.
- Investigate, reports of security breaches, and security related matters from both internal & external reports.
- Lead Engineering, Legal, PR, and Stakeholders through Intelligence-Driven Incident Response Cycle, ensuring assessment, containment, and incident remediation phase.
- Educated teams across Ring through; Incident Response Readiness approach: *Crises Management, Tabletops, Documentation*

EXPERIENCE

Verizon Digital Media Services -Security Analyst, Web Application Firewall

Verizon I 2018

- Managed Cloud-based Web Application Firewall (WAF) based on ModSecurity rule sets from OWSAP & Trustwave for VDMS customers running Content Delivery Networks
- Integrated python automation into security investigation workflow (ex. Identifying IPs based on anomaly scores/triggers generating global POP/WAF blacklist
- Developed effective Related System Models (MBSE) that helped define, design, and communicate system aspects to stakeholders and project ENG teams.

Google - Information Technology, Operations Support Specialist

Google I 2016 - 2018

- Provided direct and remote support to 130K+ Googlers across a Linux, OS X, Windows, Chrome OS and Android platform in addition to network-based applications.
- Diagnosed, troubleshot, triaged Google's corporate resources, application issues, and bug escalations to NetOps, SecOps, and production service teams, allocating resources, and ensuring timely resolution.

Google Cloud Platform - Full Stack Engineer (Rotation)

Google I 2017

- Optimized Google Cloud Storage partner data tracking dashboards by reducing load times by 80%.
- Developed data analytics platform for cloud infrastructure optimization, architecting a Tableau-equivalent solution that migrated legacy PLX scripts and dashboard configurations to Google BigQuery. Implemented security best practices including least privilege access controls and version control systems to ensure data governance and operational integrity.
- Developed and participated in open source project integrating Ansible with Google Cloud Platform to create and bootstrap instances, install Apache, and setup Compute