Alfe Corona

ENTERPRISE & CLOUD SECURITY · SECURITY ARCHITECTURE & RISK REDUCTION

alfe@alfecorona.com · LinkedIn · Evidence dossier

Professional summary

My work includes coordinating hardware security module remediation at Wells Fargo, leading SOC 2 audit readiness at IBM, and creating an email QA guide for Google Maps Local Guides. My independent Exposure Control project demonstrates finding prioritization, ownership routing, and closure checks with synthetic data.

Selected contributions

Wells Fargo: Coordinated HSM remediation owners, dates, status, and escalation

IBM: Led SOC 2 audit readiness with engineers and PwC auditors

Google: Created a step-by-step email QA guide for Local Guides

99.6%: Inventory validity during U.S. Navy submarine service

Read the remediation coordination case study · Scope, contribution, and evidence boundaries.

Selected professional experience

Lead Information Security Engineer, VP · Wells Fargo · Aug 2024–Present

Coordinated hardware security module (HSM) vulnerability remediation and documented an application-vulnerability process that clarified technical owners, deadlines, status, and escalation paths.

IBM · Aug 2021–Sep 2024

Senior Information Security Engineer / Cloud Security Lead · Oct 2021–Sep 2024. Led SOC 2 audit readiness for IBM Cloud's Cloud Shell, CLI, and Developer Experience teams, working with engineers and PwC auditors.

IBM Cloud Development Security Focal · Aug 2021–Aug 2022. Additional assignment: Drive to Digital Architect · Aug 2022.

Additional IBM work: coordinated security assessments and remediation across IBM Technology Lifecycle Services, documented procedures, and kept application, privacy, and incident-response teams aligned through weekly follow-ups.

Enterprise Testing / Operational Risk · Wells Fargo · Aug 2019–Aug 2021

Gathered evidence and documented logical-access provisioning processes with security engineers for internal-control testing.

Quality Assurance & Security Validation — Google Maps · Jan 2015–Aug 2019

Created a step-by-step email QA guide for Google Maps Local Guides, working with developers and the program manager to document testing procedures.

Intelligence Specialist / Supervisor · U.S. Navy Reserve · Aug 2017–Aug 2019

Served in the Navy Reserve alongside a civilian technology career.

Submarine Service, Petty Officer Third Class · U.S. Navy · 2010–2014

Maintained 99.6% inventory validity during submarine service. Earned the Navy and Marine Corps Achievement Medal.

Education and credentials

CISSP | Microsoft Certified: Azure Fundamentals (AZ-900)

M.S., Cybersecurity · Fordham University | M.S., Organizational Leadership · Nyack College (Alliance University) | B.S., Organizational Management · Nyack College (Alliance University)

Bilingual: English and Spanish

Selected cybersecurity project

Exposure Control: Cyber-Exposure Management Reference Implementation

Live portfolio · Synthetic dashboard · Verified evidence

exposure.alfecorona.com

• Designed and implemented a reference project using synthetic findings. It normalizes security findings, applies deterministic P0–P4 scoring, and creates or updates GitHub Issues that record an owner identifier, stable identity, priority, and evidence.

• Built JSON/JSONL file ingestion, a GitHub Issues workflow adapter, SQLite and PostgreSQL persistence, forced tenant row-level-security policies, schemas, dashboard generation, and idempotent workflow identities.

• Implemented a closure gate that checks tenant and exposure identity, logical source separation, evidence freshness, and a resolved outcome; the demo separates the logic inside one GitHub Actions environment.

• Added scheduled and on-demand dependency and repository scans, CI on pull requests and main updates, SHA-pinned Actions, restricted workflow-token permissions, a non-root container, and Kubernetes deployment references.

Demonstrated capabilities

Synthetic finding ingestion; policy-based prioritization; owner routing; closure validation; Python; PostgreSQL; SQLite; JSON Schema; GitHub Actions; GitHub Issues; containers; Kubernetes deployment references; dependency scans; restricted workflow permissions; and technical documentation.

Project evidence

• Successful architecture, build, type, lint, test, security, and smoke-test quality gates verified before publication.

• Implementation source is maintained privately; controlled technical review is available for legitimate hiring and due-diligence conversations.

The repository enforces a coverage gate. A single coverage percentage is intentionally omitted until statement and branch metrics are labeled consistently. These are repository checks, not customer outcomes.

alfecorona.com | LinkedIn | alfe@alfecorona.com