

Alfe Corona

ENTERPRISE SECURITY ARCHITECTURE · AI GOVERNANCE · CYBER EXPOSURE MANAGEMENT

alfe@alfecorona.com | [LinkedIn](#) | alfecorona.com

Professional summary

Enterprise cybersecurity leader with 10+ years translating security, cloud, and AI risk into secure operating models, technical controls, and executive decisions across regulated enterprise, technology, healthcare, and U.S. Navy environments. Builds repeatable systems that connect architecture, engineering, governance, and business priorities.

Measured outcomes

1,000+ - Vulnerabilities a team closed through a cryptography-focused remediation initiative I led; closure validated

~900 - Open remediation items clarified across roughly 15 teams

20+ - Professionals trained and coordinated across distributed technology teams

99.6% - Mission-critical inventory validity during U.S. Navy submarine service

[Enterprise case study: scope, contribution, and evidence](#)

Selected professional experience

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

Leads enterprise security, vulnerability, asset, compliance, and executive decision-support work across complex infrastructure and application environments.

IBM · Aug 2021-Sep 2024

Senior Information Security Engineer / Cloud Security Lead · Oct 2021-Sep 2024. Operationalized cloud-security and compliance practices and supported regulated-control readiness.

IBM Cloud Development Security Focal · Aug 2021-Aug 2022. Created reusable guidance for technical owners.

Additional assignment: Drive to Digital Architect · Aug 2022.

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

Led vulnerability, security-testing, access, and operational-risk work; trained and coordinated 20+ professionals across distributed technology teams.

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

Functional focus: quality assurance, security validation, and global release readiness for Google Maps across 27 languages.

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

Completed six strategic deterrent patrols and managed mission-critical inventory with 99.6% validity in a high-reliability operating environment.

Education and credentials

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

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

Selected cybersecurity project

Exposure Control: Cyber-Exposure Management Reference Implementation

[Exposure Control](#) | [Dashboard](#) | [Evidence](#)

- Designed and implemented a portfolio vertical slice that 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

Security architecture; threat modeling; vulnerability management; risk prioritization; remediation orchestration; Python; PostgreSQL; SQLite; JSON Schema; GitHub Actions; GitHub Issues; containers; Kubernetes references; CI/CD; secure software supply chain controls; observability; 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.