Alfe Corona

ARQUITECTURA DE CIBERSEGURIDAD - INGENIERIA DE SEGURIDAD - AUTOMATIZACION DE SEGURIDAD EN LA NUBE

alfe@alfecorona.com - exposure.alfecorona.com/es/evidence

RESUMEN PROFESIONAL

Profesional de ciberseguridad que demuestra criterio de arquitectura e implementación práctica mediante Exposure Control, una referencia de portafolio que conecta hallazgos de seguridad con prioridad explicable, responsabilidad registrada, remediación trazable y cierre condicionado por evidencia. Enfoque en automatización segura, auditabilidad y comunicación clara entre seguridad, ingeniería y riesgo.

PROYECTO SELECCIONADO DE CIBERSEGURIDAD

Exposure Control - Referencia de gestión de exposición y riesgo

- Diseñé e implementé un corte vertical de portafolio que normaliza hallazgos de seguridad, aplica scoring determinístico P0-P4 y crea o actualiza issues en GitHub con identidad estable, prioridad, responsable y evidencia.
- Construí ingestión JSON/JSONL, adaptador de workflow con GitHub Issues, persistencia en SQLite y PostgreSQL, políticas obligatorias de row-level security por tenant, esquemas, generación de dashboard e identidades idempotentes de workflow.
- Implementé una compuerta de cierre que valida tenant, identidad del hallazgo, separación lógica de fuente, vigencia de evidencia y resultado resuelto; la demo separa la lógica dentro de un ambiente de GitHub Actions.
- Agregué escaneos programados y bajo demanda de dependencias y repositorio, CI para pull requests y main, Actions con SHA fijo, permisos restringidos de workflow token, contenedor no root y referencias de despliegue en Kubernetes.

CAPACIDADES DEMOSTRADAS

Arquitectura de seguridad; modelado de amenazas; gestión de vulnerabilidades; priorización de riesgo; orquestación de remediación; Python; PostgreSQL; SQLite; JSON Schema; GitHub Actions; GitHub Issues; contenedores; referencias de Kubernetes; CI/CD; controles de cadena de suministro; observabilidad; documentación técnica.

EVIDENCIA DEL PROYECTO

- Compuertas de arquitectura, build, tipos, lint, pruebas, seguridad y smoke test verificadas antes de publicar.
- Cuatro categorías de escaneo programado y bajo demanda: dependencias, código fuente, configuración y hallazgos de secretos.
- Ciclo sintético y dashboard de decisión públicos, con filtros desde el resumen ejecutivo hasta el detalle de trabajo responsable.
- Narrativa pública de arquitectura, límites de producción y una ruta de revisión controlada; el código de implementación se mantiene privado.

El repositorio aplica una compuerta de cobertura. Se omite un porcentaje único de cobertura hasta que las métricas de statement y branch estén etiquetadas de forma consistente. Son chequeos del repositorio, no resultados de clientes.

Exposure Control es un MVP funcional de portafolio y una implementación de referencia con datos sintéticos. No representa un despliegue de cliente. La lógica de validación de la demostración corre dentro del mismo ambiente de automatización; producción requeriría identidades con permisos separados y retesteos desde fuentes autoritativas.