Engineer Asesoramiento

Análisis continuo de seguridad

Establecí un programa continuo de seguridad — análisis de código, DAST, comprobación de dependencias y vulnerabilidades, generación de SBOM, detección de secretos y acciones fijadas por SHA —, junto con 21 auditorías de seguridad documentadas.

2025

21

auditorías de seguridad escritas
junto con las automáticas

Situación. La seguridad de la aplicación — política de seguridad de contenido, roles de mínimo privilegio y revisión de derechos — protege durante la ejecución. No informa sobre lo que se publica: si una dependencia recibió una vulnerabilidad conocida el martes anterior, si se confirmó y después retiró una credencial o si una acción de terceros fijada a una etiqueta se ha convertido silenciosamente en otro código.

Tarea. La seguridad del código y de la cadena de suministro debía ser continua y automática, para que su estado fuera un resultado de compilación y no una opinión.

Acción. CodeQL realiza el análisis estático, ZAP prueba dinámicamente una instancia activa y govulncheck comprueba las dependencias Go. Cada compilación genera una lista de materiales de software con Anchore y Syft para saber qué se publica, sin reconstruirlo después. Gitleaks busca credenciales en el historial. Todas las GitHub Actions de terceros se fijan a un hash de commit en lugar de una etiqueta: lo que mantiene fija esa referencia a la dependencia aunque cambie la etiqueta. Dependabot vigila 6 ecosistemas. La automatización se acompaña de 21 auditorías escritas, incluidos un modelo de amenazas y una evaluación frente a la guía de pruebas OWASP. Los escáneres encuentran clases de problemas ya descritas; el modelo de amenazas nombra las específicas de esta plataforma.

Resultado. Una vulnerabilidad reconocida por las comprobaciones configuradas puede hacer fallar la compilación. El volumen de hallazgos es el coste real: un escáner que informa de todo enseña a ignorarlo, por lo que mantener una señal útil exige clasificación continua y no una configuración aislada.

Aplique esta experiencia a su proyecto

Utilice «Análisis continuo de seguridad» como punto de partida para un reto similar en su organización. Los servicios que respaldan este trabajo están disponibles para su proyecto. Traspasos, procedimientos operativos y manuales para que su personal pueda operar el sistema sin llamar a quien lo construyó.

Explore nuestros servicios Póngase en contacto →

Mire más allá del resultado

Lea la situación, las decisiones y el resultado de este ejemplo. Podemos hablar de qué partes se adaptan a sus restricciones y cuáles necesitan otro enfoque. Análisis continuo de seguridad — 21 auditorías de seguridad escritas junto con las automáticas

Explore nuestros servicios Póngase en contacto →

¿Quiere comprobar la seguridad en cada compilación?

Converse sobre su proyecto con la ingeniera responsable de la entrega. Acordamos por escrito el alcance, la base del precio y el traspaso antes de empezar a trabajar.

Contexto de la función: Ingeniera de seguridad. Se apoya en DevOps, Automatización y CI/CD, Fiabilidad y copias de seguridad, Seguridad y Documentación. Y ya que está aquí, también se nos da bien DevOps y automatización CI/CD, Seguridad y gestión de accesos, Seguridad de agentes de IA y Documentación técnica.

Póngase en contacto Explore nuestros servicios

Una parte de **una trayectoria más amplia** — y toda ella está en este sitio.

Cada entrada sigue la misma estructura: la situación, la tarea, lo que hicimos y lo que cambió.

Vea la trayectoria completa

Defina la mejora que necesita

Describa la decisión, las personas afectadas y las opciones ya consideradas. Podemos hacer explícitos los compromisos entre objetivos y dejar una recomendación documentada.

Vea cuánto cuesta Póngase en contacto →

¿Quiere comprobar la seguridad en cada compilación?

Pregunte por las decisiones detrás de «Análisis continuo de seguridad». Hablará con las personas que pueden explicar el trabajo y valorar su propio proyecto.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://advisory.engineer.company/es/portfolio/ran-a-continuous-security-scanning-programme/