Engineer Beratung

Kontinuierliche Sicherheitsprüfungen etabliert

Ein kontinuierliches Sicherheitsprogramm aufgebaut — Codeanalyse, DAST, Abhängigkeits- und Schwachstellenprüfungen, SBOM-Erzeugung, Geheimnissuche und per SHA festgelegte Actions — ergänzt durch 21 schriftliche Sicherheitsaudits.

2025

21

schriftliche Sicherheitsaudits neben den automatisierten Prüfungen

Situation. Die Sicherheitsmaßnahmen der Anwendung — Content-Security-Policy, minimal berechtigte Datenbankrollen und wiederholte Zugangsprüfungen — schützen zur Laufzeit. Über die ausgelieferte Software sagen sie nichts: ob eine Abhängigkeit seit letztem Dienstag eine bekannte Schwachstelle hat, Zugangsdaten committet und wieder entfernt wurden oder eine auf einen Tag festgelegte Drittanbieter-Action inzwischen anderen Code enthält.

Aufgabe. Lieferketten- und Codesicherheit sollten kontinuierlich und automatisch geprüft werden. Ihr Zustand musste ein Buildergebnis sein statt einer Einschätzung.

Massnahmen. CodeQL übernimmt statische Analyse, ZAP dynamische Tests gegen eine laufende Instanz und govulncheck die Go-Abhängigkeiten. Anchore und Syft erzeugen bei jedem Build ein Softwarekomponentenverzeichnis, damit die ausgelieferte Zusammensetzung bekannt ist und nicht später rekonstruiert werden muss. Gitleaks durchsucht die Historie nach Zugangsdaten. Jede Drittanbieter-GitHub-Action ist auf einen Commit-Hash statt einen Tag festgelegt. Dadurch bleibt dieser Verweis auf die Abhängigkeit fest, selbst wenn der Tag verschoben wird. Dependabot überwacht 6 Ökosysteme. Daneben stehen 21 schriftliche Sicherheitsaudits, einschließlich

Bedrohungsmodell und Bewertung nach dem OWASP-Testleitfaden. Scanner finden bereits beschriebene Problemklassen; im Bedrohungsmodell werden die plattformspezifischen benannt.

Ergebnis. Eine von den konfigurierten Prüfungen erkannte Schwachstelle kann den Build scheitern lassen. Die Befundmenge ist der eigentliche Aufwand. Ein alles meldender Scanner gewöhnt Menschen ans Ignorieren; ein brauchbares Signal verlangt fortlaufende Sichtung statt einmaliger Einrichtung.

Diese Erfahrung für Ihr Projekt nutzen

Nutzen Sie „Kontinuierliche Sicherheitsprüfungen etabliert“ als Ausgangspunkt für eine ähnliche Herausforderung in Ihrer Organisation. Die Leistungen hinter dieser Arbeit stehen auch für Ihr Projekt zur Verfügung. Übergaben, Betriebsanleitungen und Handbücher ermöglichen Ihren Mitarbeitenden, das System zu betreiben, ohne die ursprünglichen Entwickler anrufen zu müssen.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter das Ergebnis schauen

Lesen Sie die Situation, die Entscheidungen und das Ergebnis dieses Beispiels. Wir können besprechen, welche Teile sich auf Ihre Rahmenbedingungen übertragen lassen und welche einen anderen Ansatz erfordern. Kontinuierliche Sicherheitsprüfungen etabliert — 21 schriftliche Sicherheitsaudits neben den automatisierten Prüfungen

Unsere Leistungen entdecken Kontakt aufnehmen →

Soll Sicherheit bei jedem einzelnen Build geprüft werden?

Besprechen Sie Ihr Projekt mit der Ingenieurin, die für die Umsetzung verantwortlich ist. Wir vereinbaren Umfang, Preisgrundlage und Übergabe schriftlich, bevor die Arbeit beginnt.

Rollenkontext: Sicherheitsingenieurin. Die Arbeit baut auf DevOps, Automatisierung und CI/CD, Zuverlässigkeit und Sicherungen, Sicherheit und Dokumentation. Und wenn Sie schon hier sind: Wir sind auch ziemlich gut in DevOps- und CI/CD-Automatisierung, Sicherheits- und Zugriffsverwaltung, Sicherheit von KI-Agenten und Technische Dokumentation.

Kontakt aufnehmen Unsere Leistungen entdecken

Ein Teil einer **längeren Arbeitsbilanz** — vollständig auf dieser Website zu finden.

Jeder Eintrag folgt demselben Aufbau: die Situation, die Aufgabe, unser Vorgehen und die Veränderungen.

Alle Arbeiten ansehen

Die benötigte Verbesserung definieren

Benennen Sie die Entscheidung, die betroffenen Menschen und die bereits betrachteten Optionen. Wir können die Abwägungen deutlich machen und eine dokumentierte Empfehlung hinterlassen.

Preise ansehen Kontakt aufnehmen →

Soll Sicherheit bei jedem einzelnen Build geprüft werden?

Fragen Sie nach den Entscheidungen hinter „Kontinuierliche Sicherheitsprüfungen etabliert“. Sie sprechen mit den Menschen, die die Arbeit erklären und Ihr eigenes Projekt einschätzen können.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://advisory.engineer.company/de/portfolio/ran-a-continuous-security-scanning-programme/