Engineer Rådgivning

Har kørt et løbende sikkerhedsscanningsprogram

Har etableret et løbende sikkerhedsprogram — code scanning, DAST, afhængigheds- og sårbarhedstjek, SBOM-generering, secret scanning og SHA-pinnede actions — sammen med 21 skriftlige sikkerhedsgennemgange.

2025

21

skriftlige sikkerhedsgennemgange
ved siden af de automatiske

Situation. Sikkerhedsarbejdet inde i applikationen — Content-Security-Policy'en, least-privilege-databaserollerne, den gentagne kontrol af rettigheder — beskytter platformen under kørsel. Intet af det siger noget om det, der bliver leveret: om en afhængighed fik en kendt sårbarhed i tirsdags, om en adgangsoplysning blev committet og rullet tilbage, eller om en action fra en tredjepart, der er låst til et tag, i det stille er blevet til et andet stykke kode.

Opgave. Sikkerheden i forsyningskæden og koden skulle være løbende og automatiseret, så status var et buildresultat og ikke en holdning.

Handling. Statisk analyse kører gennem CodeQL, dynamisk test mod en kørende instans gennem ZAP, og Go-afhængigheder tjekkes med govulncheck. En SBOM genereres ved hvert build med Anchore og Syft, så man ved, hvad der blev leveret, i stedet for at skulle rekonstruere det bagefter. Gitleaks gennemsøger historikken efter adgangsoplysninger. Hver GitHub Action fra en tredjepart er låst til en commit-hash og ikke til et tag, hvilket holder referencen til afhængigheden fast, selv hvis tagget flyttes. Dependabot holder øje med 6 økosystemer. Ved siden af automatiseringen ligger 21 skriftlige sikkerhedsgennemgange, heriblandt en trusselsmodel og en vurdering op mod

OWASP-testguiden — for scannere finder de typer problemer, som nogen allerede har beskrevet, og det er i en trusselsmodel, at de problemer, der er særlige for netop denne platform, får et navn.

Resultat. En sårbarhed, som de konfigurerede tjek genkender, kan få buildet til at fejle. Mængden af fund er den reelle pris — en scanner, der rapporterer alt, lærer folk at ignorere den, og at holde signalet brugbart kræver løbende triage og ikke en engangsopsætning.

Brug erfaringen i jeres projekt

Brug »Har kørt et løbende sikkerhedsscanningsprogram« som udgangspunkt for en lignende udfordring i jeres organisation. Ydelserne bag arbejdet kan også bruges i jeres projekt. Overdragelser, driftsvejledninger og manualer, der lader jeres egne folk drive systemet uden at ringe til den, der byggede det.

Se vores ydelser Kontakt os →

Se bag resultatet

Læs om situationen, beslutningerne og resultatet i eksemplet. Vi kan drøfte, hvad der passer til jeres vilkår, og hvad der kræver en anden tilgang. Har kørt et løbende sikkerhedsscanningsprogram — 21 skriftlige sikkerhedsgennemgange ved siden af de automatiske

Se vores ydelser Kontakt os →

Vil du have sikkerheden tjekket ved hvert eneste build?

Tal om jeres projekt med den ingeniør, der har ansvaret for leverancen. Vi aftaler omfang, prisgrundlag og overdragelse skriftligt, før arbejdet begynder.

Rolle i opgaven: Sikkerhedsingeniør. Det trækker på DevOps, Automatisering & CI/CD, Driftssikkerhed & backup, Sikkerhed og Dokumentation. Og når I alligevel er her, er vi ret dygtige til DevOps & CI/CD-automatisering, Sikkerhed & adgangsstyring, Sikkerhed for AI-agenter og Teknisk dokumentation.

Kontakt os Se vores ydelser

Ét stykke af **en længere fortegnelse** — og det hele ligger her på sitet.

Hver post er skrevet på samme måde: situationen, opgaven, hvad vi gjorde, og hvad der ændrede sig.

Se hele fortegnelsen

Definér den ønskede forbedring

Medbring beslutningen, de berørte mennesker og de overvejede muligheder. Vi kan gøre afvejningerne tydelige og efterlade en dokumenteret anbefaling.

Se, hvad det koster Kontakt os →

Vil du have sikkerheden tjekket ved hvert eneste build?

Spørg til beslutningerne bag »Har kørt et løbende sikkerhedsscanningsprogram«. I taler med mennesker, der kan forklare arbejdet og vurdere jeres eget projekt.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://advisory.engineer.company/da/portfolio/ran-a-continuous-security-scanning-programme/