Engineer Rådgivning

Drev ett löpande program för säkerhetsskanning

Etablerade ett kontinuerligt säkerhetsprogram — kodskanning, DAST, kontroller av beroenden och sårbarheter, generering av SBOM, skanning efter hemligheter och SHA-låsta actions — vid sidan av 21 skriftliga säkerhetsgranskningar.

2025

21

skriftliga säkerhetsgranskningar,
vid sidan av de automatiserade

Situation. Säkerhetsarbetet i applikationen — innehållssäkerhetspolicyn, databasrollerna med minsta möjliga behörighet, de upprepade behörighetskontrollerna — skyddar plattformen under körning. Inget av det säger något om det som levereras: om ett beroende fick en känd sårbarhet i tisdags, om en inloggningsuppgift committades och sedan togs bort igen, eller om en action från tredje part som är låst till en tagg i tysthet har blivit en helt annan kodbit.

Uppgift. Säkerheten i leveranskedjan och i koden måste vara kontinuerlig och automatiserad, så att dess tillstånd var ett byggresultat och inte en åsikt.

Handling. Statisk analys körs med CodeQL, dynamisk testning mot en körande instans med ZAP, och Go-beroenden skannas med govulncheck. En materialförteckning för programvaran genereras vid varje bygge med Anchore och Syft, så att det som levererades är känt i stället för rekonstruerat i efterhand. Gitleaks söker igenom historiken efter inloggningsuppgifter. Varje GitHub Action från tredje part är låst till en commit-hash i stället för en tagg, vilket håller referensen till beroendet fast även om taggen flyttas. Dependabot bevakar 6 ekosystem. Vid sidan av automatiseringen finns 21 skriftliga säkerhetsgranskningar, däribland en hotmodell och en bedömning mot OWASP:s

testguide — eftersom skannrar hittar de kategorier av problem som någon redan har beskrivit, och en hotmodell är där de problem som är specifika för den här plattformen får ett namn.

Resultat. En sårbarhet som de konfigurerade kontrollerna känner igen kan få bygget att misslyckas. Mängden fynd är den verkliga kostnaden — en skanner som rapporterar allt lär folk att ignorera den, och att hålla signalen användbar kräver löpande triagering i stället för en engångsinstallation.

Använd erfarenheten i ert projekt

Använd ”Drev ett löpande program för säkerhetsskanning” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Överlämningar, driftinstruktioner och manualer som låter din egen personal driva systemet utan att ringa den som byggde det.

Se våra tjänster Hör av er →

Se bakom resultatet

Läs om situationen, besluten och resultatet i exemplet. Vi kan diskutera vad som passar era förutsättningar och vad som kräver ett annat angreppssätt. Drev ett löpande program för säkerhetsskanning — 21 skriftliga säkerhetsgranskningar, vid sidan av de automatiserade

Se våra tjänster Hör av er →

Vill du få säkerheten kontrollerad vid varje enskilt bygge?

Prata om ert projekt med ingenjören som ansvarar för leveransen. Vi avtalar omfattning, hur priset beräknas och överlämning skriftligt innan arbetet börjar.

Roll i uppdraget: Säkerhetsingenjör. Det bygger på DevOps, Automatisering och CI/CD, Tillförlitlighet och säkerhetskopiering, Säkerhet och Dokumentation. Och nu när ni är här: vi är ganska bra på DevOps och CI/CD-automatisering, Säkerhet och behörighetshantering, Säkerhet för AI-agenter och Teknisk dokumentation.

Hör av er Se våra tjänster

En del av **en längre historik** — och den finns i sin helhet här.

Varje post är skriven på samma sätt: situationen, uppgiften, vad vi gjorde och vad som förändrades.

Se hela historiken

Definiera förbättringen ni behöver

Ta med beslutet, människorna som berörs och alternativen som övervägts. Vi kan tydliggöra avvägningarna och lämna en dokumenterad rekommendation.

Se vad det kostar Hör av er →

Vill du få säkerheten kontrollerad vid varje enskilt bygge?

Fråga om besluten bakom ”Drev ett löpande program för säkerhetsskanning”. Ni talar med personer som kan förklara arbetet och bedöma ert eget projekt.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://advisory.engineer.company/sv/portfolio/ran-a-continuous-security-scanning-programme/