Engineer Rådgivning

Drev et løpende program for sikkerhetsskanning

Etablerte et kontinuerlig sikkerhetsprogram — kodeskanning, DAST, kontroll av avhengigheter og sårbarheter, SBOM-generering, skanning etter hemmeligheter og SHA-låste actions — sammen med 21 skriftlige sikkerhetsrevisjoner.

2025

21

skriftlige sikkerhetsrevisjoner,
ved siden av de automatiserte

Situasjon. Sikkerhetsarbeidet i applikasjonen — Content Security Policy, databaseroller med minste privilegium, de gjentatte rettighetskontrollene — beskytter plattformen under kjøring. Ingenting av det sier noe om det som faktisk blir levert: om en avhengighet fikk en kjent sårbarhet sist tirsdag, om påloggingsinformasjon ble committet og så tilbakestilt, eller om en tredjeparts action som er låst til en tagg, i det stille har blitt en helt annen kodebit.

Oppgave. Sikkerheten i forsyningskjeden og koden måtte være kontinuerlig og automatisert, slik at tilstanden var et byggresultat og ikke en mening.

Handling. Statisk analyse kjøres gjennom CodeQL, dynamisk testing mot en kjørende instans gjennom ZAP, og Go-avhengigheter kontrolleres med govulncheck. En stykkliste for programvaren genereres ved hver bygging med Anchore og Syft, slik at det som ble levert, er kjent i stedet for rekonstruert i ettertid. Gitleaks skanner historikken etter påloggingsinformasjon. Hver tredjeparts GitHub Action er låst til en commit-hash i stedet for en tagg, noe som holder referansen til avhengigheten fast selv om taggen flyttes. Dependabot overvåker 6 økosystemer. Ved siden av automatiseringen ligger 21 skriftlige sikkerhetsrevisjoner, inkludert en trusselmodell og en vurdering opp mot OWASP-testveiledningen — fordi skannere finner de problemklassene noen allerede har beskrevet, og en trusselmodell er der de som er spesifikke for denne plattformen, får et navn.

Resultat. En sårbarhet som de konfigurerte sjekkene gjenkjenner, kan få byggingen til å feile. Mengden funn er den egentlige kostnaden — en skanner som rapporterer alt, lærer folk å ignorere den, og å holde signalet brukbart krever løpende triagering i stedet for et engangsoppsett.

Bruk erfaringen i prosjektet deres

Bruk «Drev et løpende program for sikkerhetsskanning» som utgangspunkt for en lignende utfordring i organisasjonen deres. Tjenestene bak arbeidet er tilgjengelige for prosjektet deres. Overleveringsdokumenter, driftsinstrukser og håndbøker som lar dine egne ansatte drifte systemet uten å ringe den som bygde det.

Se tjenestene våre Ta kontakt →

Se bak resultatet

Les om situasjonen, beslutningene og resultatet i eksemplet. Vi kan drøfte hva som passer deres rammer, og hva som krever en annen tilnærming. Drev et løpende program for sikkerhetsskanning — 21 skriftlige sikkerhetsrevisjoner, ved siden av de automatiserte

Se tjenestene våre Ta kontakt →

Vil du ha sikkerheten kontrollert ved hvert eneste bygg?

Snakk om prosjektet med ingeniøren som har ansvaret for leveransen. Vi avtaler omfang, prisgrunnlag og overlevering skriftlig før arbeidet begynner.

Rolle i oppdraget: Sikkerhetsingeniør. Det bygger på DevOps, Automatisering og CI/CD, Pålitelighet og sikkerhetskopier, Sikkerhet og Dokumentasjon. Og nå som dere er her: vi er ganske gode på DevOps og CI/CD-automatisering, Sikkerhet og tilgangsstyring, Sikkerhet for AI-agenter og Teknisk dokumentasjon.

Ta kontakt Se tjenestene våre

Ett stykke av **en lengre oversikt** — og den ligger i sin helhet her.

Hver oppføring er skrevet på samme måte: situasjonen, oppgaven, hva vi gjorde, og hva som endret seg.

Se hele oversikten

Definer forbedringen dere trenger

Ta med beslutningen, menneskene som berøres og alternativene som er vurdert. Vi kan tydeliggjøre avveiningene og etterlate en dokumentert anbefaling.

Se hva det koster Ta kontakt →

Vil du ha sikkerheten kontrollert ved hvert eneste bygg?

Spør om beslutningene bak «Drev et løpende program for sikkerhetsskanning». Dere snakker med folk som kan forklare arbeidet og vurdere deres eget prosjekt.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://advisory.engineer.company/nb/portfolio/ran-a-continuous-security-scanning-programme/