Engineer Advisory

Ran a continuous security scanning programme

Established a continuous security programme — code scanning, DAST, dependency and vulnerability checks, SBOM generation, secret scanning and SHA-pinned actions — alongside 21 written security audits.

2025

21

written security audits, beside the automated ones

Situation. The security work in the application — the content security policy, the least-privilege database roles, the entitlement re-checks — protects the platform at runtime. None of it says anything about the thing being shipped: whether a dependency picked up a known vulnerability last Tuesday, whether a credential was committed and reverted, or whether a third-party action pinned to a tag has quietly become a different piece of code.

Task. Supply chain and code security had to be continuous and automated, so the state of it was a build result rather than an opinion.

Action. Static analysis runs through CodeQL, dynamic testing against a live instance through ZAP, and Go dependencies are checked with govulncheck. A software bill of materials is generated on every build with Anchore and Syft, so what shipped is known rather than reconstructed later. Gitleaks scans history for credentials. Every third-party GitHub Action is pinned to a commit hash rather than a tag, which keeps that dependency reference fixed even if the tag moves. Dependabot watches 6 ecosystems. Alongside the automation sit 21 written security audits, including a threat model and an assessment against the OWASP testing guide — because scanners find the classes of problem someone has already described, and a threat model is where the ones specific to this platform get named.

Result. A vulnerability recognised by the configured checks can fail the build. The volume of findings is the real cost — a scanner that reports everything trains people to ignore it, and keeping the signal usable takes ongoing triage rather than a one-time setup.

Bring this experience to your project

Use “Ran a continuous security scanning programme” as a starting point for a similar challenge in your organisation. The services behind this work are available for your project. Handovers, runbooks and manuals that let your own staff operate the system without ringing whoever built it.

Explore our services Get in touch →

Look behind the result

Read the situation, decisions and result in this example. We can discuss which parts transfer to your constraints and which need another approach. Ran a continuous security scanning programme — 21 written security audits, beside the automated ones

Explore our services Get in touch →

Want security checked on every single build?

Talk through your project with the engineer responsible for delivery. We agree the scope, price basis and handover in writing before work begins.

Role context: Security Engineer. It draws on DevOps, Automation & CI/CD, Reliability & Backups, Security and Documentation. And while you are here, we are rather good at DevOps & CI/CD Automation, Security & Access Management, AI Agent Security and Technical Documentation.

Get in touch Explore our services

One piece of **a longer record** — and it is all on this site.

Every entry is written the same way: the situation, the task, what we did and what changed.

See the whole record

Define the improvement you need

Bring the decision, the people affected and the options already considered. We can make the tradeoffs explicit and leave a documented recommendation.

See what it costs Get in touch →

Want security checked on every single build?

Ask about the decisions behind “Ran a continuous security scanning programme”. You will speak with the people who can explain the work and assess your own project.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

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

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://advisory.engineer.company/portfolio/ran-a-continuous-security-scanning-programme/