Engineer 技術助言

継続的なセキュリティ検査を運用

コード検査、DAST、依存関係・脆弱性検査、SBOM生成、秘密情報検査、SHA固定のActionsと、21件の文書によるセキュリティ監査を組み合わせた継続的なセキュリティ活動を確立した。

2025

21

自動監査に加えて文書化したセキュリティ監査

状況. CSP、最小権限DBロール、利用権限再検証などは実行時を守るが、配布物については何も示さない。先週判明した依存先の脆弱性、コミット後に取り消された認証情報、タグ固定の外部Actionが別コードに変わった可能性は、別の問題だった。

題. サプライチェーンとコードの安全性を、意見でなくビルド結果として示せるよう、継続的に自動検査する必要があった。

動. CodeQLで静的分析、ZAPで稼働環境への動的試験、govulncheckでGo依存先を検査した。毎ビルドでAnchore・SyftのSBOMを生成し、後で推定せず配布内容を把握する。Gitleaksで履歴内の認証情報を探し、第三者GitHub Actionは移動可能なタグでなくコミットハッシュへ固定した。Dependabotは6つのエコシステムを監視する。自動化と並行して、脅威モデルとOWASP試験ガイドに基づく評価を含む21件の監査を文書化した。検査器は既知の問題を探すもので、この基盤特有の問題は脅威モデルで名指しする必要があるためだった。

果. 設定した検査が認識した脆弱性によって、ビルドを失敗させられるようになった。実際の費用は指摘量である。何でも報告する検査器は無視を学習させるため、有用な情報を保つには一度の設定ではなく、継続的な選別が必要だった。

この経験をお客様のプロジェクトに

「継続的なセキュリティ検査を運用」を、お客様の組織の似た課題を考える出発点にしてください。この実績を支えたサービスを、お客様のプロジェクトにも提供できます。 構築した人に電話しなくても自社の担当者が運用できるよう、引き継ぎ資料、運用手順書、マニュアルを整えます。

サービスを見る お問い合わせ →

結果の背景を確かめる

この事例の状況、判断、結果をご覧ください。どの部分がお客様の制約の下でも生かせるか、どこに別の方法が必要かをご相談いただけます。 継続的なセキュリティ検査を運用 — 21 自動監査に加えて文書化したセキュリティ監査

サービスを見る お問い合わせ →

ビルドのたびにセキュリティを確認したいですか？

納品を担当するエンジニアに、プロジェクトについてご相談ください。着手前に、業務範囲、価格の算定方法、引き継ぎ内容を書面で合意します。

担当した役割：セキュリティエンジニア。 関連する分野： DevOps, 自動化・CI/CD, 信頼性・バックアップ, セキュリティ および 文書作成. こちらのサービスも得意としています DevOps・CI/CD自動化, セキュリティ・アクセス管理, AIエージェントのセキュリティ および 技術文書の作成.

お問い合わせ サービスを見る

より多くの実績の **一つです** — そのすべてをこのサイトで公開しています。

どの項目も、状況、課題、実施内容、変化という同じ構成で記載しています。

すべての実績を見る

必要な改善を定める

必要な判断、影響を受ける人々、すでに検討した選択肢をお知らせください。選択に伴う利点と不利益を明確にし、推奨案を文書に残せます。

料金を見る お問い合わせ →

ビルドのたびにセキュリティを確認したいですか？

「継続的なセキュリティ検査を運用」の判断の背景についてお尋ねください。仕事内容を説明し、お客様のプロジェクトを検討できる担当者が対応します。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

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

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://advisory.engineer.company/ja/portfolio/ran-a-continuous-security-scanning-programme/