Engineer

{ AIエージェントのセキュリティ }

AIが扱ってよいものだけを扱わせる

各エージェントのアクセスを必要な範囲に限定し、エージェント自身が改変できない場所に操作を記録し、安全策を信じるだけでなく検証します。

必要なことを整理している段階ですか？

うまくいっていないことや、つくりたいものをお聞かせください。何が必要か、おおよそいくらかかるか、私たちが適任かどうかをお伝えします。

時間単価は1,400 DKKから（VAT別）で、ご依頼期間が長いほど下がります。

お問い合わせ　料金を見る

このサービスに関する実績を抜粋してご紹介します。

サービスを成果につなげる

「AIエージェントのセキュリティ」を事業の成果につなげましょう。技術的な作業を、それが支えるべき利用者、運用、意思決定に結び付けるお手伝いをします。 各エージェントのアクセスを必要な範囲に限定し、エージェント自身が改変できない場所に操作を記録し、安全策を信じるだけでなく検証します。

お問い合わせ

関連する実績を確かめる

このページの関連実績から、私たちの取り組み方をご確認ください。それぞれの成果の背景にある条件や、何を優先して何を見送ったかについてもお尋ねください。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成　お問い合わせ →

Linuxサーバーを守る1,000件のRBACルールを作成

開発者、アプリケーションインスタンス、PostgreSQL、MS SQL、その他のLinuxサーバーに1,000件のRBACルールを実装して不正アクセスを防ぎ、データセキュリティを強化。Ansibleによる自動化として記録した。

M365・SSO全体のアクセス管理を主導

M365、1Password、Red Hat SSO、OKTA SSOを用いたアクセス管理を主導し、セキュリティ侵害を防いだ。

異常時拒否のレート制限・不正利用対策を構築

Redisによる22個のレートリミッター、Cloudflare Turnstile、リクエストの冪等性、オリジン制限を備え、異常時は拒否する不正利用対策を構築し、呼び出し元を無条件に信頼せずボットや大量アクセスを排除した。

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。

3つあったが、どれも機能していなかった防御

一度も機能していなかったSSH総当たり攻撃対策を3件発見・修正。デーモンが1986番で待ち受けるのに22番を監視する遮断jail、上位の広いルールに隠されたレート制限、バイナリを解決できず遮断を一度も実行できなかったアクションを直した。

実行ごとに侵入元の遮断を実証

堅牢化の実行ごとに、予約済みテストアドレスを遮断し、生成されたカーネルルールを読み、必ず実行する後処理で遮断を解除する一連の検証を設け、jailの故障が正常報告ではなく実行失敗になるようにした。

秘密情報の1秒の事前検査を追加

本番実行が9番目のタスクで停止し、すでにスワップ設定が稼働ホストへ書き込まれた事態を受け、運用担当者のローカルな秘密情報に対し、収束処理と同じコードを約1秒で実行する事前検査プレイを追加した。

認証情報漏出後に対象範囲の規則を記述

構成変更によって別会社の資産一覧、ファイアウォール許可、文章が混入したことを受け、リポジトリの対象範囲を定める規則を記述し、隔離した残存物も除外せず秘密情報検査の対象に残した。

すべての運用秘密情報をホストごとに分離

2ホストで1つのデッドマンズスイッチを共有すると2つのスイッチより監視能力が下がり、バックアップのパスフレーズ共有では、リポジトリが別々でも、そのパスフレーズを入手し、両リポジトリの暗号化データと鍵ファイルを読める相手が2ホストのバックアップを復号できることを確認し、ホストごとの運用秘密情報4つを分離した。

AIエージェントのセキュリティをお探しですか？

リンク先の実績から、必要な経験があるかをご判断ください。つくりたいものをお聞かせいただければ、業務範囲、進め方、引き継ぎについてご相談いただけます。

お問い合わせ すべての実績

発注前に業務範囲を定める

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

要件について話し合う

「AIエージェントのセキュリティ」に求めることを、納期や保守を担当するチームも含めてお聞かせください。実行可能な進め方をご相談いただけます。

お問い合わせ

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://engineer.company/ja/services/ai-security/