Engineer

セキュリティ

44 件の実績

システムの各部分を結び付ける

「セキュリティ」に分類した実績は、稼働するシステムの一部分を示しています。その部分を他の業務につなげるお手伝いをします。 会社全体を支えるデータベースについて、稼働、バックアップ、気づかないうちに進む劣化まで責任を持って管理します。

サービスを見る お問い合わせ →

比較できる課題を探す

ご自身の状況に近い事例をご覧ください。振り返りでは、技術名だけでは分からない、結果を導いた判断を説明しています。 PostgreSQL・MS SQL・BigQueryのデータウェアハウス100個を運用 — 100設計・運用したデータウェアハウス

PostgreSQL・MS SQL・BigQueryのデータウェアハウス100個を運用 お問い合わせ →

PostgreSQLでGIS地図を10倍に高速化

データの切り替えを含め、データベースをMSSQLからPostgreSQLへ計画的に移行。処理とデータセキュリティを最適化し、地図アプリケーションの性能を10倍に向上させた。

UbuntuでPostgreSQL・MS SQLサーバー10台を運用

Ubuntu Linux VPS上にPostgreSQL・MS SQLサーバー10台を設計・デプロイ・保守し、性能と信頼性を維持した。

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。

Ubuntu Linux VPSインスタンス30台を管理

Ubuntu Linux VPSインスタンス30台を管理し、災害復旧方針の実装とネットワーク構成の最適化を行った。

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。

WireGuard・IPsec VPN接続8本を管理

WireGuard VPN・IPsec VPNの8接続を管理して問題に対処し、Google CloudとLinuxシステム間の安全な通信を確保した。

チームの意思疎通と協働を改善

Slack、Mattermost、1Password、Jiraを導入してチームの意思疎通と協働を改善し、8,000時間の作業を削減した。

ネットワークインフラを管理

1,000台を超えるサーバーのネットワークインフラを管理し、適切なシステム構築、セキュリティ、障害対応を行った。

Dockerアプリ100個のSSL/TLS証明書を自動化

Dockerアプリケーション100個のSSL/TLS証明書の作成を自動化し、Ubuntu Linuxホスト上での安全な接続を確保した。

Wi-Fiルーター1,000台を設定・導入

1,000台のWi-Fiルーターを設定・導入し、顧客のネットワーク接続性と性能を改善した。

利用者の組織コンテキスト切り替えを構築

クライアントのlocalStorageとサーバー側Cookieへの複製を用いて組織の操作コンテキストを切り替える仕組みを設計し、最小権限の認可を維持しながら管理対象の組織として操作できるようにした。

切り替えと配信ログを備えるメール機能を構築

メール送信をプラットフォームの共通機能として構築。3つのプロバイダーによるフェイルオーバー、配信Webhook、送信・配信ログ、テンプレート、キャンペーンを備え、送信手段がなければ起動を拒否する検査を設けた。

PostgreSQL関数中心のデータ層を設計

34スキーマにまたがる1,275個のストアド関数を持つ、PostgreSQL関数中心のデータ層を設計。すべての読み書きをテーブル直接操作ではなく、データベースで実行権限を付与できる関数経由にした。

Azureインフラをコードとして構築

Bicepで、開発・ステージング・本番の各環境に、Container Apps、PostgreSQL Flexible Server、Front Door/WAF、ネットワークを含むAzureインフラをコードとして構築した。

GitHub Actions CI/CDパイプラインを構築

本番フロントエンド用のdistrolessイメージと複数環境間の昇格を備えた、GitHub ActionsのCI/CDパイプラインを構築した。

Azureへのプラットフォーム導入を一貫して担当

プラットフォームのAzureへのデプロイを最初から最後まで担当し、開発・ステージング・本番環境のリリースを管理した。

nonce付きCSPでアプリケーションを堅牢化

nonce付きCSP、HSTS、SameSite Cookie、最小権限のデータベースロール、サーバー側の利用権限再検証により、アプリケーションを堅牢化した。

プラットフォームの基礎技術方針を策定

2025年11月のリポジトリ開設後の数週間に、多層構成、データベース中心のデータアクセス、警告ゼロという基礎方針を定め、9か月後も維持した。

基幹インフラ全体を一から構築

グリーンエネルギー分野のSaaSスタートアップで初期に採用された社員の1人として、基幹インフラ全体と運用工程を一から設計・構築し、急成長の基盤を整えた。

チームの協働を自動化

チームの協働、パスワード管理、タスク・時間管理を自動化し、プロジェクト実績を半自動で紹介する仕組みも構築して、チームの生産性を高めた。

全社共通のパスワード管理を導入

全社共通のパスワード管理システムを導入し、セキュリティを強化してアクセス管理を効率化した。

Stripe・アプリ内購入の利用権限を構築

StripeとApple・Googleのアプリ内購入に対応する決済・利用権限層を構築し、サーバーで検証する11テーブルのアクセスモデルによって、一覧、検索、エクスポートの利用を制御した。

独自のエラー監視・トレースを構築

ペイロードの無害化、急増・再発の検知、シンボル解決、擬似ハートビートを備える独自のエラー監視とOpenTelemetryトレースを外部購入せず構築し、11画面の運用ビューから扱えるようにした。

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。

企業所有権の申請・審査を構築

利用者による企業所有権の申請から管理者の審査までを実装し、承認時に編集権限を決める認可グラフが更新される、一連の仕組みを構築した。

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。

SSHの24設定項目を検証・堅牢化

SSHの24設定項目を、候補ファイル、統合済み設定、デーモン自身の読み戻しによる3段階で検証するよう堅牢化。読み戻しによって、稼働中のサーバーが24項目のうち2項目を黙って上書きしていたことを検出した。

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。

ファイアウォールルールを位置で検証

存在するルールが実際のパケットに到達されるとは限らないため、番号付きルール一覧と稼働中のパケットフィルターチェーンを読み、ファイアウォールルールを存在だけでなく位置で検証した。

復元方法を明示したバックアップ自動化

resticのバックアップを、保持期間、整合性検査、毎月の復元テストとともに自動化し、ストレージの有効化と実環境での復元検証を別の運用手順として記録した。

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。

20レコードのDNSゾーンをコードで照合

20レコードのDNSゾーンをCloudflare APIと宣言的に照合し、監査とBIND形式の書き出しを別の実行入口として提供。CDNプロキシは構築後、プライバシーの観点から再び無効にした。

全ユニットのsystemdサンドボックス露出を低減

この基盤が導入するすべてのユニットのsystemdサンドボックスの露出度を低減。デッドマンズスイッチのサービスを9.6 UNSAFEから1.5へ、インターネット公開のgitホスティングを8.3 EXPOSEDから1.5へ改善し、3つのユニットテンプレートで黙って無視されていた設定名の誤記を受け、収束時の構文検査を加えた。

PodmanとQuadletでコンテナを運用

Dockerの既定のブリッジネットワークでのポート公開がUFWルールを迂回する場合があるため、systemd配下のPodman・Quadletでコンテナ基盤を構築。デプロイにはrootではなく、固定コマンド1つを使う非特権ユーザーを用いた。

2台目のサーバーをコードで構築

別のクラウド事業者で2台目のサーバーの構築を自動化。先にファイアウォールを作成し、起動時から保護されるようにし、両事業者のファイアウォールをREST APIから直接操作して、第三者のcollectionへの依存を避けた。

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。

全FFI呼び出しを検証する構文解析器を作成

手書きの仮Cヘッダーで、削除済みの3関数を呼んでもコンパイル・リンクが通り実行時に落ちた問題を受け、実際の7,308行のCヘッダーを読み、全呼び出し箇所、列挙定数、ポインター所有クラスのfinal指定を検証する構文解析器を作成した。

未使用だったコアの半分の機能を実装

バックアップ転送、消えるメッセージ、編集・再送、確認済み招待、プロキシ、暗号化方針など、アプリケーションが未使用だったメッセージングコアの半分の機能に対応し、モックなしで実ライブラリに対して全テストを実行した。

利用者を責めないエラーメッセージに改訂

実際にはプロバイダーがアプリ専用パスワードを要求していたのに、サインイン拒否を利用者の入力誤りとするエラー表示を受け、文書化した文体基準に従ってメッセージを書き直し、プロバイダー名を明示するテストを加えた。

公開するすべての部品のライセンスを把握

毎回のビルドで644個のRust crateのライセンス互換性を監査し、1つのcrateのライセンスを書き換えた場合と、再生成せずコアの固定リビジョンを変えた場合に検査が働くことを実証した。

追跡せずに13アドレスを測定

Cookie、トラッカー、第三者サービスを使わず、Webサーバーのアクセスログのみから13アドレスを測定。書き込み時に接続元ネットワークをマスクし、21の日別集計と20の月別分析軸からなる永続アーカイブへまとめた。

読みやすいTor onionミラーを公開

engineerで始まる読みやすいTor onionアドレスでサイトのミラーを公開。鍵はホスト外で生成し、このリポジトリにもノートパソコンにも置かず、4つの入口のうち計測しない唯一の入口にした。

技術的な取り組みを絞り込む

代表的なデータセット、そこから答えを得たい問い、現在のボトルネックをお知らせください。品質、処理量、復旧の測り方を合意できます。

料金を見る お問い合わせ →

自社の状況に当てはめる

お使いのシステムで「セキュリティ」がどのように関わっているかをお聞かせください。適したサービスを選び、その業務範囲を定めるお手伝いをします。

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://engineer.company/ja/categories/security/