Engineer Software

Sicherheit

15 Leistungen

Die Teile Ihres Systems verbinden

Die unter „Sicherheit“ gesammelten Arbeiten zeigen einen Teil eines funktionierenden Systems. Wir können helfen, diesen Teil mit dem Rest Ihres Betriebs zu verbinden. Der Teil, den Nutzer nie sehen: wo die Daten liegen, welche Regeln gelten und wie andere Systeme darauf zugreifen dürfen.

Unsere Leistungen entdecken Kontakt aufnehmen →

Eine vergleichbare Herausforderung finden

Folgen Sie einem Beispiel, das Ihrer Situation ähnelt. Die Rückschau beschreibt die Entscheidungen hinter dem Ergebnis und geht über die bloße Technologiebezeichnung hinaus. 6 ETL/ELT-Pipelines entworfen und betrieben — 6 ETL-Pipelines über drei Datenbankengines hinweg

6 ETL/ELT-Pipelines entworfen und betrieben Kontakt aufnehmen →

GIS-Karte mit PostgreSQL 10-mal schneller

Die Performance einer geografischen Kartenanwendung durch einen gezielten Datenbankwechsel von MSSQL zu PostgreSQL einschließlich Datenumschaltung um das 10-Fache verbessert und dabei Verarbeitung und Datensicherheit optimiert.

Organisationswechsel für Nutzer entwickelt

Einen Wechsel des Organisationskontexts mit clientseitigem localStorage und serverseitiger Cookie-Spiegelung entworfen, sodass Nutzer im Namen verwalteter Organisationen handeln können, während das Prinzip minimaler Berechtigungen gilt.

E-Mail mit Failover und Zustellprotokoll gebaut

E-Mail als Plattformfunktion entwickelt — drei Anbieter mit Ausfallsicherung, Zustell-Webhooks, Versand- und Zustellprotokollen, Vorlagen und Kampagnen — hinter einer Startprüfung, die ohne eingerichteten Anbieter den Systemstart verhindert.

PostgreSQL-Datenschicht mit Funktionen entworfen

Eine PostgreSQL-Datenschicht nach dem Function-first-Prinzip entworfen — 1.275 gespeicherte Funktionen in 34 Schemata — sodass jeder Lese- und Schreibzugriff über eine gezielt berechtigbare Funktion statt über eine Tabelle erfolgt.

Anwendung mit Nonce-basierter CSP gehärtet

Die Anwendung mit Nonce-basierter CSP, HSTS, SameSite-Cookies, Datenbankrollen mit minimalen Berechtigungen und erneuten serverseitigen Zugangsprüfungen gehärtet.

Technische Grundlagen der Plattform festgelegt

Die grundlegenden Plattformentscheidungen in den Wochen nach der Eröffnung des Repositorys im November 2025 festgelegt — Schichtenarchitektur, datenbankzentrierter Datenzugriff und Warnungsfreiheit — die neun Monate später weiterhin gelten.

Die gesamte Kerninfrastruktur neu aufgebaut

Als eine der ersten Mitarbeiterinnen die gesamte Kerninfrastruktur und die unterstützenden Prozesse eines Green-Energy-SaaS-Start-ups von Grund auf entworfen und aufgebaut und damit die Grundlage für schnelles Wachstum gelegt.

Stripe- und In-App-Kaufberechtigungen entwickelt

Die Zahlungs- und Berechtigungsschicht aufgebaut — Stripe sowie In-App-Käufe von Apple und Google — und Verzeichnis, Suche und Export durch ein serverseitig geprüftes Zugriffsmodell mit 11 Tabellen abgesichert.

Eigene Fehlerüberwachung und Tracing entwickelt

Eigene Fehlerüberwachung und OpenTelemetry-Tracing entwickelt statt eingekauft — Bereinigung von Nutzdaten, Erkennung von Fehlerspitzen und Regressionen, Symbolauflösung und synthetisches Lebenszeichen — mit 11 Betriebsansichten.

Bei Fehlern sperrenden Missbrauchsschutz gebaut

Bei Fehlern sperrende Missbrauchsschutzmechanismen aufgebaut — 22 Redis-gestützte Ratenbegrenzer, Cloudflare Turnstile, Anfrage-Idempotenz und eine Ursprungssperre — damit die Plattform Bots und Überlastungsangriffe abweist, statt ihren Aufrufern zu vertrauen.

Unternehmensbesitzansprüche und Prüfung umgesetzt

Die Bearbeitung von Unternehmensbesitzansprüchen durchgängig umgesetzt: Ein Nutzer beansprucht ein Unternehmen, ein Administrator entscheidet und eine Genehmigung verändert den Berechtigungsgraphen, der die Bearbeitungsrechte festlegt.

Parser zur Prüfung aller FFI-Aufrufe geschrieben

Einen Parser geschrieben, der den echten C-Header mit 7.308 Zeilen liest und jede Aufrufstelle, jede Enum-Konstante sowie final für jede pointerbesitzende Klasse prüft, nachdem ein handgeschriebener Platzhalterheader Aufrufe dreier entfernter Funktionen kompilieren und linken ließ, die zur Laufzeit abstürzten.

Die ungenutzte Hälfte des Kerns erschlossen

Die zuvor ungenutzte Hälfte des Messaging-Kerns erschlossen — Sicherungsübertragung, verschwindende Nachrichten, Nachrichtenbearbeitung und erneutes Senden, verifizierte Einladungen, Proxys und Verschlüsselungsrichtlinien — und jeden Test ohne Mocks gegen die echte Bibliothek ausgeführt.

Fehlermeldungen ohne Schuldzuweisung verfasst

Die Fehlermeldungen der Anwendung anhand eines schriftlichen Tonalitätsstandards neu verfasst, nachdem eine abgewiesene Anmeldung dem Nutzer einen Tippfehler vorwarf, obwohl der Anbieter ein anwendungsspezifisches Passwort verlangte; den Fall mit einem anbieterspezifischen Test abgesichert.

Lesbaren Tor-Onion-Spiegel veröffentlicht

Die Website als Tor-Onion-Spiegel unter einer lesbaren, mit engineer beginnenden Adresse veröffentlicht, den Schlüssel außerhalb des Hosts erzeugt, sodass er weder dieses Repository noch einen Laptop erreichte, und diesen einen von vier Zugängen von der Zählung ausgenommen.

Die technische Arbeit gezielt einsetzen

Beschreiben Sie den Arbeitsablauf, die vorhandenen Schnittstellen und die Nutzer, die die Veränderung benötigen. Wir können eine prüfbare Lieferung definieren und die Übergabe so gestalten, dass Ihr Team die gelieferten Bestandteile warten kann.

Preise ansehen Kontakt aufnehmen →

Das Thema in Ihren Kontext einordnen

Erzählen Sie uns, welche Rolle „Sicherheit“ in Ihrem eigenen System spielt. Wir können helfen, die passende Leistung auszuwählen und die damit verbundene Arbeit zu definieren.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://software.engineer.company/de/categories/security/