Engineer Plattform

{ Sicherheits- und Zugriffsverwaltung }

Festlegen, wer worauf zugreifen darf

Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Sie klären noch, was Sie benötigen?

Erzählen Sie uns, was nicht funktioniert oder was Sie entwickeln möchten. Wir sagen Ihnen, was dafür nötig wäre, was es ungefähr kosten würde und ob wir die Richtigen dafür sind.

Ab 1.400 DKK pro Stunde, zuzüglich Mehrwertsteuer — und weniger pro Stunde bei längerer Buchung.

Kontakt aufnehmen Preise ansehen

Ausgewählte Arbeiten, die diese Leistung zeigen.

Die Leistung in ein Ergebnis überführen

Machen Sie „Sicherheits- und Zugriffsverwaltung“ für ein Geschäftsergebnis nutzbar. Wir können die technische Arbeit mit den Nutzern, Betriebsabläufen und Entscheidungen verbinden, die sie unterstützen soll. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Kontakt aufnehmen

Die passenden Arbeiten prüfen

Prüfen Sie unser Vorgehen anhand der zugehörigen Arbeiten auf dieser Seite. Fragen Sie nach den Abwägungen und den Bedingungen hinter jedem Ergebnis. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

1.000 RBAC-Regeln für sichere Linux-Server

Die Datensicherheit durch 1.000 RBAC-Regeln für Entwickler, Anwendungsinstanzen, PostgreSQL, MS SQL und weitere Linux-Server erhöht, unberechtigte Zugriffe verhindert und die Regeln mit Ansible-Automatisierung dokumentiert.

Zugriffsverwaltung mit M365 und SSO geleitet

Durch die Leitung von Vorhaben zur Zugriffsverwaltung mit M365, 1Password, Red Hat SSO und OKTA SSO Sicherheitsverletzungen verhindert.

8 WireGuard-/IPsec-VPN-Verbindungen verwaltet

8 WireGuard-VPN- und IPsec-VPN-Verbindungen verwaltet und entstört und eine sichere Kommunikation zwischen Google-Cloud- und Linux-Systemen sichergestellt.

Teamkommunikation und Zusammenarbeit verbessert

Teamkommunikation und Zusammenarbeit durch die Einführung von Slack, Mattermost, 1Password und Jira verbessert und 8.000 Arbeitsstunden eingespart.

Netzwerkinfrastruktur administriert

Die Netzwerkinfrastruktur für über 1.000 Server administriert und eine geeignete Systembereitstellung, Sicherheit und Fehlerdiagnose sichergestellt.

SSL/TLS für 100 Docker-Apps automatisiert

Die Erstellung von SSL/TLS-Zertifikaten für 100 Docker-Anwendungen automatisiert und sichere Verbindungen auf Ubuntu-Linux-Hosts sichergestellt.

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.

Azure-Infrastruktur als Code provisioniert

Azure-Infrastruktur mit Bicep als Code provisioniert — Container Apps, PostgreSQL Flexible Server, Front Door/WAF und Netzwerke — für Entwicklungs-, Staging- und Produktivumgebung.

Anwendung mit Nonce-basierter CSP gehärtet

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

Teamzusammenarbeit automatisiert

Teamzusammenarbeit, Passwortverwaltung sowie Aufgaben- und Zeitmanagement automatisiert und ein halbautomatisches System zur Projektpräsentation entwickelt, um die Teamproduktivität zu steigern.

Unternehmensweiten Passwortmanager integriert

Ein unternehmensweites Passwortverwaltungssystem integriert, die Sicherheit erhöht und die Zugriffskontrolle vereinfacht.

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.

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.

Kontinuierliche Sicherheitsprüfungen etabliert

Ein kontinuierliches Sicherheitsprogramm aufgebaut — Codeanalyse, DAST, Abhängigkeits- und Schwachstellenprüfungen, SBOM-Erzeugung, Geheimnissuche und per SHA festgelegte Actions — ergänzt durch 21 schriftliche Sicherheitsaudits.

Drei Türschlösser, keines davon abgeschlossen

Drei nie funktionierende SSH-Brute-Force-Schutzmechanismen gefunden und korrigiert: eine Sperr-Jail für Port 22 bei einem auf 1986 lauschenden Daemon, eine durch eine allgemeinere vorherige Regel verdeckte Ratenbegrenzung und eine Sperraktion, deren Programm nie gefunden wurde, sodass nie eine Sperre griff.

SSH mit 24 geprüften Direktiven gehärtet

SSH auf 24 geprüfte Direktiven gehärtet und dreistufig validiert — Kandidatendatei, zusammengesetzte Konfiguration und anschließend die Rückmeldung des Daemons selbst — nachdem diese gezeigt hatte, dass der laufende Server zwei der vierundzwanzig Direktiven stillschweigend überschrieb.

Angriffssperren bei jedem Lauf nachgewiesen

Den Pfad zur Angriffssperre bei jedem Härtungslauf durchgängig nachgewiesen: eine reservierte Testadresse gesperrt, die entstandene Kernelregel ausgelesen und die Sperre in einem garantierten Aufräumblock aufgehoben, sodass eine ausgefallene Jail den Lauf scheitern lässt, statt einen gesunden Zustand zu melden.

Firewallregeln nach Position geprüft

Firewallregeln nach ihrer Position statt bloß ihrer Existenz geprüft, anhand der nummerierten Regelliste und der aktiven Paketfilterkette, denn eine vorhandene Regel wird nicht zwingend von einem Paket erreicht.

Sekunden-Preflight für Geheimnisse ergänzt

Ein Preflight-Play ergänzt, das denselben Code wie der Konvergenzlauf mit den lokal beim Betreiber liegenden Geheimnissen in etwa einer Sekunde ausführt, nachdem ein teilweise durchgelaufener Produktivlauf bei Aufgabe neun abbrach, während die Swap-Einstellungen bereits auf dem Produktivhost geschrieben waren.

DNS-Zone mit 20 Einträgen als Code abgeglichen

Eine DNS-Zone mit 20 Einträgen deklarativ über die Cloudflare-API abgeglichen, mit separaten Einstiegspunkten für Audit und BIND-Export, und den zuvor eingerichteten CDN-Proxy aus Datenschutzgründen wieder abgeschaltet.

Alle systemd-Units stärker isoliert

Die Angriffsfläche der systemd-Sandboxen für jede von der Plattform installierte Unit verringert — einen Totmannschaltungsdienst von 9,6 UNSAFE auf 1,5, eine internetseitig erreichbare Git-Forge von 8,3 EXPOSED auf 1,5 — und eine Parserprüfung beim Konvergenzlauf ergänzt, nachdem eine falsch geschriebene Direktive in drei Unit-Vorlagen stillschweigend ignoriert worden war.

Container mit Podman und Quadlet betrieben

Eine Containerebene mit Podman und Quadlet unter systemd statt Docker bereitgestellt, da Dockers standardmäßige Portfreigaben im Bridge-Netz UFW-Regeln umgehen können; für Bereitstellungen einen unprivilegierten Nutzer mit einem festen Befehl statt root eingerichtet.

Einen zweiten Server aus Code provisioniert

Die Provisionierung eines zweiten Servers bei einem zweiten Cloud-Anbieter automatisiert und die Firewall vor dem Rechner angelegt, damit er von Anfang an geschützt ist; die Firewalls beider Anbieter direkt über deren REST-APIs gesteuert, um eine Drittanbieter-Collection zu vermeiden.

Zuständigkeit nach Geheimnisleck klar geregelt

Eine Regel zum Zuständigkeitsumfang im Repository festgeschrieben, nachdem eine Umstrukturierung Inventar, Firewallfreigaben und Texte eines anderen Unternehmens hineingetragen hatte; die isolierten Rückstände weiterhin auf Geheimnisse prüfen lassen, statt sie auszuschließen.

Jedes Betriebsgeheimnis je Host getrennt

Die vier betrieblichen Geheimnisse je Host getrennt, nachdem sich gezeigt hatte, dass zwei Hosts mit einer gemeinsamen Totmannschaltung weniger zuverlässig alarmieren als zwei getrennte Schaltungen und eine gemeinsame Sicherungspassphrase die Sicherungen beider Hosts auch in getrennten Repositorys offenlegen kann, wenn jemand die Passphrase erlangt und die verschlüsselten Daten und Schlüsseldateien beider Repositorys lesen kann.

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.

Die Lizenz aller ausgelieferten Komponenten kennen

644 Rust-Crates bei jedem Build auf Lizenzverträglichkeit geprüft und die Wirksamkeit durch das Ändern einer Crate-Lizenz sowie das Verschieben der festgelegten Kernrevision ohne Neuerzeugung nachgewiesen.

13 Adressen ohne Tracking gemessen

Dreizehn Adressen ausschließlich anhand des eigenen Webserver-Zugriffsprotokolls gemessen — ohne Cookie, Tracker oder Drittanbieterdienst — das Clientnetz beim Schreiben jeder Zeile maskiert und das Ergebnis dauerhaft mit 21 täglichen Zählwerten und 20 monatlichen Facetten archiviert.

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.

Sie suchen Sicherheits- und Zugriffsverwaltung?

Beurteilen Sie anhand der verlinkten Arbeiten die einschlägige Erfahrung. Erzählen Sie uns, was Sie entwickeln möchten; wir können Umfang, Vorgehen bei der Umsetzung und Übergabe besprechen.

Kontakt aufnehmen Gesamtes Portfolio

Den Umfang vor der Beauftragung festlegen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Ihre Anforderungen besprechen

Erzählen Sie uns, was Sie von „Sicherheits- und Zugriffsverwaltung“ benötigen, einschließlich des Termins und des Teams, das die Wartung übernehmen wird. Wir können einen praktikablen Weg besprechen.

Kontakt aufnehmen

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://platform.engineer.company/de/services/security-access/