Wir betreiben die Plattformen, **auf denen Ihre Software ausgeliefert wird** — aus Code wiederaufgebaut, überwacht und dokumentiert.

Cloud, Infrastructure as Code, CI/CD, Container, Monitoring, Sicherungen, Netzwerke und Zugriff — aus Kopenhagen.

---

company
Engineer
Plattform

Infrastruktur, die Sie aus einem Repository neu aufbauen können

+45 50 10 61 84 · Kopenhagen, Dänemark

Mit Sorgfalt und Liebe gestaltet von D.

Cloud-Infrastruktur als Code, automatisierte Bereitstellung und Wiederherstellungsplanung für die Systeme, auf die Ihr Unternehmen angewiesen ist. Die Arbeitsnachweise beschreiben die Ausgangslage, die ausgeführten Arbeiten und das Ergebnis.

Beginnen Sie mit einem Bereitstellungsweg oder einem Betriebsrisiko. Wir können eine Prüfung oder Umsetzung mit einem dokumentierten Plan für Einführung, Rollback und Verantwortlichkeiten vereinbaren, damit Ihr Team weiß, was es wie betreiben soll.

Infrastrukturarbeit · Preise und Zusammenarbeitsformen · Ihr Projekt besprechen

Das benötigte Ergebnis zuerst

Sagen Sie uns, was Ihr Unternehmen erreichen muss. Wir verbinden Software, Daten und Infrastruktur mit Blick auf die Menschen, die sie nutzen.

Unsere Leistungen entdecken Kontakt aufnehmen →

So gehen wir an die Arbeit heran

Finden Sie die Leistung, die zu Ihrem Ziel passt, und sehen Sie anhand von Beispielen, was umgesetzt wurde und wie.

Fallstudien Kontakt aufnehmen →

Entdecken Sie die Arbeiten **in ihrem Kontext** — die Entscheidungen, die Umsetzung und die dokumentierten Ergebnisse.

Gesamten Katalog ansehen

Ein Partner für **10 Leistungen** vom ersten Server bis zum Alarm um 3 Uhr morgens.

Im Katalog stöbern

{ Cloud, Infrastruktur und DevOps }

Wo die Software läuft

Cloud-Infrastruktur und Cloud-Migration

Server werden nach dem tatsächlichen Bedarf dimensioniert und in die Cloud oder aus ihr heraus verlagert — die monatlichen Kosten stehen vorher fest.

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.

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.

Öffentliche Dienste auf einem kleinen Server

Die öffentlichen Unternehmensdienste auf einem Single-Core-Host mit 512 MB gehostet — Git-Forge, Webserver für sieben Domains, Tor, zwei Server für alternative Protokolle und Angriffssperren — mit 464 MB nutzbarem Arbeitsspeicher als Entwurfsgrenze; Sicherungsautomatisierung ist eine getrennte Implementierung.

Alle 9 Leistungen ansehen

Wie wir arbeiten

Zuerst verstehen

Wir verstehen das Problem, bevor wir eine Lösung vorschlagen. Ihr Briefing ist der Anfang dieses Gesprächs, nicht sein Ende.

Auf Dauer auslegen

Beständigkeit geht vor Schnelligkeit, Klarheit vor Raffinesse. Das System muss auch für die Menschen handhabbar bleiben, die es übernehmen.

Dahinterstehen

Laufenden Betrieb oder Support vereinbaren wir im Rahmen des Auftrags. Bei der Übergabe werden Zuständigkeiten und der nächste Kontaktweg geklärt.

{ Cloud, Infrastruktur und DevOps }

Server, die Sie aus versionierter Konfiguration neu aufbauen können

Infrastructure as Code

Die gesamte Einrichtung wird in Dateien festgehalten, damit sie sich exakt wiederherstellen lässt und nicht nur im Kopf einer einzelnen Person existiert.

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.

Forge-CI-Hook geprobt und 2 Fehler gefunden

Den CI-Hook auf der Forge probeweise ausgeführt und zwei beim bloßen Lesen unerreichbare Fehler gefunden: einen Fallback mit einem nicht auflösbaren Eingabeargument und eine Git-Umgebungsvariable, die der Qualitätsprüfung in den Checkout folgte und 19 Tests scheitern ließ.

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.

Alle 17 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Änderungen ohne Aufregung ausliefern

DevOps- und CI/CD-Automatisierung

Geprüft, veröffentlicht und rückgängig zu machen: Änderungen erreichen Ihre Kunden am Dienstagnachmittag statt spät am Freitagabend.

4 Repositorys auf einen Historienstandard geeint

Vier Repositorys auf einen einheitlichen Historienstandard verpflichtet — Conventional Commits, ohne Emojis und Attribution-Trailer, durch einen Commit-Message-Hook erzwungen — ergänzt durch 48 Anweisungsdokumente zur Arbeitsweise.

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.

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.

Alle 43 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Software, die überall gleich läuft

Containerisierung und Orchestrierung

So verpackt, dass sie auf dem Laptop, dem Testserver und im Produktivbetrieb gleich funktioniert und bei höherer Auslastung mitwächst.

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.

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.

GitHub-Actions-CI/CD-Pipelines aufgebaut

GitHub-Actions-CI/CD-Pipelines mit einem Distroless-Frontend-Image für den Produktivbetrieb und der Übernahme von Releases über mehrere Umgebungen entwickelt.

Alle 5 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Bescheid wissen, bevor Ihre Kunden es tun

Site Reliability und Monitoring

Monitoring und Alarme melden sich, solange ein Fehler noch klein ist; Kennzahlen zeigen, wie oft das gelingt.

Sechs Sammler weisen übersprungene Eingaben aus

Sechs Berichtssammler um Angaben zu ungelesenen Eingaben ergänzt — ungeöffnete Dateien, nicht installierte Sonden, unbekannte Journalzeilen — und Schwellenwerte anhand von 116 gemessenen Stichproben bestimmt, nachdem eine blinde Erfassung und ein gesunder Host dieselbe Seite ergeben hatten.

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.

Eine begrenzte Ereignispipeline für eine macOS-App

Ereignispuffer und Protokollierung nach einem dokumentierten macOS-Vorfall mit 41 MB Wachstum pro Sekunde und 111 GB komprimierten Speicherseiten auf einem Rechner mit 36 GB begrenzt; ein dokumentierter vollständiger Testlauf reduzierte Kernprotokollzeilen von 610.996 auf 1.411.

Alle 23 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Nach einem schlechten Tag alles zurückbekommen

Datensicherung und Notfallwiederherstellung

Sicherungen, deren Funktion geprüft und nicht vorausgesetzt wird, und ein schriftlicher Plan für den Morgen, an dem ein Server nicht wieder startet.

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.

Sicherungsautomatisierung mit klarem Wiederherstellungsweg

restic-Sicherungsautomatisierung mit Aufbewahrung, Integritätsprüfungen und monatlichem Wiederherstellungstest umgesetzt; Speicheraktivierung und Nachweis einer tatsächlichen Wiederherstellung als getrennte Betriebsschritte dokumentiert.

Sicherungen und Notfallwiederherstellung als Code

Die Aufbewahrung von Datenbanksicherungen als Infrastructure as Code konfiguriert, anschließend die Wiederherstellbarkeit geprüft und das Wiederherstellungsverfahren dokumentiert — mit ausdrücklich benannten Lücken, statt sie erst im Ernstfall entdecken zu lassen.

Alle 5 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Den Betrieb am Laufen halten

Systemadministration

Server, E-Mail, Konten und Updates werden im Alltag betreut, damit die Dinge, auf die alle angewiesen sind, unauffällig funktionieren.

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.

Sechs Sammler weisen übersprungene Eingaben aus

Sechs Berichtssammler um Angaben zu ungelesenen Eingaben ergänzt — ungeöffnete Dateien, nicht installierte Sonden, unbekannte Journalzeilen — und Schwellenwerte anhand von 116 gemessenen Stichproben bestimmt, nachdem eine blinde Erfassung und ein gesunder Host dieselbe Seite ergeben hatten.

Forge-CI-Hook geprobt und 2 Fehler gefunden

Den CI-Hook auf der Forge probeweise ausgeführt und zwei beim bloßen Lesen unerreichbare Fehler gefunden: einen Fallback mit einem nicht auflösbaren Eingabeargument und eine Git-Umgebungsvariable, die der Qualitätsprüfung in den Checkout folgte und 19 Tests scheitern ließ.

Alle 28 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Ihre Standorte und Mitarbeitenden verbinden

Netzwerke und VPN-Einrichtung

WLAN, Firewalls und Fernzugriff werden so eingerichtet, dass Mitarbeitende von überall arbeiten können und nur Berechtigte Zugang erhalten.

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.

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.

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.

Alle 11 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Festlegen, wer worauf zugreifen darf

Sicherheits- und Zugriffsverwaltung

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

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.

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.

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.

Alle 31 Leistungen ansehen

{ Cloud, Infrastruktur und DevOps }

Ihre KI darf nur tun, was sie soll

Sicherheit von KI-Agenten

Der Zugriff jedes Agenten wird erfasst und auf das Nötige begrenzt, jede Handlung außerhalb seiner Änderungsbefugnis protokolliert und jede Schutzmaßnahme geprüft statt bloß vorausgesetzt.

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.

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.

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.

Alle 9 Leistungen ansehen

Wir arbeiten mit **den Plattformen,** auf denen Ihr Unternehmen bereits aufbaut.

Apple Microsoft DigitalOcean AWS Google

Gesamten Technologie-Stack ansehen

Sicherheitsprüfung für die KI-Agenten im vereinbarten Umfang

Erfasst

Ein vereinbartes Verzeichnis der einbezogenen Agenten, Zugangsdaten und Datenzugriffe, zusammen mit Ihrer Konfiguration aufbewahrt.

Abgesichert

Jeder Agent mit eigener Identität und minimalen Rechten; gelesener Text wird als Daten behandelt, niemals als Anweisung.

Protokolliert

Jede Aktion wird mit der Person protokolliert, für die sie ausgeführt wurde, an einem Ort, den der Agent nicht verändern kann; bei Auffälligkeiten erfolgen Meldungen.

Absicherung von Agenten ansehen Zu Ihren Agenten anfragen →

Erzählen Sie uns, was Sie entwickeln.

Kein Formular, kein Verkaufstrichter, keine Vertriebssequenz — nur eine E-Mail an einen Menschen, der sie liest.

Das Gespräch beginnen

Diese Adresse zeigt nur die Infrastrukturarbeit. Das Unternehmen entwickelt auch Software, arbeitet mit Daten und berät Teams — diese Bereiche finden Sie auf engineer.company.
Das gesamte Angebot von Engineer ApS ansehen →

Mit einer gezielten Verbesserung beginnen

Ein Arbeitsablauf, ein Datenfluss oder ein System, das besser funktionieren soll, kann eine sinnvolle erste Aufgabe sein. Den Umfang können wir gemeinsam vereinbaren.

Preise ansehen Kontakt aufnehmen →

Das erste Gespräch vorbereiten

Nennen Sie uns das gewünschte Ergebnis, die vorhandenen Systeme und Ihren zeitlichen Rahmen. Damit können wir den nächsten Schritt besprechen.

Unsere Leistungen entdecken

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

Auf dem Server arbeiten wir mit **quelloffenem Linux** — ohne Lizenzkosten und ohne Verborgenes.

Ubuntu Debian

Wie wir Server betreiben

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/