Engineer Plataformas

Seguridad

40 logros

Conecte las partes de su sistema

Los trabajos reunidos en «Seguridad» muestran una parte de un sistema en funcionamiento. Podemos ayudar a conectar esa parte con el resto de su operación. Una persona responsable del sistema en el que se apoya toda la empresa: que funcione, tenga copias de seguridad y no se deteriore sin que nadie lo advierta.

Explore nuestros servicios Póngase en contacto →

Encuentre un reto comparable

Siga un ejemplo que se parezca a su situación. Su reseña describe las decisiones detrás del resultado, más allá de la etiqueta tecnológica. 10 servidores PostgreSQL y MS SQL en Ubuntu — 10 servidores de bases de datos desplegados y mantenidos

10 servidores PostgreSQL y MS SQL en Ubuntu Póngase en contacto →

10 servidores PostgreSQL y MS SQL en Ubuntu

Diseñé, desplegué y mantuve 10 servidores PostgreSQL y MS SQL en VPS con Ubuntu Linux, para mantener un rendimiento y una fiabilidad adecuados.

1.000 reglas RBAC para servidores Linux

Reforcé la seguridad de los datos mediante 1.000 reglas RBAC para desarrolladores, instancias de aplicaciones, PostgreSQL, MS SQL y otros servidores Linux, evitando accesos no autorizados y documentando la configuración mediante automatización con Ansible.

Administración de 30 VPS Ubuntu Linux

Administré 30 instancias VPS con Ubuntu Linux, implementé estrategias de recuperación ante desastres y mantuve configuraciones de red adecuadas.

Gestión de accesos con M365 y SSO

Prevení brechas de seguridad al dirigir iniciativas de gestión de accesos con M365, 1Password, Red Hat SSO y OKTA SSO.

Gestión de 8 conexiones VPN WireGuard e IPsec

Administré y resolví incidencias en 8 conexiones VPN de WireGuard e IPsec, manteniendo comunicaciones seguras entre Google Cloud y sistemas Linux.

Mejor comunicación y colaboración del equipo

Mejoré la comunicación y la colaboración del equipo mediante Slack, Mattermost, 1Password y Jira, ahorrando 8.000 horas de trabajo.

Administración de infraestructura de red

Administré la infraestructura de red de más de 1.000 servidores, atendiendo al despliegue, la seguridad y la resolución de incidencias de los sistemas.

SSL/TLS automático para 100 aplicaciones Docker

Automaticé la creación de certificados SSL/TLS para 100 aplicaciones Docker, manteniendo conexiones seguras entre servidores Ubuntu Linux.

Configuración y despliegue de 1.000 routers Wi-Fi

Configuré y desplegué 1.000 routers Wi-Fi, mejorando el acceso a la red y su rendimiento para los clientes.

Cambio de contexto entre organizaciones

Diseñé un sistema de cambio de contexto entre organizaciones con localStorage en el cliente y una copia en cookies del servidor, que permite actuar en nombre de las organizaciones administradas y aplica autorizaciones de mínimo privilegio.

Correo con conmutación y registro de entregas

Desarrollé el correo electrónico como capacidad de la plataforma — tres proveedores con conmutación por error, webhooks de entrega, registros de envío y entrega, plantillas y campañas — con una comprobación de arranque que impide iniciar el sistema sin un proveedor.

Infraestructura Azure como código

Aprovisioné infraestructura Azure como código con Bicep — Container Apps, PostgreSQL Flexible Server, Front Door/WAF y redes — en los entornos de desarrollo, preproducción y producción.

Flujos CI/CD en GitHub Actions

Desarrollé flujos CI/CD en GitHub Actions con una imagen de producción distroless para la interfaz y promoción entre varios entornos.

Despliegues completos de la plataforma en Azure

Asumí los despliegues completos de la plataforma en Azure y gestioné las versiones en desarrollo, preproducción y producción.

Aplicación reforzada con CSP basada en nonces

Reforcé la aplicación con CSP basada en nonces, HSTS, cookies SameSite, roles de base de datos de mínimo privilegio y nuevas comprobaciones de derechos de acceso en el servidor.

Infraestructura principal creada desde cero

Como una de las primeras incorporaciones, diseñé y construí desde cero toda la infraestructura principal y los procesos de soporte de una startup SaaS de energía verde, sentando las bases para un crecimiento rápido.

Colaboración del equipo automatizada

Automaticé la colaboración del equipo, la gestión de contraseñas, tareas y tiempo, y desarrollé un sistema semiautomático de presentación de proyectos que elevó la productividad del equipo.

Gestor de contraseñas para toda la empresa

Integré un sistema de gestión de contraseñas para toda la empresa, reforzando la seguridad y simplificando el control de accesos.

Stripe y acceso por compras en aplicaciones

Desarrollé la capa de pagos y derechos de acceso — Stripe junto con las compras dentro de las aplicaciones de Apple y Google —, regulando el acceso al directorio, la búsqueda y la exportación mediante un modelo de 11 tablas comprobado en el servidor.

Monitorización de errores y trazas propias

Desarrollé internamente la monitorización de errores y las trazas OpenTelemetry, en lugar de adquirirlas — saneamiento de cargas, detección de picos y regresiones, resolución de símbolos y una señal de actividad sintética —, con 11 vistas para operaciones.

Límites de tasa y protección contra abusos

Desarrollé controles contra abusos que deniegan el acceso ante fallos — 22 limitadores de tasa con Redis, Cloudflare Turnstile, idempotencia de solicitudes y bloqueo del origen — para rechazar bots y avalanchas de solicitudes sin confiar en quienes las envían.

Reclamaciones y decisiones de titularidad

Desarrollé el proceso completo de reclamación de titularidad de empresas: un usuario solicita una empresa, un administrador decide y la aprobación actualiza el grafo de autorizaciones que determina quién puede editar cada recurso.

Análisis continuo de seguridad

Establecí un programa continuo de seguridad — análisis de código, DAST, comprobación de dependencias y vulnerabilidades, generación de SBOM, detección de secretos y acciones fijadas por SHA —, junto con 21 auditorías de seguridad documentadas.

Tres cerraduras en la puerta, ninguna cerrada

Detecté y corregí tres protecciones contra fuerza bruta SSH que nunca habían funcionado: una jail de bloqueo que vigilaba el puerto 22 mientras el demonio escuchaba en el 1986, un límite de tasa oculto bajo una regla más amplia y una acción de bloqueo cuyo binario nunca se encontraba, por lo que no se había aplicado ningún bloqueo.

SSH reforzado con 24 directivas verificadas

Reforcé SSH con 24 directivas verificadas mediante validación en tres etapas — archivo candidato, configuración ensamblada y lectura de la configuración por el propio demonio —, después de que esta última detectara que el servidor en ejecución anulaba silenciosamente dos de las veinticuatro.

Bloqueo de intrusiones probado en cada ejecución

Verifiqué de extremo a extremo el bloqueo de intrusiones en cada ejecución de refuerzo, bloqueando una dirección reservada para pruebas, comprobando la regla resultante del núcleo y retirando el bloqueo en un bloque de limpieza garantizado, para que una jail averiada haga fallar la ejecución en vez de presentarse como operativa.

Reglas de cortafuegos verificadas por posición

Verifiqué las reglas del cortafuegos por su posición, además de por su existencia, leyendo la lista numerada de reglas y la cadena activa del filtro de paquetes, porque una regla presente puede no recibir nunca un paquete.

Automatización de copias con un método explícito de restauración

Implementé automatización de copias con restic, retención, comprobaciones de integridad y un flujo mensual de prueba de restauración; documenté la activación del almacenamiento y la verificación de restauración real como pasos operativos separados.

Comprobación de secretos en un segundo

Añadí una comprobación previa que ejecuta en aproximadamente un segundo el mismo código de convergencia sobre secretos locales del operador, después de que una ejecución de producción parcialmente aplicada fallara en su novena tarea con los ajustes de intercambio ya escritos en el servidor activo.

Zona DNS de 20 registros como código

Concilié declarativamente una zona DNS de 20 registros con la API de Cloudflare mediante puntos de entrada separados para auditoría y exportación BIND, y desactivé el proxy CDN por motivos de privacidad después de implementarlo.

Menor exposición en cada unidad systemd

Reduje la exposición de aislamiento systemd en todas las unidades que instala la plataforma — un servicio de monitorización por ausencia de señal pasó de 9,6 UNSAFE a 1,5 y una forja git expuesta a Internet de 8,3 EXPOSED a 1,5 — y añadí una comprobación del analizador durante la convergencia tras encontrar una directiva mal escrita que se ignoraba silenciosamente en tres plantillas de unidades.

Contenedores con Podman y Quadlet

Desplegué una plataforma de contenedores con Podman y Quadlet bajo systemd en lugar de Docker, porque la publicación predeterminada de puertos en redes bridge de Docker puede eludir las reglas UFW, y asigné a los despliegues un usuario sin privilegios con una única orden fija, en vez de root.

Segundo servidor aprovisionado desde código

Automaticé el aprovisionamiento de un segundo servidor en un segundo proveedor de nube y creé el cortafuegos antes que la máquina para que naciera protegida, con los cortafuegos de ambos proveedores configurados directamente mediante sus API REST para evitar una colección de terceros.

Regla de alcance tras una fuga de credenciales

Incorporé al repositorio una regla de alcance tras una reorganización que había introducido el inventario, los permisos de cortafuegos y textos de otra empresa, y mantuve los residuos en cuarentena bajo el detector de secretos, sin excluirlos.

Secretos operativos separados por servidor

Separé los cuatro secretos operativos de cada servidor tras constatar que dos servidores que comparten una señal de actividad alertan menos que dos señales independientes, y que una contraseña compartida de copias de seguridad puede exponer las copias de ambos servidores, incluso en repositorios separados, si alguien la obtiene y puede leer los datos cifrados y los archivos de claves de ambos repositorios.

Analizador que verifica cada llamada FFI

Escribí un analizador que lee la cabecera C real de 7.308 líneas y verifica cada punto de llamada, cada constante de enumeración y que toda clase propietaria de un puntero sea final, después de que una cabecera provisional escrita a mano permitiera compilar y enlazar llamadas a tres funciones eliminadas que causaban fallos al ejecutarse.

La mitad sin utilizar del núcleo, implementada

Implementé la mitad del núcleo de mensajería que la aplicación no utilizaba — transferencia de copias de seguridad, mensajes temporales, edición y reenvío de mensajes, invitaciones verificadas, proxies y política de cifrado —, ejecutando cada prueba contra la biblioteca real, sin simulaciones.

Conocer la licencia de todo lo que se publica

Audité la compatibilidad de licencias de 644 crates Rust en cada compilación y probé que el control se activa al cambiar la licencia de una crate y al modificar la revisión fijada del núcleo sin regenerar los datos.

13 direcciones medidas sin rastreo

Medí trece direcciones únicamente a partir del registro de accesos del servidor web — sin cookies, rastreadores ni servicios de terceros —, enmascarando la red del cliente al escribir cada línea e incorporando el resultado a un archivo permanente de 21 recuentos diarios y 20 facetas mensuales.

Espejo onion de Tor con una dirección legible

Publiqué el sitio como espejo onion de Tor en una dirección legible que comienza por engineer, con la clave generada fuera del servidor para que nunca llegara a este repositorio ni a un portátil, y lo mantuve como la única de las cuatro puertas de entrada que nunca se contabiliza.

Centre el esfuerzo de ingeniería

Traiga un conjunto de datos representativo, las preguntas que debe responder y el cuello de botella actual. Podemos acordar cómo medir la calidad, la capacidad de procesamiento y la recuperación.

Vea cuánto cuesta Póngase en contacto →

Sitúe el tema en su contexto

Cuéntenos cómo aparece «Seguridad» en su propio sistema. Podemos ayudarle a elegir el servicio relevante y definir el trabajo en torno a él.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

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

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://platform.engineer.company/es/categories/security/