Engineer Asesoramiento

Cómo trabajamos de forma segura

Cómo construye y opera Engineer ApS de forma segura: nuestras prácticas, las medidas de protección de este sitio y dónde comunicar una vulnerabilidad.

La seguridad no es un servicio que vendamos por separado. Es nuestra forma de trabajar: el modelo de amenazas forma parte del diseño, el refuerzo de la seguridad forma parte de la construcción y las pruebas forman parte del traspaso.

Diseñe los controles desde el principio

Integre el acceso, el despliegue y la recuperación en la ingeniería desde el principio.

Explore nuestros servicios Póngase en contacto →

Mire detrás de una afirmación de seguridad

Pida la configuración y las pruebas que respaldan una afirmación de seguridad, con su alcance explícito.

Casos prácticos Póngase en contacto →

Cómo construimos

- **Mínimo privilegio como norma.** Los servicios se ejecutan con sus propios usuarios sin privilegios y con el acceso más limitado que les permite funcionar. Los límites de acceso se diseñan para limitar el movimiento entre componentes si uno de ellos se ve comprometido.
- **Los secretos nunca llegan al repositorio.** Las credenciales residen en un almacén de secretos o en la capa de despliegue, nunca en el código fuente ni en un artefacto de compilación. El análisis automático se ejecuta en cada commit, y una detección impide el commit.
- **Infraestructura descrita como código.** Los servidores se construyen a partir de una descripción que puede leerse, revisarse y reconstruirse, de modo que la configuración de una máquina sea un documento bajo control de versiones, no un recuerdo en la cabeza de alguien.
- **Dependencias fijadas y auditadas.** Se documenta de qué está hecho un sistema, y la lista se contrasta con los avisos publicados, en lugar de confiar en ella porque funcionaba el mes pasado.

- **Cifrado en tránsito en todas partes.** Los certificados se emiten y renuevan automáticamente, y se supervisa la renovación, porque un fallo habitual de TLS es un certificado que nadie vigilaba.
- **Automatización de copias de seguridad con pruebas de restauración separadas.** Una copia de seguridad es una afirmación hasta que alguien restaura a partir de ella. Implementamos flujos de trabajo separados para las copias de seguridad y las pruebas de restauración; la verificación se basa en los datos realmente restaurados y comprobados.

Cada línea anterior forma parte de **un día de trabajo corriente** — no de una fase que se añade al final.

Acuerde los límites de seguridad, las responsabilidades y las comprobaciones como parte del diseño.

Cómo está construido este sitio

Aplicamos el mismo nivel de exigencia a nuestro propio sitio, y puede verificar cada punto desde su navegador.

- **Sin backend, base de datos ni acceso de administrador.** Cada página es un archivo estático generado antes de que se solicite. Esto evita las sesiones de aplicación y los puntos de acceso para consultas a bases de datos, lo que reduce la superficie de ataque del sitio a nivel de aplicación.
- **Nada de JavaScript ejecutable.** Las páginas, los menús y los enlaces utilizan HTML y CSS nativos; los datos estructurados son JSON-LD inerte. No hay scripts de navegador que hagan solicitudes o guarden preferencias.
- **Una política de seguridad de contenidos estricta**, declarada en la propia página, con `form-action 'none'` : el sitio no envía formularios a ningún lugar.
- **Integridad de subrecursos en la hoja de estilos.** El paquete recibe una huella y un hash durante la generación, para que el navegador pueda verificar que ha llegado sin modificaciones.
- **Sin solicitudes a terceros.** Sin herramientas de analítica de terceros, servicios externos de fuentes ni widgets externos de mapas, y sin banner de consentimiento. Abra el panel de red del navegador y cuente los servidores: hay uno, y es el nuestro.
- **Sin cookies.** La página de cookies detalla todo lo que se almacena y lo que no.

- **Una política de comunicación de vulnerabilidades legible por máquinas** en `/.well-known/security.txt` , para que quien investigue y encuentre algo sepa dónde comunicarlo sin tener que preguntar.

Cómo se opera

Un pequeño servidor en Toronto, descrito como código, con el registro de acceso enmascarado al escribirse y conservado unos treinta días. La página de créditos identifica cada programa que utiliza; la página de privacidad explica exactamente qué registra al responder.

Comunicar una vulnerabilidad

Si ha encontrado una debilidad en este sitio o en cualquier sistema que operemos, escriba a welcome@engineer.company e indique qué ha encontrado y cómo reproducirlo. Confirmaremos su recepción, le diremos qué estamos haciendo al respecto y le atribuiremos el hallazgo si lo desea. No hay un programa de recompensas ni amenazas legales: solo una dirección que llega a una ingeniera.

¿Quiere aplicar el mismo rigor a sus propios sistemas? pídanos que los revisemos.

Esta página hace una afirmación **que puede auditar** — desde el navegador en el que la está leyendo.

Sin backend, sin cookies, cero JavaScript ejecutable y una política declarada en la propia página.

Pídanos que revisemos la suya Qué ofrecemos →

Identifique qué necesita protección

Empiece por los activos, los límites de confianza y los permisos del sistema que necesita proteger.

Vea cuánto cuesta Póngase en contacto →

Acuerde un encargo de seguridad de alcance concreto

Hablemos de una revisión o implementación de alcance concreto, con controles y comprobaciones de aceptación específicos.

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://advisory.engineer.company/es/security/