

¿Qué riesgo de cumplimiento genera el depósito en custodia de claves de cifrado (key escrow), y por qué Cyber Crucible no lo hace?

Respuesta breve: Almacenar claves de cifrado de forma centralizada crea un punto único de falla, un objetivo de alto valor y exposición a la divulgación obligatoria. El enfoque de prevención de Cyber Crucible no depende de capturar o depositar en custodia las claves, por lo que no existe un almacén central de claves que asegurar, que sea objeto de una citación judicial o que pueda vulnerarse.

“ Para la respuesta directa sobre el producto, consulte el artículo existente "**¿Cyber Crucible recopila claves de cifrado?**". Esta página aborda el razonamiento de cumplimiento y soberanía de datos detrás de esa respuesta.

Por qué esto es deliberado

Cyber Crucible originalmente desarrolló y patentó tecnología de captura de claves para la defensa contra ransomware. Para 2021, las variantes de ransomware habían evolucionado para derrotarla, utilizando bibliotecas de cifrado personalizadas, implementaciones únicas por ejecución y cifrados de flujo (streaming ciphers) inmunes a la captura de claves. Presentamos ese criptoanálisis públicamente en BSides Pittsburgh en 2021.

El riesgo que decidimos no crear

Además de haber dejado de funcionar, la captura de claves requiere el almacenamiento centralizado de claves de cifrado. Eso introduce un punto único de falla, un objetivo de alto valor y la posibilidad de divulgación obligatoria sin conocimiento del cliente.

Prevenir el ataque antes de que comience el cifrado elimina por completo la necesidad de claves, lo cual constituye tanto una defensa más sólida como una superficie de cumplimiento más reducida.

Revision #1

Created 2026-07-24 01:51:49 UTC by Dennis Underwood

Updated 2026-07-24 01:51:49 UTC by Dennis Underwood