Que risco de conformidade cria o depósito (escrow) de chaves de criptografia, e por que a Cyber Crucible não o faz?

Resposta curta: Armazenar chaves de criptografia de forma centralizada cria um ponto único de falha, um alvo de alto valor e exposição à divulgação forçada. A abordagem de prevenção da Cyber Crucible não depende da captura ou do depósito de chaves, portanto não há um repositório central de chaves para proteger, intimar judicialmente ou violar.

> Para a resposta direta sobre o produto, consulte o artigo existente **"A Cyber Crucible coleta chaves de criptografia?"** Esta página aborda o raciocínio de conformidade e soberania de dados por trás dessa resposta.

Por que isso é deliberado

A Cyber Crucible originalmente desenvolveu e patenteou uma tecnologia de captura de chaves para defesa contra ransomware. Em 2021, as variantes de ransomware haviam evoluído para derrotá-la — utilizando bibliotecas de criptografia personalizadas, implementações exclusivas por execução e cifras de fluxo imunes à captura de chaves. Apresentamos essa criptoanálise publicamente na BSides Pittsburgh em 2021.

O risco que optamos por não criar

Além de não funcionar mais, a captura de chaves exige o armazenamento centralizado de chaves de criptografia. Isso introduz um ponto único de falha, um alvo de alto valor e a possibilidade de divulgação forçada sem o conhecimento do cliente.

Prevenir o ataque antes que a criptografia comece elimina completamente a necessidade de chaves — o que representa tanto uma defesa mais forte quanto uma superfície de conformidade menor.

Revision #1
Created 2026-07-24 05:50:13 UTC by Dennis Underwood

Updated 2026-07-24 05:50:13 UTC by Dennis Underwood