Quel risque de conformité l'entiercement des clés de chiffrement crée-t-il, et pourquoi Cyber Crucible ne le pratique-t-il pas ?

Réponse courte : Le stockage centralisé des clés de chiffrement crée un point de défaillance unique, une cible de grande valeur, et une exposition à une divulgation forcée. L'approche de prévention de Cyber Crucible ne dépend pas de la capture ou de l'entiercement des clés ; il n'existe donc aucun stockage central de clés à sécuriser, à soumettre à une assignation, ou à compromettre.

> Pour la réponse directe concernant le produit, consultez l'article existant « **Cyber Crucible collecte-t-il les clés de chiffrement ?** » Cette page couvre le raisonnement en matière de conformité et de souveraineté des données qui sous-tend cette réponse.

Pourquoi c'est délibéré

Cyber Crucible a initialement développé et breveté une technologie de capture de clés pour la défense contre les rançongiciels. Dès 2021, les souches de rançongiciels avaient évolué au point de la déjouer — en utilisant des bibliothèques de chiffrement personnalisées, des implémentations uniques à chaque exécution, et des chiffrements de flux immunisés contre la capture de clés. Nous avons présenté publiquement cette cryptanalyse lors de la conférence BSides Pittsburgh en 2021.

Le risque que nous avons choisi de ne pas créer

Au-delà du fait qu'elle ne fonctionne plus, la capture de clés nécessite un stockage centralisé des clés de chiffrement. Cela introduit un point de défaillance unique, une cible de grande valeur, et la possibilité d'une divulgation forcée à l'insu du client.

Empêcher l'attaque avant que le chiffrement ne commence élimine entièrement le besoin de clés — ce qui constitue à la fois une défense plus solide et une surface de conformité réduite.

Revision #1
Created 2026-07-24 07:00:57 UTC by Dennis Underwood
Updated 2026-07-24 07:00:57 UTC by Dennis Underwood