Que signifie la souveraineté des données pour les déploiements de Cyber Crucible ?

Réponse brève : Vos données restent là où vous les placez. L'analyse et l'application des mesures se font au niveau du point de terminaison (endpoint), et Cyber Crucible peut être déployé entièrement sur site — fonctionnant dans des baies de serveurs physiquement sécurisées plutôt que dans un cloud public, sans plateformes tierces, sans accès externe et sans partage de données.

Pourquoi la centralisation des données de sécurité constitue un risque

Les architectures de sécurité qui centralisent des éléments sensibles — clés de chiffrement, jetons de session, données d'identité — créent un point de défaillance unique et une cible de grande valeur, tant pour les attaquants criminels que pour les acteurs soutenus par des États.

Il existe un second risque, moins souvent évoqué : un gouvernement pourrait contraindre l'accès à des données détenues de manière centralisée par le biais d'une assignation classifiée ou d'une lettre de sécurité nationale, à l'insu du client et sans son consentement. Il s'agit là d'une exposition majeure en matière de souveraineté des données, sans aucune transparence.

L'option sur site

Pour les organisations exigeant un contrôle absolu, Cyber Crucible propose une installation entièrement sur site, incluant un déploiement en environnement isolé (air-gapped) ainsi qu'une architecture multi-tenant adaptée à la gestion de plusieurs départements ou agences à partir d'une seule instance sécurisée.

Revision #1
Created 2026-07-24 07:00:46 UTC by Dennis Underwood
Updated 2026-07-24 07:00:46 UTC by Dennis Underwood