¿Qué significa la soberanía de datos para las implementaciones de Cyber Crucible?

Respuesta breve: Sus datos permanecen donde usted los coloque. El análisis y la aplicación de medidas ocurren en el endpoint, y Cyber Crucible puede implementarse completamente en las instalaciones (on-premises), operando en racks de servidores físicamente protegidos en lugar de una nube pública, sin plataformas de terceros, sin acceso externo y sin compartir datos.

Por qué los datos de seguridad centralizados son un riesgo

Las arquitecturas de seguridad que centralizan material sensible —claves de cifrado, tokens de sesión, datos de identidad— crean un único punto de falla y un objetivo de alto valor tanto para atacantes criminales como para aquellos patrocinados por estados.

Existe un segundo riesgo que recibe menos atención: un gobierno podría exigir acceso a datos almacenados de forma centralizada mediante una citación clasificada o una carta de seguridad nacional, sin el conocimiento ni el consentimiento del cliente. Se trata de una exposición profunda en materia de soberanía de datos, sin transparencia alguna.

La opción on-premises

Para las organizaciones que requieren un control absoluto, Cyber Crucible ofrece una instalación completamente on-premises, incluida la implementación con espacio de aire (air-gapped) y una arquitectura multiinquilino (multi-tenant) adecuada para gestionar múltiples departamentos o agencias desde una única instancia segura.

Revision #1
Created 2026-07-24 01:51:40 UTC by Dennis Underwood
Updated 2026-07-24 01:51:40 UTC by Dennis Underwood