O que significa soberania de dados para as implantações da Cyber Crucible?

Resposta curta: Os seus dados permanecem onde forem colocados. A análise e a aplicação ocorrem no endpoint, e a Cyber Crucible pode ser implantada totalmente no local (on-premises) — funcionando em racks de servidores fisicamente seguros em vez de numa nuvem pública, sem plataformas de terceiros, sem acesso externo e sem partilha de dados.

Por que motivo os dados de segurança centralizados representam um risco

As arquiteturas de segurança que centralizam material sensível — chaves de encriptação, tokens de sessão, dados de identidade — criam um único ponto de falha e um alvo de elevado valor tanto para atacantes criminosos como para os patrocinados por estados.

Existe um segundo risco que recebe menos atenção: um governo pode obrigar ao acesso a dados detidos centralmente através de uma intimação classificada ou de uma carta de segurança nacional, sem o conhecimento ou consentimento do cliente. Trata-se de uma exposição profunda em termos de soberania de dados, sem qualquer transparência.

A opção no local (on-premises)

Para organizações que exigem controlo absoluto, a Cyber Crucible oferece uma instalação totalmente no local, incluindo implantação em ambiente isolado (air-gapped) e uma arquitetura multi-tenant adequada para gerir múltiplos departamentos ou agências a partir de uma única instância segura.

Revision #1
Created 2026-07-24 05:50:04 UTC by Dennis Underwood
Updated 2026-07-24 05:50:04 UTC by Dennis Underwood