Was bedeutet Datensouveränität für Cyber-Crucible-Implementierungen?

Kurze Antwort: Ihre Daten bleiben dort, wo Sie sie platzieren. Analyse und Durchsetzung erfolgen auf dem Endpunkt, und Cyber Crucible kann vollständig On-Premises bereitgestellt werden — in physisch gesicherten Serverracks statt in einer Public Cloud, ohne Plattformen von Drittanbietern, ohne externen Zugriff und ohne Datenweitergabe.

Warum zentralisierte Sicherheitsdaten ein Risiko darstellen

Sicherheitsarchitekturen, die sensible Materialien zentralisieren – Verschlüsselungsschlüssel, Sitzungstoken, Identitätsdaten – schaffen einen einzelnen Ausfallpunkt (Single Point of Failure) und ein hochwertiges Ziel sowohl für kriminelle als auch staatlich unterstützte Angreifer.

Es besteht ein zweites Risiko, dem weniger Aufmerksamkeit geschenkt wird: Eine Regierung könnte sich durch eine geheime Vorladung oder einen National-Security-Letter Zugang zu zentral gespeicherten Daten verschaffen, ohne Wissen oder Zustimmung des Kunden. Dies stellt eine erhebliche Gefährdung der Datensouveränität ohne jegliche Transparenz dar.

Die On-Premises-Option

Für Organisationen, die absolute Kontrolle benötigen, bietet Cyber Crucible eine vollständige On-Premises-Installation an, einschließlich Air-Gapped-Bereitstellung und einer Multi-Tenant-Architektur, die sich eignet, um mehrere Abteilungen oder Behörden von einer einzigen sicheren Instanz aus zu verwalten.

Revision #1
Created 2026-07-24 04:38:06 UTC by Dennis Underwood
Updated 2026-07-24 04:38:06 UTC by Dennis Underwood