¿Cómo respalda Cyber Crucible a los entornos gubernamentales y de alta seguridad?

Respuesta breve: Mediante la soberanía total de los datos — instalación completamente local (on-premises) en racks físicamente protegidos, operación en redes aisladas (air-gapped) y arquitectura multiinquilino — sin nube pública, sin SOC de terceros y sin intercambio de datos.

Soberanía por diseño arquitectónico

Para las organizaciones que requieren un control absoluto, no es necesario que nada salga del entorno. No existen plataformas de terceros en la ruta, ni acceso externo, ni análisis de sus datos alojado por el proveedor.

Esto es importante porque muchos proveedores suben datos de identidad sensibles — claves privadas, tokens de sesión — a sus equipos de SOC alojados. Ese almacenamiento centralizado es un único punto de fallo y un objetivo de alto valor para atacantes patrocinados por estados, y puede ser accedido mediante compulsión legal sin su conocimiento.

Silencioso por defecto

Las amenazas se neutralizan de forma silenciosa a nivel del kernel. Solo usted sabe que se intentó un ataque, y si no se accedió a ningún dato, normalmente no se generan alertas externas ni se requieren divulgaciones.

Multiinquilino

La arquitectura admite implementaciones multiinquilino, lo cual resulta adecuado para gestionar múltiples departamentos o agencias desde una única instancia local segura.

Revision #1
Created 2026-07-24 01:52:26 UTC by Dennis Underwood
Updated 2026-07-24 01:52:26 UTC by Dennis Underwood