¿Cómo se protegen los datos de Cyber Crucible en tránsito?

Respuesta breve: Todas las comunicaciones entre el agente y el servidor exigen TLS 1.3. Los payloads de datos operativos utilizan además JSON Web Encryption (JWE) con pares de claves criptográficas únicos por agente, de modo que los payloads no pueden interceptarse ni manipularse en tránsito. El acceso administrativo requiere autenticación basada en claves además de validación de tokens OAuth 2.0.

Las capas

- **Canales cifrados** — toda comunicación entre el agente y el servidor exige TLS 1.3.
- **Cifrado de payload por agente** — los payloads operativos utilizan JWE con pares de claves únicos por agente. Como cada agente tiene su propio par de claves, comprometer un circuito de tránsito no expone a los demás, y se impide la interceptación o manipulación en línea.
- **Administración autenticada** — el acceso al sistema requiere autenticación individual de usuario basada en claves y validación de tokens OAuth 2.0, restringiendo las acciones administrativas al personal autorizado.

Por qué son importantes las claves por agente

El cifrado de transporte por sí solo protege el canal. El cifrado de payload por agente protege el *contenido del mensaje* de forma independiente del canal, de modo que un atacante posicionado en línea, o un intermediario comprometido, aun así no puede leer ni alterar lo que envió el agente.

Infraestructura compartida

Cuando se utilizan entornos de nube pública o nube privada virtual para la administración del backend, Cyber Crucible aplica un estricto aislamiento lógico de inquilinos junto con cifrado de extremo a extremo de los payloads. Los proveedores de nube y los operadores de infraestructura tienen **visibilidad cero** sobre los payloads de datos operativos o los estados de los sistemas de los clientes.

Revision #1
Created 2026-07-24 01:55:23 UTC by Dennis Underwood
Updated 2026-07-24 01:55:23 UTC by Dennis Underwood