

Comment les données de Cyber Crucible sont-elles protégées en transit ?

Réponse courte : Toutes les communications agent-serveur imposent TLS 1.3. Les charges utiles de données opérationnelles utilisent en outre le chiffrement JSON Web Encryption (JWE) avec des paires de clés cryptographiques uniques par agent, de sorte que les charges utiles ne peuvent être interceptées ni manipulées en transit. L'accès administratif nécessite une authentification par clé ainsi qu'une validation de jeton OAuth 2.0.

Les couches

- **Canaux chiffrés** — toutes les communications agent-serveur imposent TLS 1.3.
- **Chiffrement des charges utiles par agent** — les charges utiles opérationnelles utilisent JWE avec des paires de clés uniques par agent. Comme chaque agent possède sa propre paire de clés, la compromission d'un circuit de transit n'expose pas les autres, et l'interception ou la manipulation en ligne est empêchée.
- **Administration authentifiée** — l'accès au système nécessite une authentification individuelle par clé ainsi qu'une validation de jeton OAuth 2.0, restreignant les actions administratives au personnel autorisé.

Pourquoi les clés par agent sont importantes

Le chiffrement du transport protège uniquement le canal. Le chiffrement des charges utiles par agent protège le *contenu du message* indépendamment du canal — ainsi, un attaquant positionné en ligne, ou un intermédiaire compromis, ne peut toujours pas lire ni altérer ce que l'agent a envoyé.

Infrastructure partagée

Lorsque des environnements de cloud public ou de cloud privé virtuel sont utilisés pour l'administration back-end, Cyber Crucible applique une isolation logique stricte des locataires ainsi qu'un chiffrement de bout en bout des charges utiles. Les fournisseurs de cloud et les opérateurs

d'infrastructure n'ont **aucune visibilité** sur les charges utiles de données opérationnelles ou les états des systèmes des clients.

Revision #1

Created 2026-07-24 07:04:40 UTC by Dennis Underwood

Updated 2026-07-24 07:04:40 UTC by Dennis Underwood