Quelles mesures de protection protègent les données personnelles traitées par Cyber Crucible ?

Réponse courte : Chiffrement en transit et au repos, pseudonymisation des identifiants lorsque cela est possible, contrôle d'accès basé sur les rôles, gestion des clés avec rotation, journalisation d'audit et analyses de vulnérabilités régulières — le tout appuyé par des clauses contractuelles dans les DPA clients et un programme interne de sécurité de l'information.

Technique

- Données personnelles chiffrées **en transit** (TLS 1.3) et **au repos**.
- Chiffrement JSON Web Encryption par agent des charges utiles opérationnelles, utilisant des paires de clés uniques.
- Identifiants sensibles pseudonymisés ou anonymisés dans la mesure du possible.
- Accès contrôlé via l'authentification et des autorisations basées sur les rôles.
- Politiques de gestion des clés cryptographiques garantissant que les clés sont stockées en toute sécurité et régulièrement renouvelées.
- Journalisation et audit des accès et des actions administratives afin de détecter toute activité non autorisée.
- Analyses de vulnérabilités et tests de sécurité réguliers.

Contractuel

Les contrats clients et les DPA incluent des clauses relatives à la sécurité des données, à la confidentialité et à la notification des violations. Les sous-traitants ne sont engagés que dans le cadre d'accords écrits imposant des protections équivalentes. Les employés et prestataires sont liés par des accords de non-divulgation mutuels.

Organisationnel

Un programme de gestion de la sécurité de l'information régit la conformité continue, avec une formation de sensibilisation à la sécurité pour le personnel concerné, une réponse aux incidents documentée, des procédures de conservation et de suppression des données, ainsi que des audits internes périodiques.

À propos des certifications — en toute transparence

Le programme de sécurité de Cyber Crucible est **aligné avec** des référentiels reconnus de l'industrie. **Cyber Crucible ne détient actuellement aucune certification ISO 27001 ou SOC 2, et aucune certification n'est prévue à ce jour.**

L'alignement signifie que les contrôles suivent les pratiques décrites par ces référentiels. Cela ne signifie pas qu'un auditeur externe les a évalués et certifiés, et cela ne doit pas être présenté ainsi dans votre propre documentation de conformité. Si votre processus d'achat exige des preuves certifiées, cette exigence n'est pas satisfaite à ce jour — contactez **dpo@cybercrucible.com** pour discuter de la documentation disponible.

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