Comment Cyber Crucible aide-t-il à répondre aux exigences du RGPD??

Réponse courte : Cyber Crucible vous accompagne dans le respect de vos obligations au titre du RGPD par sa conception même, plutôt que par des politiques. Le contenu, les identifiants, les clés de chiffrement et les jetons de session ne sont jamais collectés ; l'analyse s'effectue sur le poste (endpoint) ; Cyber Crucible agit en tant que sous-traitant dans le cadre d'un DPA écrit ; et les options de déploiement conservent les données personnelles au sein de l'UE — ou au sein de votre propre bâtiment.

Correspondance avec les principes du RGPD

- **Minimisation des données (Art. 5)** — la liste des données exclues est énumérée, et non décrite en termes généraux. La télémétrie se limite à ce qui est nécessaire à la détection des menaces et est configurable.
- **Intégrité et confidentialité (Art. 5, 32)** — TLS 1.3 en transit, chiffrement des charges utiles JWE par agent, chiffrement au repos, contrôle d'accès basé sur les rôles, rotation des clés, journalisation d'audit.
- **Obligations du sous-traitant (Art. 28)** — DPA écrit précisant le périmètre ; traitement uniquement sur instructions documentées ; sous-traitants liés par des conditions équivalentes.
- **Transferts (Chapitre V)** — déploiement régional dans l'UE, ou déploiement isolé du réseau (air-gapped) qui élimine tout transfert.
- **Protection des données dès la conception (Art. 25)** — l'affirmation la plus forte possible : les catégories à plus haut risque ne sont pas protégées par une politique, elles ne sont tout simplement jamais collectées.

Pseudonymisation

Lorsque la télémétrie comportementale pourrait indirectement identifier une personne, les identifiants sont pseudonymisés ou masqués — une mesure de protection expressément reconnue par le RGPD.

Ce que cela ne fait pas

Cela ne rend pas votre organisation conforme au RGPD. Vos obligations dépendent de vos propres finalités de traitement, bases légales, mentions d'information et registres. Ce que cela supprime, c'est une difficulté courante : un fournisseur de sécurité exportant en continu des données personnelles vers un pays tiers.

Revision #2
Created 2026-07-24 07:11:30 UTC by Dennis Underwood
Updated 2026-11-24 04:29:06 UTC by Dennis Underwood