Quelles données Cyber Crucible collecte-t-il — et lesquelles ne collecte-t-il jamais ?

Réponse courte : Cyber Crucible fonctionne selon une directive de Zero-Content Harvesting (absence de collecte de contenu). Il traite la télémétrie opérationnelle du système — chemins d'exécution des processus, chaînes de processus parent-enfant, indicateurs d'exécution matériels et états d'intégrité de la mémoire — analysés localement sur le poste. Il ne collecte, ne transmet, ne stocke ni ne traite les clés de chiffrement, les identifiants, les jetons de session ou vos fichiers.

Catégories strictement exclues

Le logiciel Cyber Crucible ne collecte, ne transmet, ne stocke ni ne traite :

- **Les variables cryptographiques** — clés privées, clés de déchiffrement et clés de chiffrement applicatives.
- **Les identifiants utilisateur** — mots de passe utilisateur, secrets Active Directory et clés privées d'API.
- **Les identifiants de session** — jetons OAuth, jetons d'accès, jetons de rafraîchissement et cookies de session.
- **Les données de contenu client** — fichiers propriétaires, documents, contenus de bases de données, corps d'e-mails et communications des utilisateurs.

Pourquoi une protection complète ne nécessite pas la collecte de contenu

La pleine capacité du logiciel de prévention des menaces est atteinte sans collecter ni exfiltrer le contenu privé des clients. Le moteur comportemental évalue *ce qu'un programme fait* — quels processus atteignent quoi, après avoir fait quoi auparavant — et rien de tout cela ne nécessite d'ouvrir le fichier ou de lire le secret.

C'est le même principe que celui qui sous-tend la protection des identités : l'accès est tracé et analysé sans que l'identifiant lui-même ne soit consulté.

Où l'analyse a lieu

Les chemins d'exécution des processus, la lignée des processus, les indicateurs d'exécution matériels et les états d'intégrité de la mémoire sont analysés **localement sur le poste**. Lorsque l'assistance cloud ou la gestion centralisée est activée, la télémétrie administrative sortante est strictement limitée aux indicateurs opérationnels nécessaires à la surveillance de l'état du système et aux rapports de sécurité.

Revision #1
Created 2026-07-24 07:04:03 UTC by Dennis Underwood
Updated 2026-07-24 07:04:03 UTC by Dennis Underwood