Quelle est la différence entre la télémétrie système et les données clients ?

Réponse courte : La télémétrie système décrit le comportement d'un logiciel — quel processus en a démarré un autre, à quoi ressemble la mémoire, si les schémas d'exécution sont anormaux. Les données clients sont le contenu que votre entreprise crée et détient — fichiers, e-mails, enregistrements de bases de données, identifiants. Cyber Crucible analyse le premier et ne collecte jamais le second.

Une façon utile d'y penser

La télémétrie est constituée de métadonnées sur le *comportement des machines*. Le contenu, lui, est *l'information elle-même*.

Savoir que le `processus A` a lancé le `processus B`, lequel a ensuite tenté de lire un magasin d'identifiants de navigateur tout en présentant des signes de modification en mémoire, suffit à identifier une attaque. Il n'est pas nécessaire de lire ce qui se trouvait dans ce magasin d'identifiants — et Cyber Crucible ne le fait pas.

Ce que cela signifie concrètement

- L'analyse comportementale est effectuée sur l'accès aux identités **sans traiter les informations d'identité elles-mêmes**.
- La télémétrie qui quitte effectivement le point de terminaison dans les déploiements assistés par le cloud se limite à des indicateurs opérationnels destinés à la surveillance de l'état de fonctionnement et au reporting de sécurité.
- Les métadonnées techniques et comportementales ne sont considérées comme des données personnelles que lorsqu'elles permettent d'identifier directement ou indirectement une personne — et dans ces cas, les identifiants sont pseudonymisés ou masqués.

Contrôle du client

Les sources de télémétrie sont configurables. Les organisations peuvent définir précisément quelles sources sont collectées, afin qu'aucune information superflue ne soit acquise. Les champs qui ne sont pas essentiels à la détection des menaces sont exclus ou supprimés.

Revision #1
Created 2026-07-24 07:04:12 UTC by Dennis Underwood
Updated 2026-07-24 07:04:12 UTC by Dennis Underwood