

Pourquoi les outils de sécurité de type « collecteur cloud » peinent-ils face aux attaques modernes ?

Réponse courte : un collecteur cloud est un agent léger installé sur le poste de travail qui effectue peu d'analyse locale et transmet à la place la télémétrie brute à une plateforme cloud pour traitement. Cet aller-retour ajoute un délai qu'une attaque automatisée ne vous accorde pas, et l'agent dépend précisément des composants du système d'exploitation que les attaquants compromettent désormais.

Pourquoi le secteur a conçu les choses ainsi

L'ingénierie au niveau du noyau est difficile et coûteuse. L'envoi de la télémétrie vers le cloud a permis aux éditeurs de développer des logiciels de sécurité pour poste de travail moins coûteux, de monétiser le stockage cloud et de commercialiser des capacités d'« IA cloud ». Ce modèle a été optimisé pour faciliter le développement, et non pour assurer la défense.

Les deux modes de défaillance

1. **Trop lent.** Les attaques automatisées de type « smash-and-grab » s'exécutent en quelques millisecondes. L'analyse cloud ne peut pas fournir de réponse à temps.
2. **Aveugle au moment critique.** Étant donné que ces agents dépendent des bibliothèques natives du système d'exploitation pour fonctionner et collecter des données, un attaquant qui compromet ces bibliothèques peut réduire l'agent au silence. Celui-ci continue de fonctionner mais ne signale plus rien — un tableau de bord indiquant que tout va bien pendant que les données s'échappent.

Cyber Crucible effectue le traitement localement, au niveau du noyau, et prend ses propres décisions, de sorte qu'il n'y a ni aller-retour vers le cloud, ni dépendance à un système d'exploitation potentiellement compromis.

Revision #1

Created 2026-07-24 06:55:41 UTC by Dennis Underwood

Updated 2026-07-24 06:55:41 UTC by Dennis Underwood