Cyber Crucible est-il un antivirus ?

Réponse courte : Non. Un antivirus identifie les fichiers connus comme malveillants à l'aide de signatures. Cyber Crucible n'utilise aucune signature — il évalue ce qu'un programme en cours d'exécution fait réellement et arrête les comportements malveillants, y compris les menaces que personne n'a encore jamais observées.

Pourquoi les signatures ne suffisent plus

Une signature ne peut décrire qu'une attaque déjà analysée par quelqu'un. Ce modèle échoue dans deux situations courantes :

- **Les attaques zero-day**, pour lesquelles aucune signature n'existe encore.
- **Les attaques sans fichier (fileless)**, où il n'y a aucun fichier auquel comparer une signature.

La détection basée sur les signatures nécessite également une mise à jour constante à partir de flux de renseignement sur les menaces, ce qui signifie que votre protection est toujours en retard sur l'attaquant.

Ce qui la remplace

Cyber Crucible modélise le comportement — l'activité mémoire, l'activité des processus et l'accès aux fichiers — et évalue l'intention en temps réel. C'est pourquoi il a arrêté des attaques zero-day sur les réseaux de clients jusqu'à 90 jours avant que tout autre éditeur ne les signale ou n'y réponde publiquement.

Revision #1
Created 2026-07-24 06:55:11 UTC by Dennis Underwood
Updated 2026-07-24 06:55:11 UTC by Dennis Underwood