Que signifie le fait que Cyber Crucible soit indépendant des bibliothèques Windows ?

Réponse courte : Cyber Crucible ne dépend pas des bibliothèques système Windows qu'il protège. Il en a été délibérément découplé, de sorte que lorsque des attaquants compromettent, font planter ou détournent ces bibliothèques, Cyber Crucible continue de fonctionner, continue d'appliquer les règles et continue de signaler.

Pourquoi cela a été conçu ainsi

Au cours du second semestre 2025, les attaquants se sont tournés vers l'infection des bibliothèques Windows essentielles en mémoire. Étant donné que presque tous les éditeurs de sécurité dépendent de ces mêmes bibliothèques pour fonctionner, cette seule manœuvre a rendu aveugle une grande partie du marché.

Cyber Crucible a consacré environ neuf mois à inventer de nouveaux capteurs, puis cinq mois supplémentaires d'ingénierie pour supprimer entièrement les dépendances aux bibliothèques Windows — y compris l'élimination des dépendances volatiles aux MiniFilters.

À quoi cela ressemble sur le plan architectural

L'architecture fait fonctionner sept sous-systèmes totalement indépendants au sein du noyau, incluant son propre système isolé de chiffrement, de réseau, d'analyse de métadonnées et de suivi des événements. Une phase supplémentaire de ces travaux remplace la bibliothèque réseau standard de Windows (`ws32_2.dll`) par une pile réseau personnalisée au niveau du noyau.

Éprouvé sur le terrain

Avec deux clients, des attaquants bloqués par le moteur de décision opérant uniquement au niveau du noyau ont ensuite tenté d'empêcher que le client soit notifié en attaquant la couche réseau du système d'exploitation. Étant donné que les communications réseau de Cyber Crucible sont indépendantes du système d'exploitation, la protection a tenu bon et les renseignements sont

tout de même parvenus au client.

Revision #1
Created 2026-07-24 06:58:20 UTC by Dennis Underwood
Updated 2026-07-24 06:58:20 UTC by Dennis Underwood