

Cyber Crucible intègre-t-il des bibliothèques tierces ou du code étranger ?

Réponse courte : Non. Les capteurs du noyau, les pilotes et les modèles comportementaux Genetic AI sont conçus en interne. Aucun SDK parrainé par un État étranger, aucune bibliothèque tierce non vérifiée, ni aucun mouchard de télémétrie caché n'est intégré au logiciel. Les pilotes du noyau Windows sont soumis à la certification dans le cadre du programme de compatibilité matérielle Windows de Microsoft (Windows Hardware Compatibility Program, WHCP).

L'avantage concurrentiel de l'ingénierie

Développer des capteurs du noyau et des modèles comportementaux en interne est coûteux et long. La plupart des fournisseurs assemblent des composants à la place. C'est précisément dans cet assemblage que le risque lié à la chaîne d'approvisionnement s'introduit dans un produit de sécurité — l'outil disposant des privilèges système les plus étendus est aussi celui où une dépendance non vérifiée peut causer le plus de dommages.

Les composants de Cyber Crucible sont propriétaires et maintenus en interne, ce qui élimine cette catégorie d'exposition plutôt que de simplement la gérer.

Validation externe

Tous les pilotes du noyau Windows font l'objet de tests internes d'assurance qualité et sont soumis à la certification dans le cadre du programme de compatibilité matérielle Windows de Microsoft (Windows Hardware Compatibility Program, WHCP) — une validation indépendante de la qualité et de la résistance à la falsification pour le code s'exécutant au niveau du noyau.

Aucune télémétrie cachée

Il n'existe aucun mouchard de télémétrie caché. Ce que le logiciel collecte est documenté, et les catégories qu'il ne collecte jamais sont explicitement énumérées.