Quelle validation de sécurité indépendante Cyber Crucible possède-t-elle ?

Réponse courte : Les pilotes du noyau Windows de Cyber Crucible sont testés de manière objective et signés cryptographiquement dans le cadre du programme de compatibilité matérielle Windows de Microsoft (WHCP). Il s'agit d'une attestation externe et indépendante de la qualité et de la résistance à la falsification du composant le plus privilégié du produit — le code où l'exactitude importe le plus.

Pourquoi le WHCP est significatif

La majeure partie du marché des solutions de sécurité des postes de travail a évité le développement au niveau du noyau, car il est véritablement difficile et coûteux. Cyber Crucible opère délibérément au niveau du noyau, et soumet ses pilotes au programme de Microsoft afin qu'une partie externe — et non uniquement Cyber Crucible — valide que le code le plus sensible est correct et résistant à la falsification.

- La validation est **strictement limitée au pilote**, et n'est pas présentée comme une certification de l'ensemble du produit.
- Il s'agit d'un test objectif et reproductible plutôt que d'un audit administratif subjectif.

Comment cela s'intègre dans une vision d'ensemble

Pour un évaluateur habitué à rechercher un rapport SOC 2, le WHCP constitue un élément de preuve concret et indépendant qu'un SOC 2 ne fournit pas : une validation directe du composant noyau. Il complète — plutôt qu'il ne remplace — les preuves de contrôle figurant dans le dossier fournisseur préparé par Cyber Crucible.

Revision #1
Created 2026-07-24 07:12:13 UTC by Dennis Underwood
Updated 2026-07-24 07:12:13 UTC by Dennis Underwood