Cyber Crucible ralentit-il mes systèmes ?

Réponse courte : Non. L'utilisation CPU typique est d'environ 1 % ou moins, et l'architecture évite délibérément la technique qui cause la plupart des ralentissements liés aux agents de sécurité des postes de travail — l'insertion de hooks dans les bibliothèques système de Windows.

Pourquoi les autres agents provoquent des ralentissements

Les outils de sécurité traditionnels insèrent des « hooks » dans des bibliothèques système hautement optimisées afin de surveiller les comportements malveillants. Ces bibliothèques n'ont jamais été conçues pour être modifiées à la volée. Lorsqu'un outil de sécurité et un attaquant les manipulent tous deux simultanément, le résultat est une dégradation significative du système.

Le schéma qui s'ensuit est prévisible : l'utilisateur attribue le ralentissement à l'outil de sécurité et le désinstalle. L'éditeur ne parvient pas à reproduire le problème en laboratoire, sans savoir qu'un adversaire disposant d'un accès root manipule le système. Les attaquants ont appris à exploiter cela délibérément — en dégradant les performances jusqu'à ce que les victimes désactivent elles-mêmes leurs défenses.

Une approche différente

Cyber Crucible fonctionne via des sous-systèmes indépendants au sein du noyau plutôt qu'en accrochant des composants Windows fragiles, de sorte qu'il n'entre pas en concurrence avec le système d'exploitation — ni avec un attaquant — pour les mêmes chemins de code fragiles.

Revision #1
Created 2026-07-24 06:55:49 UTC by Dennis Underwood
Updated 2026-07-24 06:55:49 UTC by Dennis Underwood