

Pourquoi Cyber Crucible répond-il en suspendant un processus plutôt qu'en arrêtant le système ?

Réponse courte : Suspendre uniquement le processus malveillant — parfois appelé un Selective Freeze — neutralise l'attaque tout en laissant le reste continuer à fonctionner. Il n'y a aucun verrouillage complet du système, aucun redémarrage, et aucune interruption du travail légitime.

Le problème des réponses de type verrouillage

Lorsque de nombreux outils de détection identifient une anomalie, les options de confinement sont brutales : isoler la machine ou la mettre hors ligne. Dans un hôpital, une usine ou une opération de trading, cette réponse peut être presque aussi dommageable que l'attaque elle-même.

Ce que la suspension sélective permet d'accomplir

L'attaque est suspendue en mémoire. Les transactions légitimes ne s'arrêtent jamais. Dans le déploiement de services financiers où près de 10 000 processus malveillants ont été interceptés, les transactions SQL légitimes se sont poursuivies sans interruption tout au long — les opérations n'ont jamais été arrêtées.

C'est ce qui rend la prévention compatible avec la continuité des activités plutôt qu'un compromis à son détriment.

Revision #1

Created 2026-07-24 06:58:36 UTC by Dennis Underwood

Updated 2026-07-24 06:58:36 UTC by Dennis Underwood