Cyber Crucible bloque-t-il toute injection de processus ?

Non !

Il existe une variété d'activités qui se produisent sur les systèmes et qui constituent de l'injection de processus, mais qui ne sont pas nécessairement malveillantes.

Cyber Crucible rend visibles toutes ces activités d'injection de processus à des fins de threat hunting et d'analyse des causes profondes, mais n'arrête pas l'activité à moins que les activités d'extorsion de données, à savoir le vol de données ou le chiffrement par ransomware, ne commencent.

Vous trouverez ci-dessous un exemple d'injection de processus effectuée par le logiciel de sécurité des terminaux PC Matic, appelé PCPitStop. Il s'agit probablement d'un comportement qu'ils adoptent pour inspecter les processus en cours d'exécution.

5373968.png?width=680
Grâce à l'analyse comportementale au niveau du noyau de Cyber Crucible, vous disposez d'une visibilité complète sur toutes les activités, quel que soit le niveau de permission du logiciel (y compris les logiciels Microsoft ou des éditeurs d'antivirus hautement privilégiés).

Si une réponse automatisée est effectuée, cette page ainsi que la page Process Creations peuvent être consultées pour fournir des résultats d'investigation rapides.

De plus, l'API REST peut être exploitée par les équipes de threat hunting pour rechercher des indicateurs de tactiques malveillantes potentielles en mémoire.

Revision #1
Created 2026-07-24 06:56:17 UTC by Dennis Underwood
Updated 2026-07-24 06:56:17 UTC by Dennis Underwood