

Cyber Crucible génère-t-il des faux positifs ? Quel est le taux de faux positifs ?

Cyber Crucible s'efforce d'offrir un environnement produit avec 0 faux positif. Cela dit, il arrive parfois qu'il y ait des faux positifs. Voyons d'où ils proviennent.

Actuellement, le taux de faux positifs est d'environ 1 réponse par mois, pour 1800 déploiements/agents, avec une traçabilité complète des raisons pour lesquelles ces réponses se produisent.

Programme corrompu effectuant des opérations rapides sur des fichiers

Que ce soit intentionnellement ou en raison d'une mauvaise programmation, il arrive parfois que des programmes se corrompent eux-mêmes, ou soient corrompus par d'autres programmes en cours d'exécution. Nous constatons cela fréquemment avec les nouvelles fonctionnalités de grandes suites logicielles, telles que Microsoft Office, ou des logiciels propriétaires développés sur mesure.

Ce qui se passe, c'est que la mémoire du programme est corrompue, ce qui augmente le niveau d'inspection du programme. Si cela est ensuite suivi d'un comportement d'accès aux fichiers s'apparentant à de l'extorsion, Cyber Crucible est contraint de suspendre le programme. Nous devenons de plus en plus efficaces pour identifier les bugs connus, et vous pouvez au moins continuer à exécuter votre programme jusqu'à ce qu'il plante (certains redémarrent automatiquement, d'autres non).

Dans un monde où les attaquants n'utilisent pas le système de fichiers, et détournent plutôt la mémoire des programmes en cours d'exécution, nous devons pécher par excès de prudence.

Cyber Crucible dispose désormais de la capacité de créer une permission, où, si le Programme A, avec les Arguments A, provoque une corruption dans le Programme B, avec les Arguments B - nous

pouvons créer une exclusion temporaire pour :

(Programme A + Arguments A) ouvre (Programme B + Arguments B)

De cette façon, aucun risque supplémentaire n'est présumé quant à l'implication d'un pirate informatique, à moins qu'il n'utilise justement exactement les mêmes arguments.

Un excellent exemple de cela s'est produit lorsque Microsoft a introduit pour la première fois l'ouverture de documents Office depuis leur logiciel de chat de bureau. Cela corrompait le programme Office... à chaque... fois... puis le programme Office se mettait à analyser tous les Documents de la machine environ 25 % du temps. Cela... nécessitait une exclusion.

Si vous rencontrez un plantage, utilisez le bouton d'assistance, et nous vous aiderons à créer une exclusion, jusqu'à ce que l'éditeur corrige le problème.

Programmes de sécurité

Cyber Crucible coexiste très bien avec les programmes de sécurité. Contrairement à ce que pensent la plupart des nouveaux clients, les outils de sécurité plus avancés ont tendance à utiliser des interactions système plus avancées que les programmes antivirus qui utilisent des technologies plus anciennes. En fait, certains outils de sécurité gratuits ou peu coûteux exécutent divers scripts Powershell non sécurisés comme élément clé de leur protection, plutôt que de véritables programmes.

En tant qu'outil de sécurité hautement résilient basé sur le noyau, Cyber Crucible est perçu comme étant plus « bas », ou plus « proche » du matériel que la plupart des autres outils. Cyber Crucible identifie automatiquement les autres outils de sécurité et les ajoute aux modèles comportementaux. Tant que les outils de sécurité ne présentent pas de signes de compromission, ils sont autorisés à fonctionner normalement.

Occasionnellement, un outil de sécurité peut provoquer une instabilité du système, lorsque ses tentatives de désactiver ou d'interférer avec le logiciel Cyber Crucible échouent. Dans ces cas, il est préférable de mettre Cyber Crucible sur liste blanche dans l'autre outil de sécurité, afin de l'empêcher d'essayer (et d'échouer) de désactiver ou d'interférer avec Cyber Crucible.

N'hésitez pas à ouvrir un ticket d'assistance auprès de Cyber Crucible, via le portail web, pour discuter de la question.

Outils administratifs ou de sauvegarde

Dans certaines circonstances, un comportement adapté doit être créé pour un outil administratif ou de sauvegarde, pendant que l'équipe Cyber Crucible développe un modèle comportemental amélioré. Dans ce cas, l'équipe Cyber Crucible aidera à la création d'une exception dans le modèle comportemental, qui isolera le programme ainsi que ses arguments pour une fenêtre d'opportunité extrêmement réduite en cas d'attaque potentielle.

Revision #1

Created 2026-07-24 07:02:40 UTC by Dennis Underwood

Updated 2026-07-24 07:02:41 UTC by Dennis Underwood