Que se passe-t-il si l’un de mes produits de sécurité entre en conflit avec Cyber Crucible ?

Cyber Crucible coexiste actuellement avec tous les principaux fournisseurs de sécurité, si l’on utilise les rapports Magic Quadrant de Gartner comme mesure des acteurs historiques du secteur.

Le logiciel de point de terminaison de Cyber Crucible est nettement plus résilient que les autres logiciels, y compris les autres outils de sécurité des postes de travail. De plus, les autres logiciels de sécurité n’ont généralement même pas une visibilité complète sur le logiciel de Cyber Crucible.

Un autre outil de sécurité tente de désactiver Cyber Crucible

Résumé :

L’autre outil tente de désactiver une partie de Cyber Crucible. Il n’y arrive pas. L’outil de l’autre fournisseur n’a jamais été testé pour le cas où un autre outil (à savoir Cyber Crucible) répond « non, je ne me désactive pas ». L’autre outil plante alors ou passe en état d’erreur.

Réponse de Cyber Crucible :

La réponse peut se faire en deux volets. Le premier consiste à mettre le logiciel Cyber Crucible sur liste blanche auprès de l’autre fournisseur. Cela amènera l’autre outil à ignorer le logiciel Cyber Crucible, ce qui (avec un peu de chance) empêchera l’autre outil de passer en état d’erreur.

Si cela ne fonctionne pas, il appartient à notre équipe de trouver une solution. Nous avons constaté que les autres fournisseurs sont beaucoup plus lents (plusieurs mois, voire jamais) à corriger un bug de leur côté.

Historiquement, dans les rares cas où cela s’est produit, nous avons essentiellement créé un environnement dans lequel l’autre outil pense avoir réussi. Une analogie non technique serait de

laisser un jeune membre de votre famille ou un enfant vous battre aux dames.

Un autre outil de sécurité tente d’exécuter du code en se faisant passer pour Cyber Crucible

Résumé :

Cela se produit très rarement, mais il y a eu des cas où un outil de sécurité tente d’injecter son code dans le programme en cours d’exécution de Cyber Crucible, et d’exécuter du code en se faisant passer pour nous.

Cela n’est pas différent d’un pirate se faisant passer pour un outil de sécurité, et il n’existe aucun moyen de distinguer si un pirate a pris le contrôle du programme de sécurité (ou de tout autre programme) « de confiance ».

Réponse de Cyber Crucible :

Il n’existe aucun scénario dans lequel Cyber Crucible permettrait à une autre entreprise (ou à un pirate) d’exécuter du code en se faisant passer pour notre produit. La seule solution à ce stade consisterait à mettre le logiciel Cyber Crucible sur liste blanche auprès de l’outil de l’autre fournisseur. Cyber Crucible ne peut fournir aucune mesure d’atténuation pour empêcher l’autre outil de tenter ce comportement.

Heureusement, il s’agit d’un événement très rare.

Cyber Crucible est désactivé par un autre outil

Il y a eu divers cas où des outils de sécurité disposant d’accès hautement privilégiés ont tenté à plusieurs reprises de désactiver le logiciel Cyber Crucible. Cela comprenait des tentatives répétées de suppression de notre pilote, ou d’arrêt forcé de notre service, encore et encore.

Bien que ces problèmes n’aient jamais affecté la défense contre l’extorsion, ils ont eu un impact négatif sur l’expérience utilisateur et les performances du système.

Tout cela relève désormais du passé.

Si un autre outil a la capacité, légitime ou non, de perturber Cyber Crucible, alors un pirate le pourrait également.

Si vous suspectez ou observez une quelconque diminution des capacités du logiciel Cyber Crucible, quel que soit le logiciel à l’origine de cette situation, veuillez nous contacter immédiatement.

Nous sommes généralement le dernier outil qui subsiste entre un extorqueur et vos données critiques. Il n’y a aucune place pour la faiblesse dans cette situation.

Revision #1
Created 2026-07-24 06:54:46 UTC by Dennis Underwood
Updated 2026-07-24 06:54:46 UTC by Dennis Underwood