Tester si le logiciel Cyber Crucible « fonctionne »

Introduction

Cyber Crucible est conçu pour fonctionner sans interrompre les utilisateurs finaux ou les employés, tout en notifiant discrètement les utilisateurs choisis du tableau de bord (généralement des membres choisis des équipes informatiques et de sécurité) des réponses automatisées.

Un grand nombre des simulateurs de rançongiciels ou de logiciels malveillants ne reproduisent pas fidèlement le comportement d'un pirate. Même si cela pose des problèmes pour des outils comme Cyber Crucible qui identifient (à juste titre) la simulation comme un faux positif, ce n'est pas nécessairement une mauvaise chose.

Certains fournisseurs conçoivent en réalité leurs moteurs de détection autour de ces simulateurs pour certaines de leurs fonctionnalités de détection, afin de s'assurer que tous les tests clients réussissent haut la main.

Les actions réelles de logiciels malveillants, comme le chiffrement par rançongiciel, présentent le risque de chiffrer ou de corrompre des données de manière irrécupérable. Chez Cyber Crucible, nous avons même constaté que certains rançongiciels activent secrètement d'autres logiciels malveillants sur le réseau, ou effectuent d'autres actions susceptibles de nuire à l'entreprise essayant de tester Cyber Crucible.

Vous ne souhaitez donc ni utiliser un logiciel malveillant, ni utiliser un simulateur si réaliste que vous risqueriez de corrompre accidentellement vos données.

Tester Cyber Crucible

Il existe un moyen simple de tester Cyber Crucible sans utiliser de logiciel malveillant ni de simulation si réaliste qu'elle mettrait en danger vos données ou celles de votre entreprise.

Cyber Crucible évalue les accès aux identités numériques à chaque milliseconde de la journée. Un grand nombre de ces identités numériques sont stockées dans les navigateurs - c'est pourquoi les attaquants placent les navigateurs web en tête de liste de leurs cibles automatisées.

L’analyse comportementale des accès aux identités par Cyber Crucible entraînera l’une des trois réponses suivantes :

1. Ne rien faire
2. Masquer les données
    1. application légitime connue qui réussit toutes les vérifications de mémoire et de noyau, mais qui n’a pas besoin d’accéder à cette donnée d’identité particulière - exemple : Windows Explorer non exploité
3. Suspendre le processus
    1. application légitime connue qui devrait avoir accès aux données d’identité mais qui est piratée, ou
    2. une application inhabituelle

Voici deux emplacements courants pour les utilisateurs Windows :

Dans ce cas, le nom d’utilisateur Windows est « denni », et ce sont les emplacements où les données de session sont stockées. Vous constaterez peut-être que la variable %LOCALAPPDATA% vous convient si vous ne souhaitez pas déterminer le nom d’utilisateur.

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
    - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

La vue sans Cyber Crucible installé

Voyons d’abord à quoi ressemble l’un de ces dossiers avec Explorer.exe, sans que Cyber Crucible soit installé.

Screenshot 2025-05-14 103339.png
Ici, nous voyons plusieurs sessions Chrome dans le profil Google Chrome « par défaut ».

Ces informations contiennent généralement des données sensibles qu’un attaquant chercherait à exploiter pour détourner des sessions liées à des programmes importants comme un portail d’administration informatique, des services bancaires, la messagerie électronique, ou des outils de stockage comme Google Drive ou Dropbox.

La vue avec Cyber Crucible installé

Après l’installation de Cyber Crucible, un test rapide peut être effectué, sans utiliser de logiciel malveillant ni aucun type de technique criminelle ou d’usage abusif du matériel informatique.

Dans ce cas, le même emplacement de stockage des sessions du navigateur est utilisé :

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
  - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
  - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

Screenshot 2025-05-14 103620.png
Cyber Crucible bloque déjà l’accès aux données de ce dossier immédiatement après l’installation.

Veuillez noter qu’il s’agit exactement du même processus Explorer qui était déjà en cours d’exécution au moment de l’installation ; le programme en cours d’exécution a donc soudainement vu son accès révoqué au niveau du « disque dur » ou du noyau. Même les programmes bénins, exploités ou malveillants déjà en cours d’exécution sont correctement évalués par Cyber Crucible.

Visualiser votre test dans le tableau de bord Cyber Crucible

Il existe un grand nombre d’accès aux données d’identité dans un système en fonctionnement, à tout moment.

Les logiciels en tant que service et les programmes basés sur le cloud ont conduit à de nombreux sites web et applications qui limitent le contenu sur le site lui-même, tandis que le navigateur (ou le navigateur intégré pour les applications) communique constamment avec des serveurs de données pour alimenter les feuilles de calcul, les tableaux, les graphiques et le contenu des réseaux sociaux.

Page Accès aux identités

Les accès aux identités jugés appropriés pour que Cyber Crucible suspende l’application incriminée sont répertoriés dans la page Accès aux identités.

Il s’agit de situations où le programme accédant aux données d’identité doit être arrêté, et pas seulement voir ses données masquées.

Dans ce cas, Explorer n’a pas été arrêté après la multitude de vérifications effectuées par Cyber Crucible. Les données ont simplement été masquées à la place.

Screenshot 2025-05-14 103741.png
Par conséquent, aucune violation d’accès aux identités n’est répertoriée ici.

Page Masquage des accès aux identités

Cyber Crucible dispose en option de la capacité de montrer aux clients du tableau de bord les situations dans lesquelles des données d’identité ont été masquées, mais où le programme accédant à ces données n’a pas été arrêté.

Explorer n’était ni exploité ni malveillant dans ce test ; il accédait simplement à des données d’identité hautement privilégiées pour les navigateurs Chrome et Edge.

La plupart des utilisateurs n’ont pas accès à ces informations, compte tenu de la charge supplémentaire imposée aux machines et réseaux des clients pour transmettre ces données aux serveurs de Cyber Crucible.

Merci de faire une demande si vous souhaitez obtenir cet accès, mais sachez que l’activité que vous observez n’est pas une activité malveillante, mais des comportements de confidentialité des données d’identité que Cyber Crucible met en œuvre dans une perspective de GRC, ou d’application de politiques.

Identity Hide Explorer.mp4
Ici, dans cette courte vidéo, nous voyons qu’Explorer a été empêché de visualiser les données de session du navigateur, même si Explorer lui-même n’a pas été interrompu.

Revision #1
Created 2026-07-24 06:39:30 UTC by Dennis Underwood
Updated 2026-07-24 06:39:30 UTC by Dennis Underwood