Déploiement et gestion des agents

Installer, configurer, mettre à jour et vérifier l'agent Cyber Crucible, y compris l'intégration, les prérequis système et la configuration réseau.

Comment puis-je tester la connexion à ces domaines ?

Comment puis-je tester la connexion à ces domaines ?

Vérification des chaînes de certificats

Le script PowerShell suivant peut être utilisé pour afficher la chaîne de certificats obtenue par une machine donnée. Cela peut être utile pour déboguer des problèmes SSL ou pour étudier l'impact d'une configuration de pare-feu SSL.

Utilisation

Dans la ligne de commande PowerShell, appelez le script avec le paramètre -TargetHost. Par exemple :

```
.\Get-SslCertificateChain.ps1 -TargetHost "agent.oauth.rpp.cybercrucible.com"
```

Le donne le résultat suivant :

```
SSL Connection established to agent.oauth.rpp.cybercrucible.com:443
Certificate Chain:
  Leaf Certificate (Subject): CN=agent.oauth.rpp.cybercrucible.com
True
    - Subject: CN=agent.oauth.rpp.cybercrucible.com
      Issuer: CN=E7, O=Let's Encrypt, C=US
      Thumbprint: 2E401711BBC229F34B8A13D0233264CFBB155C82
      Valid From: 10/05/2025 06:06:01
      Valid To: 01/03/2026 05:06:00
    - Subject: CN=E7, O=Let's Encrypt, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: 3B73C17E3DF87CF3AA77F1389219EB5EDD519E7F
      Valid From: 03/12/2024 20:00:00
      Valid To: 03/12/2027 18:59:59
    - Subject: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: CABD2A79A1076A31F21D253635CB039D4329A5E8
      Valid From: 06/04/2015 07:04:38
```

```
        Valid To: 06/04/2035 07:04:38
```

Comment puis-je surveiller l’état de santé des agents ?

Surveillance des agents hors ligne/en ligne

Page Agents

Sur la page Agents, la date et l’heure de la dernière vérification **par activité** sont suivies. De manière générale, si un agent logiciel fonctionne et est connecté à Internet, chaque comportement devrait afficher une date de moins de quelques heures. Certaines activités sont déclenchées par des actions sur le poste, tandis que d’autres sont programmées selon des minuteries, avec un décalage aléatoire (« jitter ») allant jusqu’à 30 secondes, afin que les clients n’aient pas de pics d’activité réseau.

85753879.png?width=680

Gestion des notifications hors ligne

Pour configurer la notification des agents hors ligne, utilisez la page Notifications de sécurité.

Ces notifications sont destinées aux situations suivantes :

1. Il existe un problème réseau entre un agent et les serveurs de Cyber Crucible. Cela peut être dû soit à un pare-feu (d’origine malveillante, ou simplement lié aux opérations informatiques), soit au fait que l’agent fonctionne mais est hors ligne. La protection est maintenue pendant les périodes hors ligne, mais les notifications à l’équipe de sécurité ne se produiront qu’une fois l’agent de nouveau en ligne.
2. Il existe un problème avec le logiciel Cyber Crucible. Ceci est très, très rare. Veuillez ouvrir un ticket de support auprès de Cyber Crucible immédiatement si cela se produit.
3. La machine est éteinte. C’est le scénario le plus courant. Une discussion sur les meilleures pratiques suit.

85688410.png?width=680

Meilleures pratiques pour les notifications hors ligne

Un point important à considérer concernant les notifications hors ligne est qu'une machine qui a été éteinte apparaîtra comme hors ligne pour les serveurs de Cyber Crucible. Les postes de travail, susceptibles d'être allumés et éteints pendant les opérations normales de l'entreprise, généreraient des notifications hors ligne pendant les pauses déjeuner, les déplacements entre sites, ou pendant les congés.

Les meilleures pratiques pour les groupes séparent déjà les serveurs des postes de travail. Les serveurs sont généralement mieux servis par des périodes de notification hors ligne plus courtes, en cas de problème. Les groupes axés sur les postes de travail sont mieux adaptés à des périodes plus longues avant l'apparition hors ligne.

De nombreux clients Cyber Crucible trouvent qu'il est préférable de créer des notifications automatisées uniquement pour les groupes de serveurs, et de filtrer périodiquement l'un des champs de date sur la page Gérer les agents par une date, par exemple « Montrez-moi les agents dont le champ Mise à jour des données de la machine n'a pas été mis à jour au cours de la dernière semaine ».

85688417.png?width=453

Agents qui ne sont pas entièrement mis à jour

Les agents Cyber Crucible nécessitent un redémarrage pour se mettre à jour. Une meilleure compréhension des algorithmes de mise à jour est disponible ici. Lorsqu'un agent signale qu'un redémarrage entraînera une mise à jour, la page Agents répertorie les machines qui nécessitent une mise à jour et qui sont prêtes à être mises à jour lors du redémarrage. Parfois, les machines qui ne sont pas redémarrées souvent (généralement les serveurs) accumuleront plusieurs mises à jour avant de réellement effectuer la mise à niveau. Nous en voyons un exemple dans la capture d'écran. L'heure du dernier redémarrage est également disponible.

Le rapport exécutif hebdomadaire de Cyber Crucible identifie le nombre d'agents nécessitant une mise à niveau, et combien d'entre eux sont prêts à être mis à niveau dès leur redémarrage. Les deux raisons les plus courantes pour lesquelles une machine nécessite une mise à jour, mais n'est pas prête/préparée, sont :

1. La machine a été hors ligne, par exemple un employé en vacances.

2. La machine a subi une panne matérielle ou logicielle majeure/un remplacement, et Cyber Crucible n’est en réalité plus présent sur cette machine.

En dehors de ces deux cas, les mises à jour se produisent normalement très rapidement, et sans intervention de l’administrateur en dehors des activités normales de correctifs et de redémarrage.

85688423.png

Quelles versions de Windows sont prises en charge par Cyber Crucible ?

Version de bureau	Version serveur	Prise en charge
11 10 8.1 8	2025 2022 2019 2016 2012 R2 2012 R1	Entièrement pris en charge.
7	2008 R2	Doit être corrigé (patché) pour la prise en charge de la signature de code SHA-2.
Vista et versions antérieures	2008 R1 et versions antérieures	Non pris en charge.

Quels sont les taux normaux de consommation des ressources pour la RAM et le CPU ?

L'utilisation typique du CPU est de 1 % ou moins (ce qui s'affiche comme 0 % sur la plupart des outils de surveillance, comme le Gestionnaire des tâches).

L'utilisation typique de la RAM est inférieure à 10 Mo. La plupart des utilisations sur postes de travail et serveurs se situent autour de 5 Mo.

Nous surveillons également l'utilisation de la mémoire du pilote dans l'espace noyau, afin de détecter tout problème éventuel.

Comment savoir si Cyber Crucible est en cours d’exécution sur le système ?

Services

Ouvrez le Gestionnaire des tâches.

Cliquez sur l’onglet Services.

Triez par nom si nécessaire, puis faites défiler jusqu’à CyberCrucibleAgent/ Cyber Crucible Agent

image-20250811-181519.png

Pilote noyau

Ouvrez une invite de commande en tant qu’administrateur.

Exécutez la commande observée dans la capture d’écran ci-dessous :

fltmc.exe | find « CCRRSecMon »

3047503.png?width=561
fltmc.exe répertorie les pilotes chargés.

Il y en a probablement plusieurs, c’est pourquoi la commande find n’affiche que le pilote Cyber Crucible, appelé CCRRSecMon.

Si le pilote est listé, il est chargé et fonctionne correctement dans le système d’exploitation.

Comment savoir quand un agent a terminé l'auto-configuration après l'installation ?

Sur la page Agents du tableau de bord, chaque agent possède quelques horodatages indiquant la dernière fois qu'il a reçu certains types d'informations. Un agent est considéré comme ayant terminé son auto-configuration lorsque, en plus de s'être vu attribuer une licence valide, il a enregistré des horodatages pour les colonnes suivantes :

- Dernière vérification de validation
- Dernier téléchargement des planifications
- Dernier téléchargement des comportements personnalisés
- Dernier téléchargement du pack de certificats

De plus, si le Groupe possède

Processus d'intégration

Gestion des groupes

Avant d'installer les agents, les utilisateurs peuvent souhaiter se préparer en configurant leurs groupes. Suivez les instructions de gestion des groupes ici.

Configuration des alertes de sécurité de l'agent

Les utilisateurs peuvent configurer des notifications par e-mail pour les événements de sécurité, y compris les activités de rançongiciel, les accès d'identité anormaux et les agents hors ligne. Les instructions se trouvent ici.

Meilleures pratiques de planification de l'installation de l'agent

Certains environnements présentent un comportement et une configuration similaires des utilisateurs, des applications et des systèmes dans l'ensemble de leur activité. D'autres disposent de groupes spécialisés qui se comportent différemment, comme une équipe de vente par rapport à une division d'ingénieurs logiciels.

Le déploiement et la configuration sont si rapides que consacrer quelques minutes à planifier une installation sur un sous-ensemble de postes de travail ou de serveurs partageant les mêmes comportements métier ou applications vous permettra d'évaluer si des applications doivent être prises en compte.

De plus, il est très courant que Cyber Crucible découvre des logiciels de gestion et des VPN auparavant inconnus (et non autorisés), des scripts d'administration non autorisés, des logiciels mal configurés, voire des infections lors du déploiement initial.

Installation de l'agent

Lorsque vous êtes prêt à installer vos agents, les instructions se trouvent ici et ici

Stratégies de mise à jour pour les groupes et les agents

Pour gérer les stratégies de mise à jour des groupes et des agents, suivez les instructions ici.

Comment enquêter sur la cause profonde d'une réponse à une extorsion

La page Réponse à l'extorsion se trouve sous l'onglet Opérations dans la barre latérale. Les instructions sur la manière d'enquêter sur la cause profonde d'une alerte se trouvent ici.

Comportements personnalisés

Les instructions pour créer des comportements personnalisés se trouvent ici.

Intégration REST

Certains utilisateurs peuvent souhaiter s'intégrer à notre serveur REST. La page d'intégration REST avec la documentation se trouve sur notre site web sous l'onglet Administration dans la barre latérale.

Déploiement dans un environnement déjà infecté

Contexte

Les déploiements chez les clients de Cyber Crucible aboutissent régulièrement à la découverte d'infections jusque-là inconnues. Les réseaux ne sont normalement pas exempts d'infections, même si les outils de défense en cybersécurité existants ont donné le feu vert.

Une attaque par rançongiciel constitue un point de démarcation, ou point pivot, hautement visible, permettant à une entreprise de mesurer à quelle fréquence les pirates réussissent à réattaquer, et avec quel succès.

- Les rapports en source ouverte et le renseignement sur les menaces révèlent un taux de réattaque d'environ 80 % chez les non-clients de Cyber Crucible.
- Cyber Crucible a observé qu'environ 10 % des terminaux subissent au moins une tentative d'usurpation d'identité, telle que le vol de mots de passe, de clés ou de jetons, par période de 90 jours.
- Cyber Crucible observe des attaquants tentant de reprendre pied dans un environnement environ une fois par mois.

Du point de vue de la réponse à incident ou de l'analyse judiciaire (forensique), Cyber Crucible est un excellent outil pour reprendre le contrôle du réseau. En particulier pour les victimes d'attaques, nous soupçonnons que les attaquants conservent une visibilité sur l'état de rétablissement et la santé financière des victimes, afin de mieux choisir le moment de frapper à nouveau.

Ce qui se passe immédiatement après l'installation

Cyber Crucible commence automatiquement à suspendre les programmes en cours d'exécution observés comme ayant un comportement malveillant.

Le déploiement du produit Cyber Crucible peut entraîner la suspension de plusieurs programmes sur plusieurs machines à mesure que l'environnement est nettoyé.

Parfois, un déploiement partiel de Cyber Crucible peut amener le pirate à tenter de reprendre le contrôle via les machines qui ne bénéficient pas de la protection Cyber Crucible.

Par exemple, Cyber Crucible avait été installé sur seulement une partie des postes de travail lors d'une récente violation de données subie par une victime. Les pirates ont tenté de désinstaller Cyber Crucible en se connectant depuis les machines non protégées, puis ont fini par éteindre les machines protégées.

Que se passe-t-il pour les logiciels malveillants dormants, en attente d'une future activation ?

Un logiciel malveillant qui n'agit pas pour le compte des attaquants est déclenché dès qu'il commence à accéder aux données.

Voyons un scénario :

Deux machines contiennent des logiciels malveillants. Appelons-les Machine A et Machine B.

Les deux échantillons de logiciels malveillants sont actuellement indétectables par vos outils de sécurité préférés.

Le logiciel malveillant de la Machine A ne fait rien, mais attend des instructions. Cyber Crucible ne détecte pas le logiciel malveillant. Ce dernier n'est pas non plus encore détectable par d'autres outils de sécurité.

Le logiciel malveillant de la Machine B tente d'accéder à des données ou à des données d'identité. Immédiatement après une attaque réussie, le comportement le plus courant que nous observons, lorsque les attaquants pilotent leur logiciel malveillant, consiste à s'assurer qu'ils disposent de données d'identité fraîches, telles que des mots de passe ou des jetons, et à recenser de nouvelles données. Il s'agit donc en partie de « récupérer les nouveaux mots de passe après que les administrateurs les ont réinitialisés », et en partie de « surveiller l'apparition de nouvelles données ».

Sur la Machine B, Cyber Crucible suspend immédiatement l'application.

Après une période allant d'un mois à un an, le logiciel malveillant de la Machine A finit par être repéré une fois qu'un nombre suffisant de victimes a signalé ce logiciel malveillant aux bases de données des éditeurs de sécurité. Plus les attaquants font preuve de discipline dans la distribution de cet échantillon, plus ce logiciel malveillant particulier échappera longtemps à la détection.

Le logiciel malveillant de la Machine B a été neutralisé, figé sur place.

Le logiciel malveillant de la Machine A est piégé. Dès la seconde (en fait, les 100 millisecondes) où il tente d'accéder à des données ou à des informations d'identité, le logiciel malveillant de la Machine A est suspendu. Le client est protégé, même si le logiciel malveillant existe pendant des jours, voire des années, sans être détecté par d'autres outils.

Détails supplémentaires - Les redémarrages peuvent être utiles

Certaines de nos analyses sont les plus précises lorsque le cycle de vie d'un processus peut être suivi depuis le démarrage de l'application jusqu'à l'état actuel.

Redémarrer une machine après l'installation peut être avantageux.

Les programmes déjà en cours d'exécution avant l'installation ne bénéficieront pas d'une inspection analytique complète de la part de Cyber Crucible. Le redémarrage force ces programmes à se relancer, fournissant ainsi une inspection complète pour tous les programmes.

Comment tester la connexion TLS à ces domaines ?

Au-delà du simple ping des domaines utilisés par Cyber Crucible pour s'assurer que votre point de terminaison peut atteindre toutes les adresses réseau correctes, le programme d'installation de l'agent Cyber Crucible inclut un argument de test qui garantit qu'une connexion TLS/SSL valide peut être établie dans les deux sens avec tous les serveurs requis.

Untitled-20240410-185719.png
Il suffit d'ajouter `--test-connection` à l'exécution du programme d'installation, en veillant à toujours inclure le ou les identifiants de groupe ainsi que les jetons OAuth nécessaires pour effectuer l'authentification. On voit ci-dessus une capture d'écran montrant la seule modification nécessaire au script .bat fourni, ainsi qu'une sortie réussie.

Pièces jointes :

▨ Untitled-20240410-185719.png (image/png)

Pourquoi pourrais-je avoir besoin d'un proxy ?

Bien que toute la détection comportementale et la protection de l'agent Cyber Crucible s'effectuent au niveau du point de terminaison, sans nécessiter l'envoi d'échantillons vers le cloud pour analyse, l'agent du point de terminaison nécessite tout de même une connexion à un serveur pour recevoir les informations de licence, la configuration, les mises à jour logicielles, etc.

Si votre réseau est verrouillé au point de ne pas autoriser les connexions vers les plages IP où les serveurs Cyber Crucible sont hébergés, vous devrez peut-être configurer un proxy pour permettre à l'agent (uniquement) d'atteindre son serveur pour l'installation. Consultez Comment gérer les configurations de proxy pour obtenir des informations sur la configuration de l'agent.

Quel type de proxy puis-je utiliser ?

Depuis la version 4.4.6.3 de l'agent Cyber Crucible, les configurations de proxy prennent en charge Socks5. Il n'y a aucune restriction quant à l'endroit où le serveur est hébergé (sur site ou hors site), tant que les restrictions réseau permettent aux agents de l'atteindre. Un exemple de schéma est présenté ci-dessous illustrant une configuration proxy simple où le serveur Socks5 est hébergé au sein du réseau verrouillé, et n'est autorisé qu'à se connecter à une machine externe qui achemine le trafic en tunnel.

SOCKS5H.png

Cette configuration permet aux agents de se connecter à leur(s) serveur(s), tout en maintenant la politique réseau. Elle ne nécessite qu'une seule règle autorisant l'hôte Socks5 à atteindre son serveur proxy externe sur un seul port (ssh). Cela garantit non seulement que tout le trafic passe par le port 443, mais aussi qu'il est doublement encapsulé en SSH avant de quitter le réseau, sans nécessiter de redirection de port entrant.

Quelle quantité de données est produite par Cyber Crucible ?

Les données collectées par l'agent Cyber Crucible passent par plusieurs couches de filtrage, afin de réduire le bruit provenant d'une télémétrie brute trop importante. Les données brutes produites par les capteurs du noyau sont réduites [**Filtre n° 1**] afin de diminuer à la fois l'utilisation de la mémoire du terminal et la bande passante réseau par agent. Ensuite, l'API REST associera la télémétrie brute des processus/terminaux qu'elle reçoit à des réponses automatisées, de sorte que l'analyste puisse choisir de ne visualiser que les données pertinentes [**Filtre n° 2**].

Blank diagram-20240523-165941.png

Comme le montre la figure ci-dessus, les terminaux de poste de travail d'un client moyen peuvent produire plusieurs gigaoctets de données brutes de capteurs sur une période de 24 heures, alors que seulement quelques mégaoctets de ces données seront pertinents pour une alerte du SOC en cas de tentative d'attaque.

Comment désinstaller plusieurs agents à la fois ?

Désinstaller plusieurs agents à la fois est simple.

Rendez-vous sur la page Agents.

Nous recommandons d'utiliser des filtres, tels que le nom de machine, le groupe, l'adresse IP ou les filtres de version, pour afficher à l'écran le plus grand nombre possible d'agents. Ceci est particulièrement utile pour les utilisateurs disposant de centaines, voire de milliers d'agents dans un groupe.

85983282.png?width=680
Ici, nous avons utilisé la touche Maj, tout en cliquant sur 3 lignes, pour sélectionner trois agents.

Le bouton Désinstaller tous les agents sélectionnés se trouve en haut à gauche, au-dessus de la grille.

Une fois les autorisations vérifiées sur le serveur, confirmant que vous disposez des droits nécessaires dans les groupes des agents, les commandes de désinstallation seront émises.

Les agents reçoivent une commande de désinstallation signée numériquement. Cette signature est utilisée par les agents pour valider que la commande provient réellement de Cyber Crucible, et non d'un criminel tentant de supprimer votre logiciel de protection.

Une fois les agents validés, ils préparent le système en vue de la désinstallation lors du redémarrage.

La colonne Attention affichera la mention « Désinstallation en cours » et présentera un bouton Annuler la désinstallation dans la cellule.

Une fois la machine redémarrée, l'agent valide que la désinstallation est en cours et supprime tous les fichiers.

Point important à noter : l'agent confirmera « un dernier bonjour » avant de se désinstaller complètement, il est donc possible que les agents soient encore présents pendant une courte période après le redémarrage. Cela est dû au fait que certains environnements réseau ne fonctionnent pas correctement pendant jusqu'à 30 secondes après l'apparition du bureau. Notez qu'une fois les désinstallations terminées, les licences sont automatiquement retirées des agents.

Comment désinstaller un seul agent ?

Accédez à la page Agents.

Repérez l'agent souhaité, puis cliquez sur l'icône de corbeille dans la colonne Nom de l'agent :

86081562.png?width=680

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.

Comment gérer les configurations de proxy

Notez que seuls les agents en version 4.4.6.3 et supérieure disposent de cette fonctionnalité

Où trouver le paramètre de configuration proxy actuel d’un groupe

Les utilisateurs peuvent consulter le paramètre de configuration proxy actuel d’un groupe pour les agents de ce groupe en accédant d’abord à la page Groupes, située sous l’onglet Administration dans la barre latérale.

Le paramètre de configuration proxy actuel d’un groupe se trouve dans la colonne « Proxy Server Config » de la grille.

Si le groupe n’a pas de configuration de serveur proxy activée, le texte « Do Not Use Proxy » sera affiché.

Proxy Server Config Column.png
Si le groupe a une configuration de serveur proxy activée, l’URL de la configuration proxy actuelle sera affichée

Proxy Server Config Enabled.png

Comment mettre à jour un groupe pour activer un serveur proxy

Les utilisateurs peuvent activer l'utilisation d'un serveur proxy pour les agents d'un groupe en cliquant d'abord sur l'icône de gestion des configurations proxy dans la colonne « Proxy Server Config » de la page Groupes. En cliquant sur cette icône, une fenêtre modale s'ouvrira, permettant aux utilisateurs de gérer les configurations de serveur proxy pour le groupe.

Manage Proxy Server Config Icon.png
La fenêtre modale Manage Proxy Server Configuration qui s'affiche permet de consulter et de gérer les configurations de serveur proxy pour le groupe. Les utilisateurs peuvent enregistrer plusieurs configurations au sein d'un groupe, et toutes les configurations enregistrées sont affichées dans la grille de cette fenêtre modale. Notez que toutes les configurations de serveur proxy enregistrées pour un groupe apparaîtront également dans la fenêtre modale Download Agent.

Afin de sélectionner une configuration de serveur proxy pour le groupe, la configuration doit d'abord être soumise via le formulaire New Proxy Configuration. Ce formulaire est masqué par défaut ; cliquez sur le bouton bascule pour l'afficher.

Manage Proxy Server Configs Modal.pngNew Proxy Configuration Form.png
Après avoir soumis le formulaire de nouvelle configuration, celle-ci s'affichera ci-dessous dans la grille de la fenêtre modale.

Pour sélectionner une configuration proxy que les agents de ce groupe devront utiliser, sélectionnez d'abord la configuration souhaitée, puis cliquez sur l'icône de modification au-dessus de la grille.

Select Config for Group.png
Après avoir cliqué sur l'icône de modification pour la configuration proxy souhaitée, la configuration proxy actuelle du groupe est désormais mise à jour et peut être consultée dans cette fenêtre modale ainsi que dans la colonne « Proxy Server Config ». Les agents de ce groupe utiliseront désormais la configuration proxy mise à jour du groupe. Notez que si un agent reçoit l'instruction de basculer vers un serveur proxy inaccessible, il ne basculera pas tant que ce serveur ne sera pas de nouveau accessible.

Mange Proxy Server Config Modal Setting Enabled.pngGroup Proxy Config Enabled.png

Comment mettre à jour un groupe pour ne pas utiliser de proxy

Si un groupe a un serveur proxy activé pour les agents de ce groupe et que les utilisateurs souhaitent mettre à jour le groupe afin que les agents de ce groupe n'utilisent plus de proxy, accédez d'abord à la page Groupes et localisez le groupe souhaité dans la grille.

Cliquez ensuite sur l'icône de gestion des configurations proxy dans la colonne « Proxy Server Config ». En cliquant sur cette icône, la fenêtre modale Manage Proxy Server Configuration s'affichera.

Proxy Server Config Column 2.png
Dans cette fenêtre modale, cliquez sur l'icône x pour mettre à jour les agents de ce groupe afin qu'ils n'utilisent pas de serveur proxy et qu'ils appellent nos serveurs normalement. Notez que la configuration proxy actuelle ne sera pas supprimée des configurations proxy enregistrées du groupe ; il s'agit d'une étape distincte expliquée dans la section ci-dessous.

Do Not Use Proxy Icon.png
Après avoir cliqué sur l'icône x, la fenêtre modale sera mise à jour pour refléter ce changement et la colonne « Proxy Server Config » pour ce groupe affichera désormais « Do Not Use Proxy ».

No Current Proxy Config Selected .pngDo Not Use Proxy Cell.png

Comment supprimer une configuration de proxy enregistrée dans un groupe

Pour supprimer une configuration proxy enregistrée d'un groupe, accédez d'abord à la page Groupes et localisez le groupe souhaité dans la grille.

Cliquez ensuite sur l'icône de gestion des configurations proxy dans la colonne « Proxy Server Config ». En cliquant sur cette icône, la fenêtre modale Manage Proxy Server Configuration s'affichera.

Manage Proxy Server Config Icon.png

Dans cette fenêtre modale, cliquez sur la configuration proxy enregistrée que vous souhaitez supprimer pour ce groupe, puis cliquez sur l'icône de la corbeille. Après avoir cliqué sur cette icône, la configuration proxy sélectionnée n'apparaîtra plus dans la grille en tant que configuration proxy enregistrée pour le groupe.

Remove Saved Config.png
Notez que si vous supprimez une configuration proxy enregistrée pour un groupe et que cette configuration est définie comme la configuration de serveur proxy actuelle du groupe, cela mettra également à jour la configuration de serveur proxy actuelle du groupe pour qu'il n'utilise pas de proxy.

Comment installer un agent en utilisant un proxy

Tout d'abord, accédez à la page Agents, située sous l'onglet Operations dans la barre latérale. Cliquez ensuite sur le bouton Download Agent. En cliquant sur ce bouton, la fenêtre modale Download Agent s'ouvrira.

Download Agent Button.png
Dans cette fenêtre modale, si vous sélectionnez un groupe disposant de configurations proxy enregistrées, l'option Select Proxy Configuration for Installer apparaîtra, avec le paramètre actuel du groupe sélectionné par défaut. Toutes les configurations proxy enregistrées du groupe apparaîtront également comme options, y compris une option Do Not Use Proxy.

Download Agent Modal.pngDownload Agent Modal Proxy Config Options.png
Lorsque vous choisissez d'utiliser un proxy pour le programme d'installation, le seul type de programme d'installation possible est le Command Line Installer.

Si vous sélectionnez l'option Do Not Use Proxy, nos options habituelles de type de programme d'installation apparaîtront.

Download Agent Modal Do Not Use Proxy.png
Notez que si vous sélectionnez pour le programme d'installation une configuration proxy qui n'est pas le paramètre actuel du groupe, le programme d'installation s'exécutera avec le paramètre sélectionné, puis basculera vers le paramètre de configuration proxy actuel du groupe après l'installation.

Où puis-je voir si un agent est capable de contourner le proxy ?

Les utilisateurs peuvent vérifier si les agents peuvent se connecter à nos serveurs sans utiliser de proxy en accédant d'abord à la page Agents, située sous l'onglet Operations dans la barre latérale. Localisez ensuite la colonne Agent is Able to Bypass Proxy dans la grille.

Notez que la colonne Agent is Able to Bypass Proxy ne sera visible que si l'utilisateur est membre d'un groupe ayant activé l'utilisation d'un proxy pour les agents du groupe.

Si l'agent appartient à un groupe ayant activé l'utilisation d'un proxy et que l'agent ne peut pas contourner le proxy pour se connecter à nos serveurs, une croix rouge s'affichera dans la colonne. Voir un exemple ci-dessous :

Agent Cannot Bypass Proxy.png
Si l'agent appartient à un groupe ayant activé l'utilisation d'un proxy et que l'agent est capable de contourner le proxy et de se connecter normalement à nos serveurs, une coche verte s'affichera dans la colonne. Voir un exemple ci-dessous :

Agent Can Bypass Proxy.png