Tableau de bord et rapports

Utilisation de l'application web Cyber Crucible : visibilité des agents, activité des processus, analyses de mémoire et rapports destinés à la direction.

Cyber Crucible peut-il répondre silencieusement à une attaque, sans m'alerter/me notifier ?

Vous pourriez constater qu'il existe des scénarios légitimes où vous ne souhaitez pas qu'une application fasse quelque chose (probablement sur vos machines), mais sans avoir besoin d'être notifié à chaque fois.

Il s'agit d'une situation distincte de celle où vous avez besoin d'une mise en liste blanche, où aucune action n'est entreprise par la prévention d'extorsion de données de Cyber Crucible.

La fonctionnalité que vous recherchez est celle des réponses automatisées silencieuses.

Rendre silencieuse une réponse automatisée existante pour l'avenir :

Tout d'abord, rendez-vous sur la page Gérer les incidents. Nous allons prochainement renommer cette page en Gérer les réponses.

Ensuite, cliquez sur le bouton haut-parleur/volume comme illustré ci-dessous.

4784131.png?width=680
Cliquer sur ce bouton fait apparaître la fenêtre modale « Silence Incident » ou « Silence Auto-Response ».

Nous disposons d'analyses qui vérifient si une réponse doit être silencieuse en fonction des programmes et arguments précédemment sélectionnés.

Dans ce cas, nous constatons qu'Adobe exécute un serveur web dans le cadre de sa suite logicielle, et nous ne souhaitons plus recevoir d'alertes futures indiquant que le serveur web a été suspendu.

(Dans ce cas, nous avons inséré du code javascript malveillant dans le fichier exécuté par Adobe, et Cyber Crucible a suspendu le serveur web d'Adobe pour l'empêcher de voler ou de chiffrer des données.)

4784138.png
Cliquez sur « Take me to Silent Responses Page »

Un menu apparaîtra pour insérer cette règle de silence spécifique, mais examinons d'abord la page :

5013506.png?width=680
Nous voyons ici que les règles sont basées à la fois sur le processus et sur les arguments du processus pour une réponse automatisée, qui ne devrait pas être incluse dans les e-mails de notification ou autres alertes.

La suspension a toujours lieu - simplement sans notification à ce sujet.

Nous voyons ici que nous ne voulons pas que le navigateur Microsoft Edge, ou le navigateur Chrome, puisse s'exécuter en utilisant ces arguments, avec des jokers avant et après pour tenir compte des autres arguments présents.

(Explication de sécurité : Les deux navigateurs exécutent un morceau de code identique, qui charge les navigateurs en arrière-plan sans fenêtre à l'écran, afin de scanner et de lire vos fichiers en coulisses. Nous ne voulons pas que nos navigateurs web fassent cela dans notre dos !)

Que vous créiez ou non une règle de réponse silencieuse entièrement préventive, la même fenêtre ci-dessous (dans la section suivante) constitue l'étape suivante.

Création d'une réponse silencieuse

Nous voyons ici à la fois le chemin du programme et les arguments du programme. Les jokers sont autorisés, pour garantir qu'un élément comme un nom d'utilisateur ou un numéro de version d'application n'empêche pas votre règle comportementale de fonctionner.

Un exemple illustrant pourquoi les jokers sont nécessaires est le fait qu'il pourrait y avoir un programme sur tous les postes de travail de vos employés qui appartiennent à un groupe.

C:\Users\mary\Desktop\runme.exe
C:\Users\joe\Desktop\runme.exe

La solution serait :

C:\Users*\Desktop\runme.exe

5046277.png

Ici, nous voyons que nous créons une réponse silencieuse pour l'ensemble du groupe TEMPORARY GIRAFFE 2, pour un chemin Adobe Creative Cloud, et nous ne souhaitons rendre silencieuses que les réponses ayant un argument spécifique (dans ce cas, un chemin de fichier vers un certain fichier javascript).

Il n'y a aucun élément unique dans le chemin, comme des noms d'utilisateur, nous pouvons donc créer la règle telle quelle.

Les réponses peuvent être nommées, les noms étant uniques par groupe.

Les règles commencent à être distribuées aux agents en quelques minutes.

Comment puis-je enquêter sur la cause profonde d'un événement ?

Il existe trois éléments de base d'analyse à votre disposition lors de l'investigation d'une alerte.

Il est actuellement plus probable qu'un attaquant mène diverses activités sur un système, en utilisant une combinaison de techniques en mémoire et de détournement de processus (injection ou hollowing), plutôt que d'exécuter un programme « hacker.exe » évident.

Analytique de la mémoire

Le premier élément de base se trouve sur la page Réponse ou Incident elle-même. L'analytique de la mémoire suit les comportements du processus en mémoire lors d'une inspection continue des comportements possibles d'extorsion de données (vol ou chiffrement).

Un état de mémoire indiquant une falsification probable est généralement révélateur d'un problème.

Ce n'est pas toujours malveillant en soi, car de mauvaises pratiques de programmation ou des bogues logiciels peuvent également entraîner la falsification de l'état de mémoire d'un programme en cours d'exécution.

63504385.png?width=680
Nous voyons ici un cas où un processus Adobe Acrobat présente des comportements possibles d'extorsion de données après l'ouverture d'un PDF téléchargé, et nous constatons que la mémoire du processus Acrobat avait été modifiée. Le processus Acrobat.exe sur le disque n'a été affecté d'aucune manière.

L'analyse forensique de la mémoire impliquée avec l'Acrobat.exe suspendu indiquera probablement un problème préoccupant - possiblement un exploit en cours d'utilisation, sinon une injection de processus ou un hollowing de processus.

Pour les réponses d'extorsion dont la valeur Mémoire modifiée est Vrai, une icône de téléchargement est disponible dans la colonne Analyse de la cause profonde pour télécharger le fichier de différence mémoire (Memory Diff) pour la réponse :

63602693.png?width=680
Le fichier de différence mémoire (Memory Diff File) est le code source compilé de ce qui a été injecté dans le programme. Il contient probablement un logiciel malveillant et/ou du code d'exploit, à examiner par un analyste en malwares ou en sécurité. Notez que ce fichier ne contient pas le programme entier, seulement la partie qui a été modifiée par un exploit ou une technique d'attaque comme l'injection de processus. Apprenez-en plus sur ce fichier ici.

Analytique de l'injection de processus

Le premier indicateur qu'un événement d'injection de processus pertinent pour une réponse automatisée est peut-être présent est la colonne Threads distants non fiables (Untrusted Remote Threads) pour un incident/réponse. Cela indique qu'une analyse comportementale au niveau du noyau a révélé la présence d'un thread distant non fiable observé avec le processus menant un comportement de vol de données ou de type rançongiciel.

63471635.png?width=680
Une investigation plus approfondie peut être effectuée sur la page Injection de processus. La valeur True pour Threads distants non fiables est un bon indicateur pour décider de s'y rendre.

La colonne Analyse de la cause profonde comporte également une icône permettant de vous rediriger automatiquement vers la page Injections afin de n'afficher que les injections de processus liées à la réponse.

63602703.png?width=680
Après avoir cliqué sur l'icône des injections, vous serez dirigé vers la page Injections de processus, où vous verrez uniquement les injections de processus liées à la réponse :

63569930.png?width=680
Ici, sur la page Événements d'injection de processus, nous voyons le chemin et les arguments du processus injecteur, ainsi que le chemin et les arguments du processus injecté. Habituellement, les arguments jouent un rôle très important dans l'analytique de la mémoire, ou indiquent, par exemple, quelles commandes PowerShell exécuter. Les identifiants de processus (PID) sont également présents, pour aider à retracer les injections itératives effectuées lorsqu'un attaquant passe de processus en processus, ou pour rechercher l'analyse de la cause profonde dans la page

Création de processus.

63438879.png?width=680
Comment savions-nous que rundll32.exe était en réalité un éditeur d'antivirus ? Continuez votre lecture !

Analytique de la création de processus

Il est très rare qu'un attaquant n'utilise qu'un seul processus au cours de son attaque. Il se peut même qu'il ne sache pas que les outils qu'il utilise génèrent de nouveaux processus, et qu'il utilise divers outils d'administration sur le système infecté.

La page Création de processus suit tous les processus qui ouvrent d'autres processus (ou le même), les arguments utilisés, ainsi que les identifiants de processus, ou Pids, pour chaque source et destination.

Cela est effectué au niveau du noyau, ce qui signifie que rien n'est manqué.

Remarque : la télémétrie de Microsoft dispose d'une partie de ces données, mais pas de toutes. Nous choisissons de ne pas utiliser cette source de données, car nous avons constaté que cette source de télémétrie a été observée manquer des événements importants, ou être désactivée par des attaquants lors d'une attaque.

Quelle est la qualité de notre visibilité ?

Tout assembler - une investigation de bout en bout

Quelle est la qualité de notre visibilité, et à quelle vitesse pouvez-vous effectuer une analyse de la cause profonde ? Découvrez cet exemple - un antivirus disposant sans doute de l'un des niveaux de permissions les plus élevés sur un système a été observé en train d'essayer d'injecter du code dans notre logiciel Cyber Crucible. Nous espérons que c'était pour examiner notre logiciel, mais nous entrons tout de même en mode d'auto-protection (ainsi, cela a conduit notre logiciel à rejeter la falsification de l'antivirus... il n'existe aucune porte dérobée permettant à des parties externes d'accéder, de modifier ou d'utiliser notre logiciel).

Alors, commençons ici, avec une réponse automatisée :

63569937.png?width=680

Évidemment, Cyber Crucible n'est pas un rançongiciel. Nous voyons ici qu'une tentative d'injection de processus impliquant un comportement de thread distant suspect, en conjonction avec des comportements de type extorsion de données.

D'accord - regardons ce qui se passe dans les Événements d'injection de processus en cliquant sur l'icône des injections. 5 secondes plus tard - nous avons notre réponse !

63471644.png?width=56463438879.png?width=680

Mais attendez - rundll ? Ce n'est pas un hacker, n'est-ce pas ? Ce n'est sûrement pas un programme hacker.exe. Effectuons un peu de filtrage, pour obtenir notre réponse sur la page Création de processus. Nous n'avons pas de capture d'écran ici, mais les identifiants de processus sont disponibles pour toutes les réponses et injections de processus. Retournons à la page des réponses, et cliquons sur l'icône des créations de processus pour être dirigés vers la page Créations de processus et filtrer automatiquement la grille pour afficher les créations de processus liées à cette réponse.

63537184.png63438886.png?width=680

Rapidement et facilement, nous constatons maintenant que la « racine » (sans jeu de mots) était WebRoot, un éditeur d'antivirus, qui avait généré un processus rundll32.exe pour charger l'une des DLL de WebRoot, laquelle a ensuite tenté de faire *quelque chose* avec le logiciel de Cyber Crucible, pour le forcer à itérer à travers les fichiers comme un outil de vol de données.

Pourquoi avons-nous choisi de présenter cet exemple ?

Nous disposons d'exemples abondants du savoir-faire des attaquants, avec des niveaux de compétence variables de leur part. Les antivirus atteignent un niveau de permissions sur un système qui exige un très haut niveau de compétence, de technologie et de préparation de la part des attaquants. Le fait que Cyber Crucible détecte des comportements « de type hacker » de la part d'un outil de sécurité grand public, puis les arrête automatiquement, démontre certains des plus hauts niveaux d'excellence en ingénierie et en sécurité de notre part, sans se perdre dans des exploits individuels ou le savoir-faire des attaquants.

Que montre la page Injections de processus ?

Les injections de processus sont une capacité d'ingénierie logicielle qui peut apparaître dans un contexte non malveillant, ou être directement utilisée par un attaquant. En fait, l'injection de processus et les techniques associées sont l'une des méthodes favorites des attaquants, pour diverses raisons qui dépassent le cadre de cet article (mais si vous le demandez, nous pouvons vous orienter vers une formation).

Cyber Crucible expose les événements d'injection de processus au niveau du noyau. Cela signifie que vous disposez d'une visibilité complète sur tous les processus et leurs informations, quelles que soient les permissions de ce processus. Nous avons constaté qu'une fois que les attaquants ou les logiciels atteignent un certain niveau de permissions, de nombreuses sources traditionnelles de télémétrie pour les outils de sécurité deviennent silencieuses. Ne jamais manquer une donnée importante, et ne jamais devenir silencieux, constitue une part essentielle de la conception zero trust de notre produit.

Sur la page Injections de processus, vous verrez les éléments suivants pour chaque événement, avec des filtres disponibles pour affiner vos requêtes :

CC_Showing_All_Process_Injection_Columns.mp4
Normalement, dans le cadre d'une enquête, vous constaterez qu'il existe une activité supplémentaire sur la page Création de processus.

Que montre la page Créations de processus ?

Il est très rare, voire inexistant, qu'un attaquant réalise une attaque entière depuis un seul processus.

Le fait qu'un outil d'attaque ou une bibliothèque Windows utilise plusieurs processus et programmes Windows est parfois invisible aux utilisateurs du logiciel malveillant (c'est-à-dire les criminels).

Les comportements des processus représentent une source importante de variables dans la prise de décision de Cyber Crucible, laquelle s'appuie sur des indicateurs comportementaux provenant de diverses sources.

Ces comportements de processus peuvent parfois aboutir à une suspension de processus liée à un vol de données ou à un chiffrement par ranançongiciel, et peuvent être retracés depuis le point d'entrée de l'attaquant dans le système jusqu'à l'exécution finale du logiciel d'extorsion.

Dans d'autres cas, le traçage des processus peut permettre d'identifier un accès distant non autorisé, une fraude, une menace interne ou un logiciel inattendu, mais sans extorsion de données. Il ne s'agit donc pas nécessairement de quelque chose que le logiciel de prévention de l'extorsion de données de Cyber Crucible suspendra automatiquement, mais c'est tout de même une information que vous voudrez connaître.

Que les données de processus fassent partie d'une attaque d'extorsion de données, qu'elles concernent un autre élément notable, ou qu'il s'agisse simplement d'un comportement de programme, les informations sur la source et la destination des programmes, y compris les arguments des programmes, sont mises à disposition. Cela fournit un ensemble riche de données permettant de retracer les attaquants, y compris ceux qui utilisent des tactiques de « living off the land ».

Vous trouverez ci-dessous une capture d'écran du type de données pouvant être recueillies à partir des créations de processus.

CC_process_creation_demo.mp4

Que sont les résumés de rapports exécutifs ?

Introduction

Les résumés de rapports exécutifs sont des rapports envoyés par e-mail aux utilisateurs qui détaillent des informations sur les licences, les agents et les comportements des machines des utilisateurs. Les rapports contiennent un résumé de tous les groupes dont l'utilisateur fait partie, suivi d'un résumé pour chaque groupe individuel.

Les utilisateurs ont la possibilité de recevoir des rapports hebdomadaires et mensuels, ainsi que de choisir le format du rapport envoyé dans l'e-mail (HTML, ZIP, etc.).

Comment activer ou désactiver la réception des rapports

Après s'être connectés à notre site Web et avoir accédé à la page Paramètres du compte, les utilisateurs verront les options permettant de définir leurs préférences pour la réception des rapports hebdomadaires et mensuels, ainsi que de définir le format du rapport envoyé dans l'e-mail.

24051723.png?width=442

Exemple de contenu de rapport

23887914.png?width=44224084489.png?width=44223855156.png?width=442

Comment afficher les agents masqués ?

Accédez à la page Agents et repérez la colonne Visibilité du tableau de bord.

86048770.png?width=680
Le filtre par défaut de cette colonne fait en sorte que les agents masqués ne soient pas visibles.

Pour afficher les agents masqués, ouvrez le filtre de cette colonne, cochez la case Masqué, décochez la case Visible, puis cliquez sur Appliquer.

Cela n'affichera que les agents masqués. À partir de là, vous pouvez effectuer les opérations habituelles de gestion des agents, y compris la modification de la visibilité.

86016006.png?width=45386016013.png?width=680

Comment masquer ou supprimer un agent ?

Il est important de comprendre que la suppression d'un agent entraînerait également la suppression de toutes les données collectées via cet agent. Ces informations pourraient s'avérer utiles un jour pour une enquête future.

Il est donc probablement préférable de masquer l'agent de la vue, des notifications ou des alertes.

Il existe deux façons de procéder.

Mise à jour groupée des agents

La première méthode est la plus simple lorsque plusieurs agents doivent être masqués de l'application web.

Tout d'abord, sélectionnez les agents que vous souhaitez masquer, depuis la page Agents.

Normalement, les utilisateurs utiliseront d'abord des filtres basés sur le statut d'installation, le nom de la machine ou l'adresse IP.

Ensuite, sélectionnez l'icône « Bulk Set Agent Default Visibility ».

86048779.png?width=680
Une fenêtre modale apparaîtra dans laquelle vous pourrez choisir si la visibilité par défaut des agents sélectionnés sera masquée ou visible. Cliquez ensuite sur le bouton « Update Selected Agents ».

86081547.png?width=448
Le paramètre par défaut pour les notifications de sécurité consiste à envoyer des alertes d'agent hors ligne pour les agents masqués. Pour en savoir plus sur les notifications de sécurité, consultez cette page.

Mettre à jour un seul agent

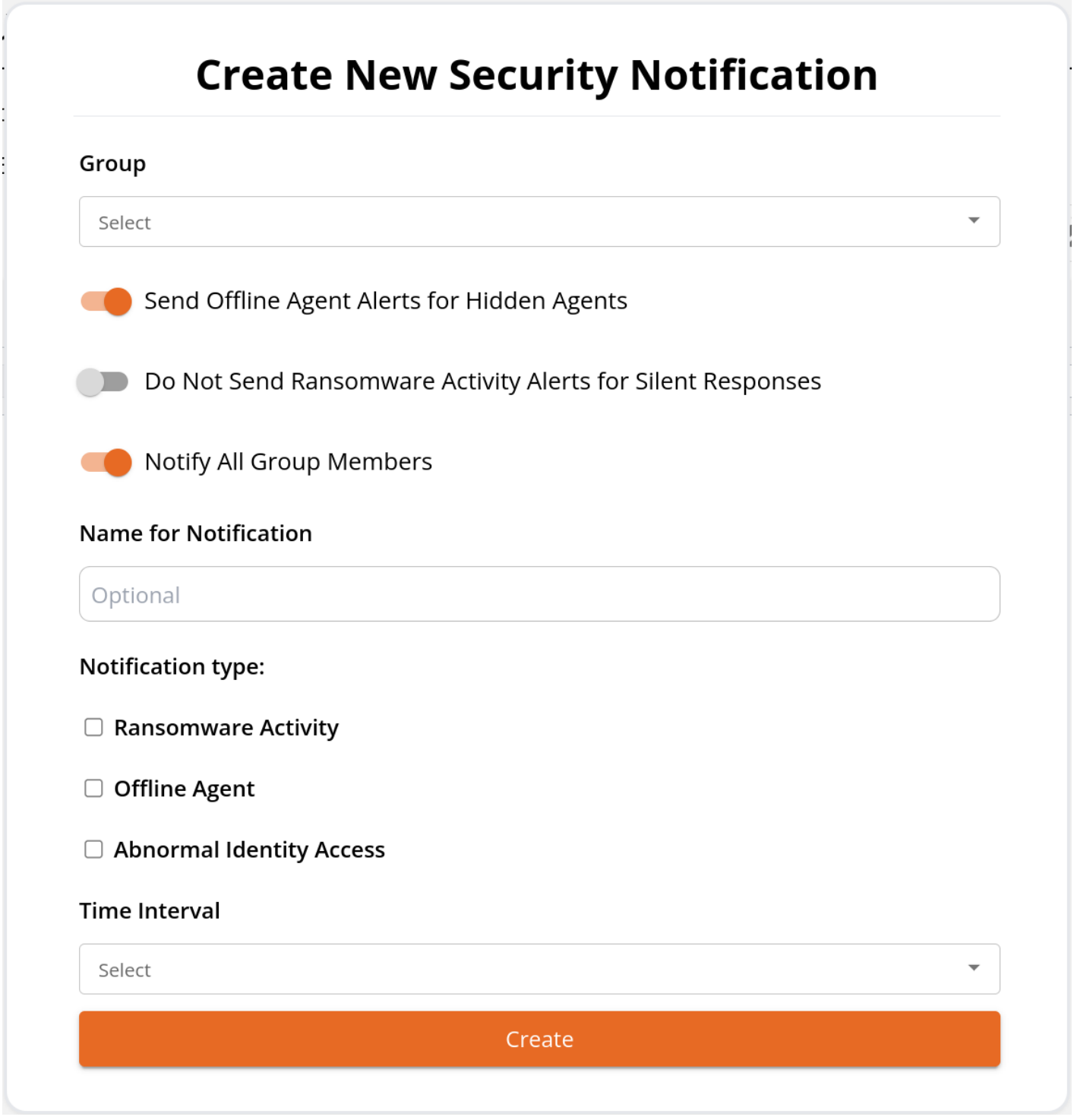
Sur la page Agents, repérez la colonne Visibilité du tableau de bord et basculez le curseur Visible de l'agent souhaité pour modifier sa visibilité.

86016024.png?width=680

Si je masque un agent, continuerai-je à recevoir des alertes et des notifications ?

Le paramètre par défaut pour les notifications consiste à envoyer des alertes d'agent hors ligne pour les agents masqués.

Nous voyons ci-dessous le paramètre par défaut lors de la création d'une notification :



Les utilisateurs créent normalement une catégorie de notification distincte pour les notifications d'agents masqués, pour les rares cas où cela est souhaité. Nous recommandons que ces notifications utilisent des alias d'adresse e-mail de destination différents et éventuellement un intervalle de notification distinct.

Si une notification existante nécessite une mise à jour de ce champ, rendez-vous sur la page Notifications de sécurité.

Faites défiler la grille vers la droite jusqu'à ce que vous voyiez la colonne Envoyer des alertes hors ligne pour les agents masqués, puis activez ou désactivez le curseur selon vos besoins.

Le changement prendra effet immédiatement.