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.

Revision #1
Created 2026-07-24 06:40:51 UTC by Dennis Underwood
Updated 2026-07-24 06:40:51 UTC by Dennis Underwood