A Cyber Crucible pode responder silenciosamente a um ataque, mas sem me alertar/notificar?

Você pode constatar que existem cenários legítimos em que não deseja que uma aplicação faça algo (provavelmente nas suas máquinas), mas não precisa ser notificado sempre que isso ocorrer.

Esta é uma situação diferente daquela em que você precisa de algo na lista de permissões (whitelist), na qual nenhuma ação é tomada pela prevenção de extorsão de dados da Cyber Crucible.

A funcionalidade que você está procurando é a de respostas automáticas silenciosas.

Tornando uma resposta automática existente silenciosa no futuro:

Primeiro, vá para a página Manage Incidents. Em breve, estaremos alterando o nome para Manage Responses.

Segundo, clique no botão de alto-falante/volume, conforme mostrado abaixo.

4784131.png?width=680
Clicar neste botão abre a janela modal “Silence Incident” ou “Silence Auto-Response”.

Temos análises que verificam se uma resposta deve ser silenciosa com base em programas e argumentos previamente selecionados.

Neste caso, vemos que o Adobe executa um servidor web como parte do seu conjunto de software, e não queremos nenhum alerta futuro de que o servidor web foi suspenso.

(Neste caso, inserimos um JavaScript malicioso no arquivo que o Adobe executou, e a Cyber Crucible suspendeu o servidor web do Adobe para impedir o roubo ou a criptografia de dados.)

4784138.png
Clique em “Take me to Silent Responses Page”

Haverá um menu para inserir essa regra de silêncio específica, mas vamos primeiro observar a página:

5013506.png?width=680
Vemos aqui que as regras são baseadas tanto no processo quanto nos argumentos do processo para uma resposta automática, que não deve ser incluída em e-mails de notificação ou outros alertas.

A suspensão ainda ocorre - apenas não há notificação sobre ela.

Vemos aqui que não queremos que o navegador Microsoft Edge, ou o navegador Chrome, possam ser executados ao usar esses argumentos, com wildcards antes e depois para contemplar outros argumentos presentes.

(Explicação técnica de segurança: Ambos os navegadores executam um trecho de código idêntico, que carrega os navegadores em segundo plano sem uma janela na tela, a fim de escanear e ler seus arquivos de forma oculta. Não queremos que nossos navegadores web façam isso pelas nossas costas!)

Independentemente de você estar criando uma regra de resposta silenciosa totalmente preventiva ou não, a mesma janela abaixo (na próxima seção) é o próximo passo.

Criando uma Resposta Silenciosa

Aqui vemos tanto o caminho do programa quanto os argumentos do programa. Wildcards são permitidos, para garantir que algo como um nome de usuário ou número de versão de aplicação não impeça que sua regra comportamental funcione.

Um exemplo de por que os wildcards são necessários é porque pode haver um programa em todas as áreas de trabalho dos seus funcionários que estão em um grupo.

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

A solução seria:

C:\Users*\Desktop\runme.exe

5046277.png

Aqui, vemos que estamos criando uma resposta silenciosa para todo o grupo TEMPORARY GIRAFFE 2, para um caminho do Adobe Created Cloud, e queremos silenciar apenas as respostas que possuem um argumento específico (neste caso, um caminho de arquivo para um determinado arquivo javascript).

Não há partes exclusivas no caminho, como nomes de usuário, então podemos criar a regra como está.

As respostas podem ser nomeadas, sendo os nomes exclusivos por grupo.

As regras começam a ser distribuídas para os agentes em poucos minutos.

Revision #1
Created 2026-07-24 05:31:23 UTC by Dennis Underwood
Updated 2026-07-24 05:31:23 UTC by Dennis Underwood