Kann Cyber Crucible auf einen Angriff still reagieren, ohne mich zu benachrichtigen/alarmieren?

Es kann legitime Szenarien geben, in denen Sie nicht möchten, dass eine Anwendung etwas tut (wahrscheinlich auf Ihren Rechnern), Sie aber nicht bei jedem Vorfall benachrichtigt werden müssen.

Dies ist eine andere Situation als die, in der Sie etwas auf die Whitelist setzen müssen, sodass durch die Datenerpressungs-Prävention von Cyber Crucible keine Maßnahme ergriffen wird.

Die Funktion, nach der Sie suchen, sind stille automatisierte Reaktionen (silent automated responses).

Eine bestehende automatisierte Reaktion künftig still schalten:

Gehen Sie zunächst zur Seite „Vorfälle verwalten“ (Manage Incidents). Wir werden den Namen in naher Zukunft in „Reaktionen verwalten“ (Manage Responses) ändern.

Klicken Sie anschließend auf die Lautsprecher-/Lautstärke-Schaltfläche, wie unten zu sehen.

4784131.png?width=680
Durch Klicken auf diese Schaltfläche öffnet sich das Modal „Vorfall stummschalten“ bzw. „Automatische Reaktion stummschalten“ (Silence Incident / Silence Auto-Response).

Wir verfügen über Analysefunktionen, die anhand zuvor ausgewählter Programme und Argumente prüfen, ob eine Reaktion still erfolgen sollte.

In diesem Fall sehen wir, dass Adobe als Teil seiner Softwaresuite einen Webserver ausführt, und wir möchten künftig keine Warnungen mehr erhalten, dass der Webserver angehalten wurde.

(In diesem Fall haben wir bösartigen JavaScript-Code in die von Adobe ausgeführte Datei eingeschleust, und Cyber Crucible hat den Webserver von Adobe daran gehindert, Daten zu stehlen oder zu verschlüsseln.)

4784138.png
Klicken Sie auf „Zur Seite für stille Reaktionen“ (Take me to Silent Responses Page)

Es wird ein Menü zum Einfügen dieser spezifischen Stummschaltungsregel angezeigt, aber schauen wir uns zunächst die Seite an:

5013506.png?width=680
Wir sehen hier, dass die Regeln sowohl auf dem Prozess als auch auf den Prozessargumenten für eine automatisierte Reaktion basieren, die nicht in Benachrichtigungs-E-Mails oder anderen Warnungen enthalten sein soll.

Das Anhalten erfolgt weiterhin – nur ohne Benachrichtigung darüber.

Wir sehen hier, dass wir nicht möchten, dass der Microsoft-Edge-Browser oder der Chrome-Browser mit diesen Argumenten ausgeführt werden können, mit Platzhaltern davor und danach, um andere vorhandene Argumente zu berücksichtigen.

(Sicherheitshinweis zur Erklärung: Beide Browser führen ein identisches Codestück aus, das die Browser im Hintergrund ohne sichtbares Fenster lädt, um im Verborgenen Ihre Dateien zu scannen und zu lesen. Wir möchten nicht, dass unsere Webbrowser das hinter unserem Rücken tun!)

Unabhängig davon, ob Sie eine vollständig präventive stille Reaktionsregel erstellen oder nicht, ist das gleiche Fenster unten (im nächsten Abschnitt) der nächste Schritt.

Erstellen einer stillen Reaktion

Hier sehen wir sowohl den Programmpfad als auch die Programmargumente. Platzhalter sind erlaubt, um sicherzustellen, dass beispielsweise ein Benutzername oder eine Anwendungsversionsnummer Ihre Verhaltensregel nicht daran hindert, zu funktionieren.

Ein Beispiel dafür, warum Platzhalter benötigt werden: Es könnte ein Programm auf allen Desktops Ihrer Mitarbeiter geben, die einer Gruppe angehören.

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

Die Lösung wäre:

C:\Users*\Desktop\runme.exe

5046277.png

Hier sehen wir, dass wir eine stille Reaktion für die gesamte Gruppe TEMPORARY GIRAFFE 2 erstellen, für einen von Adobe Creative Cloud angelegten Pfad, und wir möchten nur Reaktionen

stummschalten, die ein bestimmtes Argument aufweisen (in diesem Fall einen Dateipfad zu einer bestimmten JavaScript-Datei).

Es gibt keine eindeutigen Bestandteile im Pfad, wie z. B. Benutzernamen, sodass wir die Regel so erstellen können, wie sie ist.

Reaktionen können benannt werden, wobei die Namen pro Gruppe eindeutig sind.

Die Regeln beginnen innerhalb weniger Minuten, an die Agenten verteilt zu werden.

Revision #2
Created 2026-07-24 04:16:45 UTC by Dennis Underwood
Updated 2026-11-24 15:52:58 UTC by Dennis Underwood