Panel de control e informes

Uso de la aplicación web de Cyber Crucible: visibilidad de agentes, actividad de procesos, análisis de memoria e informes ejecutivos.

¿Puede Cyber Crucible responder silenciosamente a un ataque, pero sin alertarme/notificarme?

Puede que encuentre situaciones legítimas en las que no desea que una aplicación haga algo (probablemente en sus equipos), pero no necesita ser notificado cada vez.

Esta es una situación distinta a cuando necesita poner algo en lista blanca, donde no se realiza ninguna acción por parte de la prevención de extorsión de datos de Cyber Crucible.

La capacidad que está buscando son las respuestas automáticas silenciosas.

Hacer que una respuesta automática existente sea silenciosa en el futuro:

Primero, vaya a la página Manage Incidents. Cambiaremos el nombre a Manage Responses en un futuro cercano.

Segundo, haga clic en el botón de altavoz/volumen como se ve a continuación.

4784131.png?width=680
Al hacer clic en este botón se abre la ventana modal “Silence Incident” o “Silence Auto-Response”.

Contamos con análisis que verifican si una respuesta debe ser silenciosa según los programas y argumentos previamente seleccionados.

En este caso, vemos que Adobe ejecuta un servidor web como parte de su suite de software, y no queremos ninguna alerta futura de que el servidor web fue suspendido.

(En este caso, insertamos javascript malicioso en el archivo que ejecutaba Adobe, y Cyber Crucible suspendió el servidor web de Adobe para evitar el robo o cifrado de datos.)

4784138.png
Haga clic en “Take me to Silent Responses Page”

Aparecerá un menú para insertar esa regla de silencio específica, pero primero veamos la página:

5013506.png?width=680
Vemos aquí que las reglas se basan tanto en el proceso como en los argumentos del proceso para una respuesta automática, que no deben incluirse en los correos electrónicos de notificación ni en otras alertas.

La suspensión sigue ocurriendo, simplemente no hay notificación al respecto.

Vemos aquí que no queremos que el navegador Microsoft Edge, ni el navegador Chrome, puedan ejecutarse cuando se utilicen esos argumentos, y comodines antes y después para tener en cuenta otros argumentos presentes.

(Perspectiva explicativa de seguridad: Ambos navegadores ejecutan una pieza de código idéntica, que carga los navegadores en segundo plano sin una ventana en la pantalla, con el fin de escanear y leer sus archivos de forma encubierta. ¡No queremos que nuestros navegadores web hagan eso a nuestras espaldas!)

Independientemente de si está creando una regla de respuesta silenciosa completamente preventiva o no, la misma ventana que se muestra a continuación (en la siguiente sección) es el siguiente paso.

Creación de una respuesta silenciosa

Aquí vemos tanto la ruta del programa como los argumentos del programa. Se permiten comodines, para asegurar que algo como un nombre de usuario o un número de versión de la aplicación no impida que su regla de comportamiento funcione.

Un ejemplo de por qué se necesitan comodines es porque podría haber un programa en todos los escritorios de sus empleados que forman parte de un grupo.

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

La solución sería:

C:\Users*\Desktop\runme.exe

5046277.png

Aquí vemos que estamos creando una respuesta silenciosa para todo el grupo TEMPORARY GIRAFFE 2, para una ruta de Adobe Created Cloud, y solo queremos silenciar las respuestas que tengan un argumento específico (en este caso, una ruta de archivo hacia un determinado archivo javascript).

No hay elementos únicos en la ruta, como nombres de usuario, por lo que podemos crear la regla tal cual.

Las respuestas pueden tener un nombre, siendo los nombres únicos por grupo.

Las reglas comienzan a distribuirse a los agentes en cuestión de minutos.

¿Cómo puedo investigar la causa raíz de un evento?

Existen tres bloques fundamentales de análisis a su disposición al investigar una alerta.

Actualmente, es más probable que un atacante realice una variedad de actividades en un sistema, utilizando una combinación de técnicas en memoria y secuestro de procesos (inyección o hollowing), que ejecutar un programa "hacker.exe" evidente.

Análisis de Memoria

El primer bloque fundamental se encuentra en la propia página de Respuesta o Incidente. Los análisis de memoria rastrean los comportamientos del proceso en memoria durante la inspección continua de posibles comportamientos de extorsión de datos (robo o cifrado).

Un estado de memoria que indica una probable manipulación suele ser indicativo de un problema.

No siempre es malicioso en sí mismo, ya que las malas prácticas de programación o los errores de software también pueden hacer que el estado de memoria de un programa en ejecución se vea alterado.

63504385.png?width=680
Aquí vemos un caso en el que un proceso de Adobe Acrobat exhibe posibles comportamientos de extorsión de datos después de abrir un PDF descargado, y vemos que la memoria del proceso Acrobat había sido modificada. El proceso Acrobat.exe en el disco no se vio afectado de ninguna manera.

El análisis forense de la memoria involucrada con el Acrobat.exe suspendido probablemente indicará un problema de preocupación, posiblemente un exploit en uso, si no una inyección de proceso o un hollowing de proceso.

Para las respuestas de extorsión con un valor de Memoria Modificada de True (Verdadero), hay un ícono de descarga en la columna de Análisis de Causa Raíz para descargar el archivo de Diferencia de Memoria (Memory Diff) de la respuesta:

63602693.png?width=680
El archivo de Diferencia de Memoria (Memory Diff File) es el código fuente compilado de lo que se inyectó en el programa. Probablemente contenga malware y/o código de exploit, para que un analista de malware o de seguridad lo examine. Tenga en cuenta que este archivo no contiene el programa completo, solo la parte que fue alterada mediante un exploit o una técnica de ataque como la inyección de procesos. Obtenga más información sobre este archivo aquí.

Análisis de Inyección de Procesos

El primer indicador de que puede haber un evento de inyección de procesos relevante para una respuesta automatizada es la columna de Subprocesos Remotos No Confiables (Untrusted Remote Threads) de un Incidente/Respuesta. Esto indica que el análisis de comportamiento a nivel de kernel reveló un subproceso remoto no confiable observado con el proceso que realiza robo de datos o un comportamiento similar al ransomware.

63471635.png?width=680
Se puede realizar una investigación adicional en la página de Inyección de Procesos. Que el valor de Subprocesos Remotos No Confiables sea True (Verdadero) es un buen indicador de si se debe acudir allí.

La columna de Análisis de Causa Raíz también tiene un ícono para redirigirlo automáticamente a la página de Inyecciones, para mostrar solo las inyecciones de procesos relacionadas con la respuesta.

63602703.png?width=680
Después de hacer clic en el ícono de inyecciones, será dirigido a la página de Inyecciones de Procesos, donde verá solo las inyecciones de procesos relacionadas con la respuesta:

63569930.png?width=680
Aquí, en la página de Eventos de Inyección de Procesos, vemos la ruta y los argumentos del proceso inyector, y la ruta y los argumentos del proceso inyectado. Por lo general, los argumentos desempeñan un papel muy importante en los análisis de memoria, o indican, por ejemplo, qué comandos de PowerShell ejecutar. Los ID de proceso también están presentes, para ayudar a rastrear las inyecciones iterativas realizadas cuando un atacante salta de proceso en proceso, o para buscar el análisis de causa raíz en la página de Creación de Procesos.

63438879.png?width=680
¿Cómo supimos que rundll32.exe era en realidad un proveedor de antivirus? ¡Sigan leyendo!

Análisis de Creación de Procesos

Es muy poco común que un atacante utilice un solo proceso durante su ataque. Puede que ni siquiera sepa que las herramientas que está utilizando están generando nuevos procesos y utilizando varias herramientas administrativas en el sistema infectado.

La página de Creación de Procesos rastrea todos los procesos que abren otros procesos (o el mismo proceso), los argumentos utilizados y los ID de proceso, o Pids, para cada origen y destino.

Esto se realiza a nivel de kernel, lo que significa que no se pasa por alto nada.

Nota: la telemetría de Microsoft cuenta con parte de estos datos, pero no con todos. Optamos por no utilizar esa fuente de datos, ya que hemos observado que dicha fuente de telemetría tiende a pasar por alto eventos importantes, o los atacantes la desactivan durante un ataque.

¿Qué tan buena es nuestra visibilidad?

Uniéndolo todo: una investigación de extremo a extremo

¿Qué tan buena es nuestra visibilidad y con qué rapidez puede realizar un Análisis de Causa Raíz? Vea este ejemplo: se observó que un antivirus, que posiblemente cuenta con algunos de los permisos más altos en un sistema, intentaba inyectar código en nuestro software Cyber Crucible. Esperamos que haya sido para investigar nuestro software, pero de todos modos entramos en modo de autoprotección (por lo tanto, esto hizo que nuestro software rechazara la manipulación del antivirus... no existen puertas traseras que permitan el acceso para editar o utilizar nuestro software por parte de terceros externos).

Entonces, empecemos por aquí, con una respuesta automatizada:

63569937.png?width=680
Obviamente, Cyber Crucible no es ransomware. Aquí vemos que hubo un intento de inyección de procesos que implicaba un comportamiento sospechoso de subprocesos remotos, junto con comportamientos similares a la extorsión de datos.

De acuerdo, veamos qué está sucediendo en Eventos de Inyección de Procesos haciendo clic en el ícono de inyecciones. 5 segundos después, ¡tenemos nuestra respuesta!

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

Pero espere, ¿rundll? Eso no es un hacker, ¿verdad? Seguramente, eso no es un programa hacker.exe. Hagamos algo de filtrado para obtener nuestra respuesta en la página de Creación de Procesos. No tenemos una captura de pantalla aquí, pero los ID de proceso están disponibles para todas las respuestas e inyecciones de procesos. Volvamos a la página de respuestas y hagamos clic en el ícono de creaciones de procesos para ir a la página de Creaciones de Procesos y filtrar automáticamente la cuadrícula para mostrar las creaciones de procesos relacionadas con esta respuesta.

63537184.png63438886.png?width=680

De forma rápida y sencilla, ahora vemos que la "raíz" (sin juego de palabras) fue WebRoot, un proveedor de antivirus, que generó un proceso rundll32.exe para cargar una de las DLL de WebRoot, la cual luego intentó hacer *algo* con el software de Cyber Crucible, para forzarlo a recorrer archivos como una herramienta de robo de datos.

¿Por qué elegimos mostrar este ejemplo?

Contamos con numerosos ejemplos de las técnicas de los atacantes, con distintos niveles de competencia por parte de estos. Los antivirus alcanzan un nivel de permisos en un sistema que requiere un nivel muy alto de habilidad, tecnología y preparación por parte de los atacantes. Que Cyber Crucible detecte comportamientos "similares a los de un hacker" provenientes de una herramienta de seguridad convencional, y luego los detenga automáticamente, demuestra algunos de los niveles más altos de ingeniería y excelencia en seguridad de nuestra parte, sin perdernos en exploits individuales o técnicas específicas de los atacantes.

¿Qué muestra la página de Inyecciones de Procesos?

Las inyecciones de procesos son una capacidad de ingeniería de software que puede aparecer en un contexto no malicioso, o ser utilizada directamente por un atacante. De hecho, la inyección de procesos y las técnicas asociadas son una de las favoritas de los atacantes, por diversas razones que quedan fuera del alcance de este artículo (pero si nos lo pregunta, podemos orientarlo hacia capacitación al respecto).

Cyber Crucible expone los eventos de inyección de procesos a nivel del kernel. Esto significa que usted tiene visibilidad completa de todos los procesos y su información, independientemente de los permisos de ese proceso. Algo que hemos comprobado es que, una vez que los atacantes o el software alcanzan cierto nivel de permisos, muchas de las fuentes tradicionales de telemetría para las herramientas de seguridad dejan de reportar información. No perder nunca un dato importante, y no quedarse nunca en silencio, es una parte fundamental del diseño de nuestro producto basado en confianza cero (zero trust).

En la página de Inyecciones de Procesos, verá lo siguiente por cada evento, con filtros disponibles para refinar sus consultas:

CC_Showing_All_Process_Injection_Columns.mp4
Normalmente, en el transcurso de una investigación, encontrará que hay actividad adicional en la página de Creación de Procesos.

¿Qué muestra la página de Creaciones de Procesos?

Es muy poco común, posiblemente nunca ocurra, que un atacante ejecute un ataque completo desde dentro de un solo proceso.

El hecho de que una herramienta de ataque o una biblioteca de Windows utilice múltiples procesos y programas de Windows a veces es invisible para los usuarios del malware (es decir, los delincuentes).

Los comportamientos de los procesos representan una fuente importante de variables durante la toma de decisiones de Cyber Crucible, la cual involucra indicadores de comportamiento provenientes de una variedad de fuentes.

En ocasiones, estos comportamientos de procesos pueden derivar finalmente en la suspensión de un proceso a causa del robo de datos o del cifrado por ransomware, y pueden rastrearse desde el punto de entrada del atacante en el sistema hasta la ejecución final del software de extorsión.

En otras ocasiones, el rastreo de procesos puede identificar acceso remoto no autorizado, fraude, amenazas internas o software inesperado, pero sin extorsión de datos. Por lo tanto, no se trata de algo que el software de prevención de extorsión de datos de Cyber Crucible suspenda automáticamente, pero sigue siendo algo que usted querrá conocer.

Ya sea que los datos del proceso formen parte de un ataque de extorsión de datos, de algo más digno de mención, o simplemente del comportamiento habitual de un programa, se pone a disposición la información de origen y destino de los programas, incluidos los argumentos del programa. Esto proporciona un rico conjunto de datos para rastrear a los atacantes, incluidos aquellos que aprovechan tácticas de “living off the land”.

A continuación se muestra una captura de pantalla del tipo de datos que se pueden recopilar a partir de las creaciones de procesos.

CC_process_creation_demo.mp4

¿Qué son los Resúmenes de Informes Ejecutivos?

Introducción

Los Resúmenes de Informes Ejecutivos son informes enviados por correo electrónico a los usuarios que detallan información sobre las licencias, agentes y comportamientos de las máquinas de los usuarios. Los informes contienen un resumen de todos los grupos en los que se encuentra el usuario, seguido de un resumen para cada grupo individual.

Los usuarios tienen la opción de recibir informes semanales y mensuales, así como elegir el formato del informe enviado en el correo electrónico (HTML, ZIP, etc.).

Cómo Suscribirse y Cancelar la Suscripción para Recibir Informes

Después de iniciar sesión en nuestro sitio web y navegar a la página de Configuración de la Cuenta, los usuarios verán las opciones para establecer sus preferencias para recibir informes semanales y mensuales, así como configurar el formato del informe que se envía en el correo electrónico.

24051723.png?width=442

Contenido de Muestra del Informe

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

¿Cómo muestro los agentes ocultos?

Diríjase a la página de Agentes y localice la columna Visibilidad del Panel.

86048770.png?width=680
El filtro predeterminado de esta columna hace que los agentes ocultos no sean visibles.

Para mostrar los agentes ocultos, abra el filtro de esta columna y marque la casilla de Oculto, y desmarque la casilla de Visible, luego haga clic en Aplicar.

Esto mostrará únicamente los agentes ocultos. Desde allí, puede realizar las operaciones normales de gestión de agentes, incluido el cambio de visibilidad.

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

¿Cómo oculto o elimino un agente?

Es importante comprender que eliminar un agente también eliminaría todos los datos recopilados a través de ese agente. Esa información podría ser útil algún día para una futura investigación.

En su lugar, ocultar el agente de la vista, las notificaciones o las alertas es probablemente la acción deseada.

Hay dos formas de hacer esto.

Actualización Masiva de Agentes

El primer método es el más sencillo si hay varios agentes que necesitan ser ocultados de la aplicación web.

Primero, seleccione los agentes que desea ocultar, desde la página de Agentes.

Normalmente, los usuarios utilizarán primero filtros basados en el estado de instalación, el nombre de la máquina o la dirección IP.

Segundo, seleccione el icono “Bulk Set Agent Default Visibility” (Establecer visibilidad predeterminada de agentes en masa).

86048779.png?width=680
Aparecerá una ventana modal donde podrá seleccionar si la visibilidad predeterminada de los agentes seleccionados será oculta o visible. Luego, haga clic en el botón “Update Selected Agents” (Actualizar agentes seleccionados).

86081547.png?width=448
La configuración predeterminada para las notificaciones de seguridad es enviar alertas de agentes fuera de línea para los agentes ocultos. Consulte más información sobre las notificaciones de seguridad aquí.

Actualizar un Solo Agente

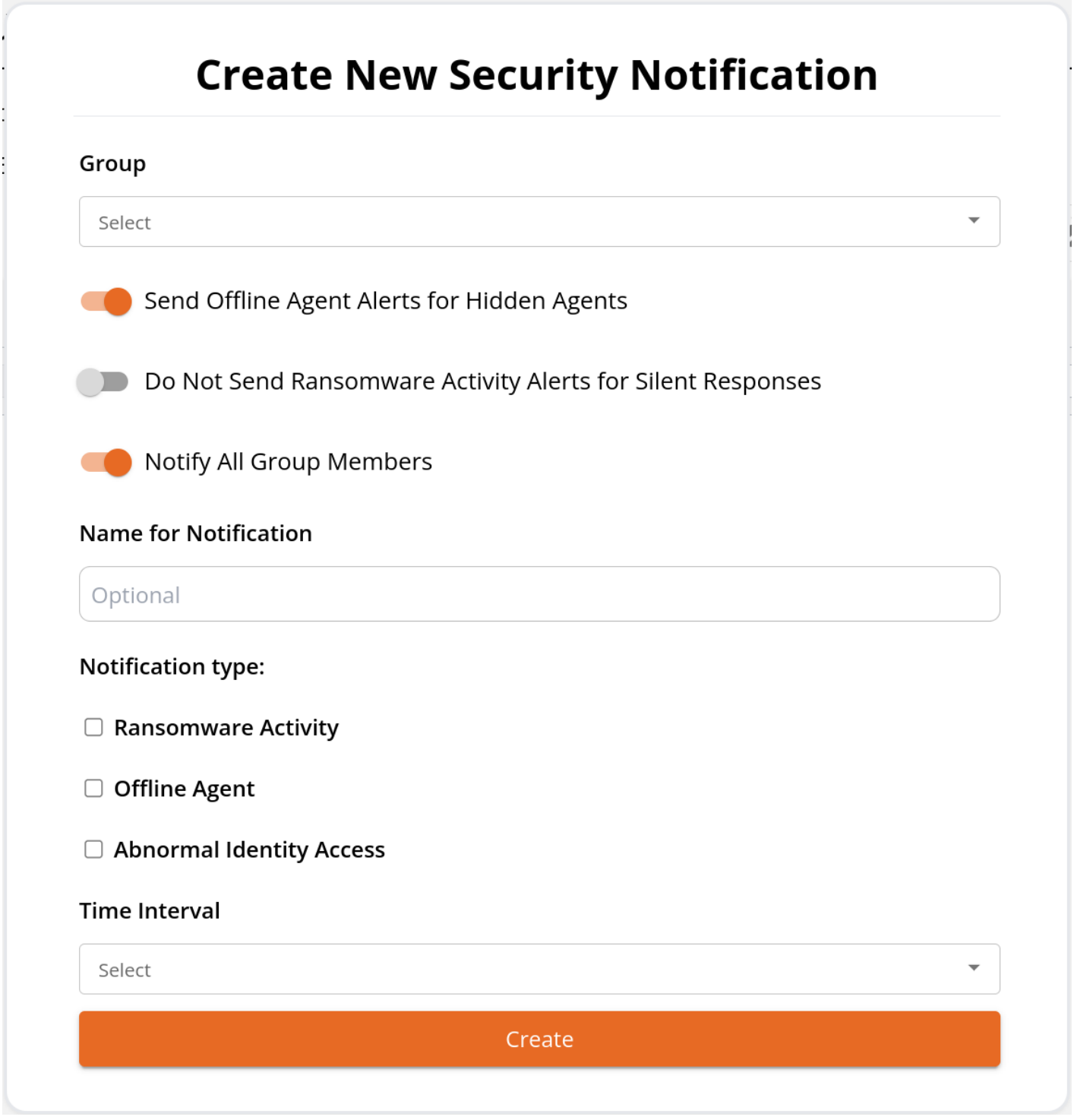
En la página de Agentes, localice la columna de Visibilidad del Panel y active o desactive el control deslizante Visible para el agente deseado con el fin de cambiar su visibilidad.

86016024.png?width=680

Si oculto un agente, ¿seguiré recibiendo alertas y notificaciones?

La configuración predeterminada para las notificaciones es enviar alertas de agente sin conexión para los agentes ocultos.

A continuación se muestra la configuración predeterminada durante la creación de notificaciones:



Normalmente, los usuarios crean una categoría de notificación independiente para las notificaciones de agentes ocultos, para los casos poco frecuentes en que esto sea deseado. Recomendamos que estas notificaciones tengan alias de correo electrónico de destino diferentes y, posiblemente, un intervalo de notificación distinto.

Si una notificación existente requiere una actualización de este campo, diríjase a la página de Notificaciones de Seguridad.

Desplácese hacia la derecha en la cuadrícula hasta que vea la columna Enviar Alertas Sin Conexión para Agentes Ocultos, y luego active o desactive el control deslizante según lo desee.

El cambio surtirá efecto de inmediato.