Implementación y Gestión de Agentes

Instalación, configuración, actualización y verificación del agente de Cyber Crucible, incluyendo la incorporación, los requisitos del sistema y la configuración de red.

¿Cómo puedo probar la conexión a estos dominios?

¿Cómo puedo probar la conexión a estos dominios?

Verificación de Cadenas de Certificados

El siguiente script de PowerShell puede utilizarse para mostrar la cadena de certificados obtenida por una máquina en particular. Esto puede ser útil para depurar problemas de SSL o investigar el impacto de una configuración de firewall SSL.

Uso

En la línea de comandos de PowerShell, invoque el script con el parámetro -TargetHost. Por ejemplo:

```
.\Get-SslCertificateChain.ps1 -TargetHost "agent.oauth.rpp.cybercrucible.com"
```

El se obtuvo el siguiente resultado:

```
SSL Connection established to agent.oauth.rpp.cybercrucible.com:443
Certificate Chain:
  Leaf Certificate (Subject): CN=agent.oauth.rpp.cybercrucible.com
True
    - Subject: CN=agent.oauth.rpp.cybercrucible.com
      Issuer: CN=E7, O=Let's Encrypt, C=US
      Thumbprint: 2E401711BBC229F34B8A13D0233264CFBB155C82
      Valid From: 10/05/2025 06:06:01
      Valid To: 01/03/2026 05:06:00
    - Subject: CN=E7, O=Let's Encrypt, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: 3B73C17E3DF87CF3AA77F1389219EB5EDD519E7F
      Valid From: 03/12/2024 20:00:00
      Valid To: 03/12/2027 18:59:59
    - Subject: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: CABD2A79A1076A31F21D253635CB039D4329A5E8
      Valid From: 06/04/2015 07:04:38
```

```
        Valid To: 06/04/2035 07:04:38
```

¿Cómo monitoreo el estado (Health) del Agente?

Monitoreo de Agentes Offline/Online

Página de Agentes

En la página de Agentes, se registra la fecha y hora del último check-in **por actividad**. En términos generales, si un agente de software está funcionando y conectado a Internet, cada comportamiento debería tener una fecha de menos de un par de horas. Algunas actividades son activadas por eventos en el endpoint, mientras que otras se establecen mediante temporizadores, pero con un desfase de "jitter" de hasta 30 segundos, para que los clientes no experimenten picos en la actividad de red.

85753879.png?width=680

Gestión de Notificaciones Offline

Para configurar la notificación de agentes offline, utilice la página de Notificaciones de Seguridad.

Estas notificaciones están pensadas para las siguientes situaciones:

1. Existe un problema de red entre un agente y los servidores de Cyber Crucible. Esto puede deberse a un firewall (provocado por un atacante, o simplemente por operaciones de TI), o a que el agente está en ejecución pero desconectado. La protección se mantiene durante los períodos sin conexión, pero las notificaciones al equipo de seguridad no ocurrirán hasta que el agente vuelva a estar en línea.
2. Existe un problema con el software de Cyber Crucible. Esto es muy, muy poco frecuente.

   Por favor, abra un ticket de soporte con Cyber Crucible de inmediato si esto ocurre.
3. La máquina está apagada. Este es el escenario más común. A continuación se analizan las mejores prácticas.

85688410.png?width=680

Mejores prácticas para la notificación offline

Una consideración importante para la notificación offline es que una máquina que ha sido apagada aparecerá como offline ante los servidores de Cyber Crucible. Las estaciones de trabajo, propensas a encenderse y apagarse durante las operaciones normales del negocio, generarían notificaciones offline durante los almuerzos, viajes entre ubicaciones o días festivos.

Las mejores prácticas para los grupos ya dividen los servidores de las estaciones de trabajo. Los servidores normalmente se benefician mejor de períodos de notificación offline más cortos, en caso de que exista un problema. Los grupos enfocados en estaciones de trabajo son más adecuados para períodos más largos de aparición offline.

Muchos clientes de Cyber Crucible consideran mejor crear notificaciones automatizadas solo para los grupos de servidores, y filtrar periódicamente uno de los campos de fecha en la página de Administrar Agentes por una fecha, como "Mostrar los agentes cuyo campo de Actualización de Datos de la Máquina no se haya actualizado en la última semana".

85688417.png?width=453

Agentes Que No Están Completamente Actualizados

Los agentes de Cyber Crucible requieren un reinicio para actualizarse. Puede encontrar una mayor comprensión de los algoritmos de actualización aquí. Cuando un agente reporta que un reinicio dará como resultado una actualización, la página de Agentes indica qué máquinas requieren una actualización y están listas para actualizarse al reiniciar. A veces, las máquinas que no se reinician con frecuencia (normalmente servidores) acumularán varias actualizaciones en espera antes de actualizarse realmente. Vemos un ejemplo de esto en la captura de pantalla. La hora del último reinicio también está disponible.

El informe ejecutivo semanal de Cyber Crucible identifica ese número de agentes que requieren una actualización, y cuántos de ellos están listos para actualizarse tan pronto como se reinicien. Las dos razones más comunes por las que una máquina requiere una actualización, pero no está lista/en espera, son:

1. La máquina ha estado desconectada, como en el caso de un empleado de vacaciones.
2. La máquina tuvo un fallo de hardware o software mayor/renovación, y Cyber Crucible en realidad ya no está en esa máquina.

Aparte de esos dos casos, las actualizaciones normalmente ocurren muy rápidamente, y sin la intervención del administrador más allá de las actividades normales de parcheo y reinicio.

85688423.png

¿Qué versiones de Windows son compatibles con Cyber Crucible?

Versión de escritorio	Versión de servidor	Compatibilidad
11 10 8.1 8	2025 2022 2019 2016 2012 R2 2012 R1	Totalmente compatible.
7	2008 R2	Debe estar parcheado para admitir la firma de código SHA-2.
Vista y anteriores	2008 R1 y anteriores	No compatible.

¿Cuáles son las tasas normales de consumo de recursos para RAM y CPU?

El uso típico de CPU es del 1% o menor (lo que se muestra como 0% en la mayoría de las herramientas de monitoreo, como el Administrador de tareas).

El uso típico de RAM es menor a 10 MB. La mayoría del uso en equipos de escritorio y servidores es de aproximadamente 5 MB.

También monitoreamos el uso de memoria del controlador en el espacio del kernel, para detectar cualquier problema.

¿Cómo puedo saber si Cyber Crucible se está ejecutando en el sistema?

Servicios

Abra el Administrador de tareas.

Haga clic en la pestaña Servicios.

Ordene por nombre si es necesario y desplácese hasta CyberCrucibleAgent/ Cyber Crucible Agent

image-20250811-181519.png

Controlador del núcleo

Abra un símbolo del sistema como Administrador.

Ejecute el comando que se observa en la siguiente captura de pantalla:

fltmc.exe | find “CCRRSecMon”

3047503.png?width=561
fltmc.exe muestra la lista de controladores cargados.

Es probable que haya varios, por lo que el comando find muestra únicamente el controlador de Cyber Crucible, denominado CCRRSecMon.

Si el controlador aparece en la lista, significa que está cargado y funcionando correctamente en el sistema operativo.

¿Cómo sé cuándo un agente ha terminado la autoconfiguración después de la instalación?

En la página Agents del panel de control, cada agente tiene varias marcas de tiempo que indican la última vez que recibió determinados tipos de información. Se considera que un agente ha terminado la autoconfiguración cuando, además de tener asignada una licencia válida, tiene registradas marcas de tiempo en las siguientes columnas:

- Last Validation Check
- Latest Schedules Download
- Latest Tailored Behaviors Download
- Latest Certificate Bundle Download

Además, si el grupo tiene

Proceso de Incorporación

Gestión de Grupos

Antes de instalar los agentes, los usuarios pueden prepararse configurando sus grupos. Siga las instrucciones de Gestión de Grupos aquí.

Configuración de Alertas de Seguridad del Agente

Los usuarios pueden configurar notificaciones por correo electrónico para eventos de seguridad, incluyendo actividades de ransomware, accesos anómalos de identidad y agentes fuera de línea. Las instrucciones se encuentran aquí.

Mejores Prácticas de Planificación de Instalación del Agente

Algunos entornos tienen un comportamiento y configuración similar de usuarios, aplicaciones y sistemas en toda su empresa. Otros tienen grupos especializados que se comportan de manera diferente, como un equipo de ventas frente a una división de ingenieros de software.

La implementación y configuración son tan rápidas que dedicar un par de minutos a planificar una instalación en un subconjunto de escritorios o servidores que comparten los mismos comportamientos empresariales o aplicaciones le permitirá evaluar si es necesario tener en cuenta alguna aplicación.

Además, es muy común que Cyber Crucible descubra software de gestión y VPN previamente desconocidos (y no autorizados), scripts de administrador no autorizados, software mal configurado, o incluso infecciones durante la implementación inicial.

Instalación del Agente

Cuando esté listo para instalar sus agentes, las instrucciones se encuentran aquí y aquí

Estrategias de Actualización para Grupos y Agentes

Para gestionar las estrategias de actualización para grupos y agentes, siga las instrucciones aquí.

Cómo Investigar la Causa Raíz de una Respuesta a Extorsión

La página de Respuesta a Extorsión se encuentra en la pestaña Operaciones de la barra lateral. Las instrucciones sobre cómo investigar la causa raíz de una alerta se encuentran aquí.

Comportamientos Personalizados

Las instrucciones para crear comportamientos personalizados se encuentran aquí.

Integración REST

Algunos usuarios pueden desear integrarse con nuestro servidor REST. La página de Integración REST con documentación se encuentra en nuestro sitio web en la pestaña Administración de la barra lateral.

Implementación en un Entorno Ya Infectado

Antecedentes

Las implementaciones de clientes de Cyber Crucible resultan rutinariamente en el descubrimiento de infecciones previamente desconocidas. Las redes normalmente no están libres de infecciones, incluso si las herramientas de defensa de ciberseguridad existentes han indicado que todo está en orden.

Un ataque de ransomware proporciona un punto de demarcación, o punto crucial, muy visible para que una empresa mida con qué frecuencia los hackers logran atacar nuevamente con éxito, y qué tan exitosos son.

- Los informes de fuentes abiertas y la inteligencia de amenazas revelan una tasa de reataque de clientes que no son de Cyber Crucible de alrededor del 80%.
- Cyber Crucible observó que alrededor del 10% de los endpoints tienen al menos un intento de robo de identidad, como contraseñas, claves o tokens, por período de 90 días.
- Cyber Crucible observa que los atacantes intentan recuperar un punto de apoyo en un entorno aproximadamente cada mes.

Desde el punto de vista de la respuesta a incidentes o forense, Cyber Crucible es una excelente herramienta para recuperar el control de la red. Especialmente en el caso de las víctimas de ataques, sospechamos que los atacantes mantienen visibilidad sobre el estado de recuperación y la salud financiera de las víctimas, para calcular mejor el momento de atacar de nuevo.

Qué Sucede Inmediatamente Después de la Instalación

Cyber Crucible comienza automáticamente a suspender los programas en ejecución que se observa que se comportan de manera maliciosa.

La implementación del producto Cyber Crucible puede resultar en la suspensión de múltiples programas en múltiples máquinas mientras se limpia el entorno.

En ocasiones, una implementación parcial de Cyber Crucible puede resultar en que el hacker intente recuperar el control a través de las máquinas que no tienen la protección de Cyber Crucible.

Por ejemplo, Cyber Crucible se instaló una vez solo en una parte de los escritorios de una víctima reciente de una filtración de datos. Los hackers intentaron desinstalar Cyber Crucible conectándose desde las máquinas no protegidas, y luego eventualmente comenzaron a apagar las máquinas protegidas.

¿Qué Sucede con el Malware Latente, en Espera de Futuras Tareas?

El malware que no está actuando en nombre de los atacantes, se activa después de que el malware comienza a acceder a los datos.

Repasemos un escenario:

Dos máquinas tienen malware en ellas. Llamémoslas Máquina A y Máquina B.

Ambas muestras de malware son actualmente indetectables por sus herramientas de seguridad favoritas.

El malware de la Máquina A no hace nada, sino que espera instrucciones. Cyber Crucible no detecta el malware. El malware tampoco es aún detectable por otras herramientas de seguridad.

El malware de la Máquina B está intentando acceder a datos o datos de identidad. Inmediatamente después de un ataque exitoso, los comportamientos más comunes que observamos de los atacantes al asignar tareas a su malware, son asegurarse de tener datos de identidad frescos, como contraseñas o tokens, y enumerar nuevos datos. Entonces, en parte, "obtener las nuevas contraseñas después de que los administradores restablecen las contraseñas", y, en parte, "mantenerse al tanto para buscar nuevos datos".

En la Máquina B, Cyber Crucible suspende inmediatamente la aplicación.

Después de un período que va de un mes a un año, el malware de la Máquina A es detectado una vez que suficientes víctimas han reportado el malware a las bases de datos de proveedores de seguridad. Cuanto más disciplinados sean los atacantes en la distribución de esa muestra, más tiempo pasará ese malware en particular sin ser detectado.

El malware de la Máquina B ha sido neutralizado, congelado en su lugar.

El malware de la Máquina A está atrapado. En el segundo (bueno, 100 milisegundos) en que intenta acceder a cualquier dato o información de identidad, el malware de la Máquina A es suspendido. El cliente está protegido, aunque el malware exista durante días, hasta años, sin ser detectado por otras herramientas.

Detalles Adicionales - Los Reinicios Pueden Ser Valiosos

Algunas de nuestras analíticas son más precisas cuando el ciclo de vida del proceso puede rastrearse desde el inicio de la aplicación hasta el estado presente.

Reiniciar una máquina después de la instalación puede ser ventajoso.

Los programas que ya se estaban ejecutando antes de la instalación no tendrán una inspección analítica completa por parte de Cyber Crucible. Reiniciar obliga a esos programas a reiniciarse, proporcionando así una inspección completa a todos los programas.

¿Cómo pruebo la conexión TLS a estos dominios?

Más allá de simplemente hacer ping a los dominios utilizados por Cyber Crucible para asegurarse de que su endpoint pueda alcanzar todas las direcciones de red correctas, el instalador del Agente de Cyber Crucible incluye un argumento de prueba que garantiza que se pueda establecer una conexión TLS/SSL válida en ambas direcciones con todos los servidores requeridos.

Untitled-20240410-185719.png
Simplemente agregue `--test-connection` a la ejecución del instalador, asegurándose de incluir aún los identificadores de grupo y los tokens de OAuth necesarios para realizar la autenticación. Se muestra arriba una captura de pantalla con la única modificación necesaria en el script .bat proporcionado, y un resultado exitoso.

Adjuntos:

▨ Untitled-20240410-185719.png (image/png)

¿Por qué podría necesitar un proxy?

Si bien toda la detección y protección conductual del agente de Cyber Crucible ocurre en el endpoint, sin necesidad de enviar muestras a la nube para su análisis, el agente del endpoint aún requiere una conexión a un servidor para recibir información de licencia, configuración, actualizaciones de software, etc.

Si su red está restringida hasta el punto de no permitir conexiones a los rangos de IP donde se alojan los servidores de Cyber Crucible, es posible que necesite configurar un proxy para permitir que el agente (únicamente) alcance su servidor para la instalación. Consulte How to Manage Proxy Configurations para obtener información sobre cómo configurar el agente.

¿Qué tipo de proxy puedo usar?

A partir de la versión 4.4.6.3 del agente de Cyber Crucible, las configuraciones de proxy admiten Socks5. No existe restricción sobre dónde se aloja el servidor (en las instalaciones o externamente), siempre que las restricciones de red permitan que los agentes lo alcancen. A continuación se muestra un diagrama de ejemplo de una configuración de proxy simple donde el servidor Socks5 está alojado dentro de la red restringida, y solo tiene permitido conectarse a una máquina externa que canaliza el tráfico.

SOCKS5H.png

Esta configuración permite que los agentes se conecten a sus servidores, manteniendo al mismo tiempo la política de red. Solo requiere 1 regla que permita al host Socks5 alcanzar su servidor proxy externo en un puerto (ssh). Esto asegura que no solo todo el tráfico va por el puerto 443, sino que además está doblemente envuelto en SSH antes de salir de la red, y no requiere reenvío de puertos entrantes (port-forwarding).

¿Cuánta información produce Cyber Crucible?

Los datos recopilados por el agente de Cyber Crucible pasan por múltiples capas de filtrado, con el fin de eliminar el ruido derivado de contar con demasiada telemetría en bruto. Los datos sin procesar producidos por los sensores del kernel se reducen [**Filtro n.º 1**] para disminuir tanto el uso de memoria del endpoint como el ancho de banda de red por agente. A continuación, la API REST asociará la telemetría en bruto de procesos/endpoints que reciba con respuestas automatizadas, de modo que el analista pueda optar por ver únicamente los datos relevantes [**Filtro n.º 2**].

Blank diagram-20240523-165941.png

Como se observa en la figura anterior, los endpoints de estaciones de trabajo de un cliente promedio pueden producir varios gigabytes de datos de sensores sin procesar durante un período de 24 horas, mientras que solo unos pocos megabytes de esos datos serán relevantes para una alerta del SOC si se intenta un ataque.

¿Cómo desinstalo varios agentes a la vez?

Desinstalar varios agentes a la vez es sencillo.

Diríjase a la página de Agentes.

Recomendamos utilizar filtros, como el nombre de la máquina, el grupo, la dirección IP o los filtros de versión, para mostrar en pantalla la mayor cantidad de agentes posible. Esto es especialmente útil para usuarios con cientos o miles de agentes en un grupo.

85983282.png?width=680
Aquí, utilizamos la tecla Shift mientras hacíamos clic en 3 filas, para seleccionar tres agentes.

La opción Desinstalar todos los agentes seleccionados se encuentra en la parte superior izquierda, encima de la cuadrícula.

Una vez que se verifican los permisos en el servidor, y se confirma que usted tiene permiso en los grupos de los agentes, se emitirán los comandos de desinstalación.

Los agentes reciben un comando de desinstalación firmado digitalmente. La firma es utilizada por los agentes para validar que el comando realmente proviene de Cyber Crucible, y no de un delincuente que intenta eliminar su software de protección.

Una vez que los agentes validan el comando, prepararán el sistema para la desinstalación al reiniciarse.

La columna Atención mostrará la entrada “Desinstalación en curso” y mostrará un botón Cancelar desinstalación en la celda.

Una vez que se reinicia la máquina, el agente valida que la desinstalación se está llevando a cabo y elimina todos los archivos.

Es importante señalar que el agente confirmará “un último saludo” antes de desinstalarse por completo, por lo que a veces los agentes estarán presentes durante un breve período después del reinicio. Esto se debe a que algunos entornos de red no funcionan correctamente durante hasta 30 segundos después de que el escritorio es visible. Tenga en cuenta que, una vez finalizadas las desinstalaciones, las licencias se eliminan automáticamente de los agentes.

¿Cómo desinstalo un solo agente?

Vaya a la página de Agentes.

Localice el agente deseado y haga clic en el icono de la papelera en la columna Nombre del Agente:

86081562.png?width=680

Comprobación de si el software de Cyber Crucible está "Funcionando"

Introducción

Cyber Crucible está diseñado para funcionar sin interrumpir a los usuarios finales o empleados, mientras notifica discretamente a los usuarios elegidos del Dashboard (normalmente miembros elegidos de los equipos de TI y Seguridad) sobre las respuestas automatizadas.

Muchos de los simuladores de ransomware o malware no capturan con precisión el comportamiento de un hacker. Aunque esto causa problemas para herramientas como Cyber Crucible que (correctamente) identifican la simulación como un falso positivo, eso no es necesariamente algo malo.

Algunos proveedores realmente construyen sus motores de detección en torno a estos simuladores para parte de su funcionalidad de detección, para asegurarse de que las pruebas de cualquier cliente se superen con éxito.

Las acciones de malware reales, como el cifrado por ransomware, corren el riesgo de cifrar o corromper datos de forma irrecuperable. En Cyber Crucible, incluso hemos visto que el ransomware activa en secreto otro malware en la red, o realiza otras acciones que podrían perjudicar a la empresa que intenta probar Cyber Crucible.

Por lo tanto, no querrá usar malware, ni tampoco querrá usar un simulador tan preciso que pueda dañar accidentalmente sus datos.

Probando Cyber Crucible

Existe una forma sencilla de probar Cyber Crucible sin usar malware ni una simulación tan realista que ponga en riesgo sus datos o los de su empresa.

Cyber Crucible evalúa los accesos a identidades digitales en cada milisegundo del día. Muchas de esas identidades digitales se almacenan en los navegadores, razón por la cual los atacantes colocan los navegadores web en el primer lugar de su lista de objetivos automatizados.

El análisis de comportamiento de acceso a identidades de Cyber Crucible dará lugar a una de tres respuestas:

1. No hacer nada
2. Ocultar los datos
    1. aplicación legítima conocida que supera todas las comprobaciones de memoria y kernel, pero que no necesita acceso a esos datos de identidad en particular - ejemplo: Windows Explorer sin explotar
3. Suspender el proceso
    1. aplicación legítima conocida que debería tener acceso a los datos de identidad pero que ha sido hackeada, o
    2. una aplicación extraña

A continuación se muestran dos ubicaciones comunes para los usuarios de Windows:

En este caso, el nombre de usuario de Windows es "denni", y estas son las ubicaciones donde se almacenan los datos de sesión. Es posible que le funcione la variable %LOCALAPPDATA% si no desea averiguar el nombre de usuario.

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
    - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

La vista sin Cyber Crucible instalado

Veamos primero cómo se ve una de estas carpetas con Explorer.exe, sin Cyber Crucible instalado.

Screenshot 2025-05-14 103339.png
Aquí vemos múltiples sesiones de Chrome bajo el perfil "predeterminado" de Google Chrome.

Esta información normalmente contiene información sensible que un atacante querría usar para secuestrar sesiones con programas importantes como portales de administración de TI, banca, correo electrónico, o herramientas de almacenamiento como Google Drive o Dropbox.

La vista con Cyber Crucible instalado

Después de instalar Cyber Crucible, se puede realizar una prueba rápida, sin usar malware ni ningún tipo de técnica criminal o uso indebido del equipo de TI.

En este caso, se utiliza la misma ubicación de almacenamiento de sesión del navegador:

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions

    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
    - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

Screenshot 2025-05-14 103620.png
Cyber Crucible, inmediatamente después de la instalación, ya está bloqueando el acceso a los datos en esa carpeta.

Tenga en cuenta que este es exactamente el mismo proceso de Explorer que ya estaba en ejecución al momento de la instalación, por lo que al programa en ejecución de repente se le ha revocado el acceso en la capa del "disco duro" o kernel. Incluso los programas, benignos, explotados o de tipo malware que ya están en ejecución son evaluados correctamente por Cyber Crucible.

Cómo ver su prueba en el Dashboard de Cyber Crucible

Hay una gran cantidad de accesos a datos de identidad en un sistema en ejecución, en todo momento.

El software como servicio y los programas basados en la nube han dado lugar a que muchos sitios web y aplicaciones tengan una funcionalidad limitada en el propio sitio web, mientras que el navegador (o el navegador integrado en el caso de las aplicaciones) se comunica constantemente con servidores de datos para completar hojas de cálculo, tablas, gráficos y contenido de redes sociales.

Página de Acceso a Identidad

Los accesos a identidad que se consideran apropiados para que Cyber Crucible suspenda la aplicación infractora se enumeran en la página de Acceso a Identidad.

Estas son situaciones en las que el programa que accede a los datos de identidad debe detenerse, no simplemente ocultar los datos.

En este caso, Explorer no fue detenido después de la multitud de comprobaciones que realizó Cyber Crucible. En su lugar, los datos simplemente fueron ocultados.

Screenshot 2025-05-14 103741.png
Por lo tanto, no hay violaciones de acceso a identidad enumeradas aquí.

Página de Ocultación de Acceso a Identidad

Cyber Crucible tiene opcionalmente la capacidad de mostrar a los clientes del Dashboard las situaciones en las que se ocultaron datos de identidad, pero en las que el programa que accedía no fue detenido.

Explorer no fue explotado ni fue malicioso de ninguna otra forma en esta prueba, simplemente estaba accediendo a datos de identidad muy privilegiados de los navegadores Chrome y Edge.

La mayoría de los usuarios no tienen acceso a esta información dada la carga adicional en las máquinas y redes de los clientes al transmitir esos datos a los servidores de Cyber Crucible.

Por favor, pregunte si desea acceso, pero tenga en cuenta que la actividad que está viendo no es actividad maliciosa, sino comportamientos de privacidad de datos de identidad que Cyber Crucible realiza desde una perspectiva de GRC, o de cumplimiento de políticas.

Identity Hide Explorer.mp4
Aquí, vemos en este breve video, que Explorer fue bloqueado para ver los datos de sesión del navegador, aunque el propio Explorer no fue interrumpido.

Cómo Gestionar las Configuraciones de Proxy

Tenga en cuenta que solo los agentes en la versión 4.4.6.3 y superiores tienen esta capacidad

Dónde Encontrar la Configuración de Proxy Actual de un Grupo

Los usuarios pueden ver la configuración actual del servidor proxy de un grupo para los agentes de este grupo a seguir, navegando primero a la página de Grupos que se encuentra en la pestaña de Administración en la barra lateral.

La configuración actual del servidor proxy de un grupo se puede encontrar en la columna "Proxy Server Config" en la cuadrícula.

Si el grupo no tiene una configuración de servidor proxy habilitada, se mostrará el texto "Do Not Use Proxy".

Proxy Server Config Column.png
Si el grupo tiene una configuración de servidor proxy habilitada, se mostrará la URL de la configuración de proxy actual

Proxy Server Config Enabled.png

Cómo Actualizar un Grupo para Habilitar un Servidor Proxy

Los usuarios pueden habilitar a los agentes de un grupo para que usen un servidor proxy haciendo clic primero en el ícono de gestionar configuraciones de proxy en la columna "Proxy Server Config" en la página de Grupos. Al hacer clic en este ícono aparecerá una ventana modal donde los usuarios pueden gestionar las configuraciones del servidor proxy para el grupo.

Manage Proxy Server Config Icon.png
El modal de Gestión de Configuración del Servidor Proxy que aparece se usa para ver y gestionar las configuraciones del servidor proxy del grupo. Los usuarios pueden guardar múltiples configuraciones dentro de un grupo, y todas las configuraciones guardadas se muestran en la cuadrícula de este modal. Tenga en cuenta que todas las configuraciones de servidor proxy guardadas para un grupo también aparecerán en el modal de Descargar Agente.

Para seleccionar una configuración de servidor proxy para el grupo, la configuración primero debe enviarse en el Formulario de Nueva Configuración de Proxy. Este formulario está oculto de forma predeterminada; haga clic en el interruptor para mostrarlo.

Manage Proxy Server Configs Modal.pngNew Proxy Configuration Form.png
Después de enviar el formulario de nueva configuración, se mostrará debajo en la cuadrícula del modal.

Para seleccionar una configuración de proxy que usarán los agentes de este grupo, primero seleccione la configuración deseada y luego haga clic en el ícono de editar encima de la cuadrícula.

Select Config for Group.png
Después de hacer clic en el ícono de editar para la configuración de proxy deseada, la configuración actual del servidor proxy del grupo ahora está actualizada y se puede ver en este modal y en la columna "Proxy Server Config". Los agentes de este grupo ahora usarán la configuración de proxy actualizada del grupo. Tenga en cuenta que si un agente recibe instrucciones de cambiar a un servidor proxy inaccesible, no cambiará hasta que ese servidor sea accesible.

Mange Proxy Server Config Modal Setting Enabled.pngGroup Proxy Config Enabled.png

Cómo Actualizar un Grupo para No Usar un Proxy

Si un grupo tiene un servidor proxy habilitado para que lo usen los agentes de este grupo y los usuarios desean actualizar el grupo para que los agentes de este grupo no usen un proxy, primero

navegue a la página de Grupos y localice el grupo deseado en la cuadrícula.

Luego haga clic en el ícono de gestionar configuraciones de proxy en la columna "Proxy Server Config". Al hacer clic en este ícono aparecerá el modal de Gestión de Configuración del Servidor Proxy.

Proxy Server Config Column 2.png
En este modal, haga clic en el ícono de x para actualizar a los agentes de este grupo para que no usen un servidor proxy y se conecten a nuestros servidores normalmente. Tenga en cuenta que la configuración de proxy actual no se eliminará de las configuraciones de proxy guardadas del grupo; este es un paso separado que se explica en la sección a continuación.

Do Not Use Proxy Icon.png
Después de hacer clic en el ícono de x, el modal se actualizará para reflejar este cambio y la columna "Proxy Server Config" para este grupo ahora mostrará "Do Not Use Proxy".

No Current Proxy Config Selected .pngDo Not Use Proxy Cell.png

Cómo Eliminar una Configuración de Proxy Guardada en un Grupo

Para eliminar una configuración de proxy guardada de un grupo, primero navegue a la página de Grupos y localice el grupo deseado en la cuadrícula.

Luego haga clic en el ícono de gestionar configuraciones de proxy en la columna "Proxy Server Config". Al hacer clic en este ícono aparecerá el modal de Gestión de Configuración del Servidor Proxy.

Manage Proxy Server Config Icon.png
En este modal, haga clic en la configuración de proxy guardada deseada para eliminar para este grupo, luego haga clic en el ícono de papelera. Después de hacer clic en este ícono, la configuración de proxy seleccionada ya no aparecerá en la cuadrícula como una configuración de proxy guardada para el grupo.

Remove Saved Config.png
Tenga en cuenta que si elimina una configuración de proxy guardada para un grupo y esta configuración está establecida como la configuración de servidor proxy actual para el grupo, esto también actualizará la configuración de servidor proxy actual del grupo para que no use un proxy.

Cómo Instalar un Agente Usando un Proxy

Primero, navegue a la página de Agentes que se encuentra en la pestaña de Operaciones en la barra lateral. Luego haga clic en el botón Descargar Agente. Al hacer clic en este botón aparecerá el modal de Descargar Agente.

Download Agent Button.png
En este modal, si selecciona un grupo que tiene configuraciones de proxy guardadas, aparecerá la opción Seleccionar Configuración de Proxy para el Instalador con la configuración actual del grupo seleccionada como valor predeterminado. Todas las configuraciones de proxy guardadas del grupo también aparecerán como opciones, incluida una opción de No Usar Proxy.

Download Agent Modal.pngDownload Agent Modal Proxy Config Options.png
Al optar por usar un proxy para el instalador, el único tipo de instalador posible es el Instalador de Línea de Comandos.

Si selecciona la opción No Usar Proxy, aparecerán nuestras opciones normales de tipo de instalador.

Download Agent Modal Do Not Use Proxy.png
Tenga en cuenta que si selecciona una configuración de proxy para el instalador que no es la configuración actual del grupo, el instalador se ejecutará con la configuración seleccionada y luego cambiará a la configuración de proxy actual del grupo después de instalar.

¿Dónde Puedo Ver si un Agente Puede Omitir el Proxy?

Los usuarios pueden ver si los agentes pueden conectarse a nuestros servidores sin usar un proxy navegando primero a la página de Agentes que se encuentra en la pestaña de Operaciones en la barra lateral. Luego localice la columna Agent is Able to Bypass Proxy en la cuadrícula.

Tenga en cuenta que la columna Agent is Able to Bypass Proxy no será visible a menos que el usuario sea miembro de un grupo que ha habilitado a los agentes del grupo para usar un proxy.

Si el agente está en un grupo que ha habilitado el uso de un proxy y el agente no puede omitir el proxy para conectarse a nuestros servidores, se mostrará la x roja en la columna. Vea un ejemplo de esto a continuación:

Agent Cannot Bypass Proxy.png

Si el agente está en un grupo que ha habilitado el uso de un proxy y el agente puede omitir el proxy y conectarse a nuestros servidores normalmente, se mostrará la marca de verificación verde en la columna. Vea un ejemplo de esto a continuación:

Agent Can Bypass Proxy.png