Cómo instalar Cyber Crucible

Cortafuegos que bloquean el acceso de la autoridad de certificación CRL/OCSP (modo DMZ)

Cómo instalar Cyber Crucible

La instalación de Cyber Crucible es sencilla. Inicie sesión en la aplicación web en https://dashboard.cybercrucible.com

Vaya a la página de Agentes y haga clic en el botón Descargar Agente.

85131265.png?width=680
Después de hacer clic en el botón, aparece el siguiente cuadro modal:

85229569.png?width=340
Seleccione el grupo en el que desea que aparezcan inicialmente los agentes que está instalando.

Si el grupo no aparece en la lista, deberá crear el grupo o pedirle al administrador del grupo que lo agregue al grupo existente.

Después de la instalación, siempre puede cambiar el grupo en el que se encuentra un agente, o de varios agentes a la vez. Por lo general, es más sencillo configurar la pertenencia al grupo antes de la implementación masiva, que organizar los agentes después de que se instalen.

Permisos requeridos

Se requiere acceso administrativo a un equipo para instalar y cargar el servicio y el controlador de Cyber Crucible.

La instalación mediante script descarga específicamente el instalador y lo configura en la ubicación predeterminada C:\. El script debe ejecutarse como un usuario o rol que tenga permiso para la ubicación de descarga y ejecución.

Por lo tanto, se necesita un usuario con permiso para usar C:\ durante la instalación, o el script (detallado a continuación) debe ajustarse para descargar y ejecutarse en una ubicación diferente.

Instalación mediante interfaz gráfica (GUI)

Este método de instalación permite al usuario configurar e instalar manualmente una instalación.

Este método de instalación requiere que un usuario con permisos para instalar en el grupo especificado pueda iniciar sesión.

Se utiliza mejor para 1 o 2 instalaciones, por un solo usuario.

Instalación mediante script

Este es, con diferencia, el método de instalación más común.

Con este método, la aplicación web de Cyber Crucible configura automáticamente el proceso de instalación y el arranque seguro del agente hacia la aplicación web.

Se utiliza un archivo por lotes (batch) de Windows. Si bien existen otros métodos de instalación más complejos posibles, este método tiene la mayor compatibilidad con las herramientas de Gestión Remota.

El archivo por lotes se puede ejecutar como un usuario con los permisos adecuados (generalmente administrador), o se puede copiar y pegar en su herramienta de implementación automática preferida.

A continuación se presenta un análisis técnico del contenido del archivo por lotes, el cual puede configurarse según sus necesidades.

Análisis detallado del script de instalación

El identificador de grupo seleccionado durante la creación del script se ingresa en el script, al igual que el token de oAuth requerido para que los agentes se unan al grupo específico.

47480849.png?width=680
Tenga en cuenta que este token de autenticación oAuth no está asociado con la aplicación web ni con ningún usuario. No se puede utilizar para realizar llamadas REST a la API de la aplicación web.

En algunos entornos, los permisos pueden obtenerse automáticamente. Esto ocurre típicamente en circunstancias en las que un usuario ejecuta el script de instalación haciendo clic en él, en lugar de un acceso programático. En entornos empresariales o herramientas de implementación automatizada, es probable que no se ejecute de esta manera.

47480857.png?width=680
En esta siguiente sección del script, se puede personalizar la ubicación del archivo desde la cual se puede descargar y ejecutar el instalador.

Se recomienda encarecidamente que esta ubicación sea local a la máquina en la que se está instalando la herramienta. Si varias máquinas descargan instaladores en la misma ubicación, se producirán fallos y sobrescrituras.

Tenga en cuenta que el reinicio automático mediante el script de instalación no se utiliza de forma predeterminada. Esto se debe a que el reinicio automático en este script carece de la capacidad de gestión para programar instalaciones en un momento específico, de métodos de apagado limpio que verifiquen si el usuario tiene actualmente una sesión iniciada o aplicaciones en ejecución, o de dar aviso al usuario sobre un reinicio inminente.

47513621.png?width=680
Esta siguiente sección realiza la descarga y el nombramiento personalizado del instalador en el equipo. Tenga en cuenta que la fecha y la hora se utilizan para proporcionar unicidad al archivo de instalación, en caso de que se descargue varias veces con diferentes configuraciones o versiones.

Bitsadmin es una utilidad de Windows que intenta descargar archivos sin afectar negativamente al equipo si el sistema operativo está actualmente bajo una carga elevada.

47448109.png?width=680
En algunos entornos, el protocolo Bits está deshabilitado. Además, Bits puede estar en un estado no operativo debido a un error de Windows. En caso de que la descarga mediante Bits falle, la siguiente sección utiliza un método alternativo (.net JSC) para descargar el archivo del instalador. Este código solo se ejecuta si el descargador de Bits anterior falló.

47415316.png?width=680
Después de que se descarga el instalador, esta sección final del script ejecuta el instalador. Tenga en cuenta que la personalización de los argumentos de línea de comandos debe probarse, para garantizar que la configuración y las protecciones de installer.exe se ajusten a los argumentos de línea de comandos proporcionados aquí.

Por favor, abra un ticket de soporte si se requieren configuraciones adicionales, o para entornos avanzados como configuraciones de intermediario SSL (man in the middle).

47480877.png?width=680
Tenga en cuenta que no se requiere reinicio, y su ejecución está comentada (deshabilitada). En raras ocasiones, más comúnmente en versiones antiguas de Windows, los controladores no se registraban ni se cargaban en el sistema operativo a pesar de que el instalador así lo indicara. En esos escenarios, el método más sencillo para garantizar que el controlador esté cargado es exportar los agentes a un documento de Excel y buscar los nombres de equipos faltantes en su lista de activos. Si todas las instalaciones están en un grupo nuevo, también se puede utilizar el recuento de agentes.

47480889.png?width=680
Esta sección al final del script de instalación es la función utilizada para descargar el instalador mediante JSC si es necesario. Solo se ejecuta si se recurre a .net JSC para descargar el instalador, como en el caso de que Bits falle.

47480895.png?width=680

¿Cómo localizo los registros de instalación?

Los instaladores de CLI sin interfaz gráfica (headless) generan su estado y registros tanto en `stdout` como en un archivo de registro, ubicado en el directorio local del ejecutable del instalador. De forma predeterminada, al utilizar un script preempaquetado, como los scripts ps1 o bat descargados desde https://dashboard.cybercrucible.com, el archivo de registro se ubicará en la raíz de la unidad C:.

Los archivos de registro de instalación se denominan `cc_installer.log`

Los instaladores con interfaz gráfica (GUI) no generan los mismos archivos de registro, ya que no son headless, y todos los registros se muestran en la sección de texto desplazable de la ventana de la GUI.

Forzar el envío del instalador al dominio de AD

En algunos entornos frágiles, particularmente si se está recuperando de un ataque o una interrupción reciente, es posible que las implementaciones normales de RMM y/o SCCM no sean una opción. Aquí encontrará un script que puede servir como plantilla de cómo podría forzar la instalación de CC en un entorno de active directory.

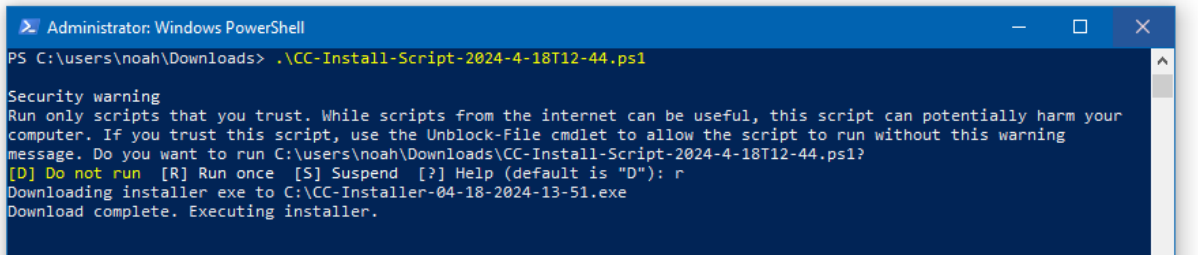
Nota: Es probable que este script deba adaptarse a su caso de uso, y requiere credenciales de dominio para ejecutarse. Se espera que este script se ejecute directamente en un controlador de dominio (primario).

Pasos a seguir

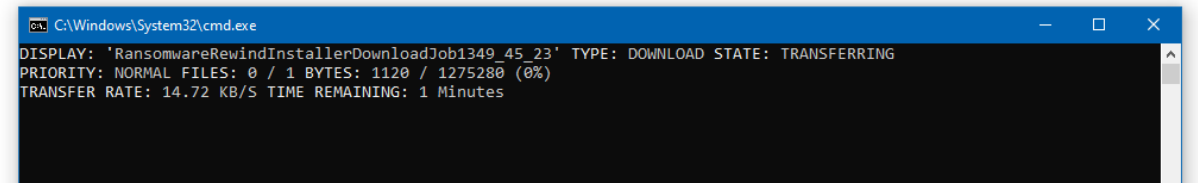
1. Actualice la variable `$install_targets` con una lista de nombres de máquinas (nombres NETBIOS o similares)
2. Descargue un script de instalación ps1 'normal' desde el panel de Cyber Crucible
3. Actualice las variables en el script push_installer_ad.ps1 para que coincidan con las variables específicas de su grupo del script del panel
    1. `${GroupId}`
    2. `${ClientAuth}`
    3. cualquier variable `--rest-pub-key`
4. Descargue un ejecutable de CLI nativo desde el panel de Cyber Crucible
    1. Coloque el CLI en un recurso compartido de red, o en algún lugar accesible para todas las máquinas que se van a instalar
        1. Esto evita que cada máquina tenga que perder tiempo y ancho de banda volviendo a descargar el mismo exe
        2. El mismo exe puede ejecutarse en diferentes sistemas operativos, ya que el instalador descargará los archivos de servicio/controlador/instalación relevantes para el sistema operativo y el rol detectados de la máquina.
    2. Configure `${OutputFilePath}` con la ruta del CLI en un recurso compartido de red
5. Posiblemente elimine la verificación en línea de ICMP (si no es necesaria / no es válida para su entorno)
6. Ejecute el script con `-credential`
    1. por ejemplo, `./push_installer_ad.ps1 -credential ad1\kyle`

Descripción General del Script de Instalación

1. El instalador más reciente se descarga desde `https://installerfiles.rpp.cybercrucible.com/installers/64/installer-cli.exe`
    1. Los scripts de instalación de PowerShell (PS1) utilizarán una instancia de WebClient.



    2. Los scripts de instalación por lotes (BAT) utilizarán BitsAdmin, o JScript si BitsAdmin falla.



2. Se ejecuta el instalador y se le pasa el ID de grupo y la autenticación de cliente proporcionados en su script.
    1. Opcionalmente, agregue `--reuse-agent-by-machine-name` a la ejecución del exe, para que el instalador reutilice el objeto de agente y la licencia de un agente previamente instalado con el mismo nombre netbios.
3. El instalador verifica las condiciones de instalación requeridas
    1. Ejecutarse con privilegios de Administrador.
    2. La máquina ejecuta una versión compatible de Windows.
    3. No hay otro instalador ya en ejecución.
    4. El agente no está instalado previamente.
4. El instalador verifica que la máquina pueda comunicarse con los servidores requeridos.
    1. Amazon oAuth 2.0 en `ransomwarerewind-agents.auth.us-west-2.amazoncognito.com`
    2. El backend de Cyber Crucible en `agent.tasking.rpp.cybercrucible.com`
5. Los archivos del agente se descargan desde `installerfiles.rpp.cybercrucible.com` a través de HTTPS.
6. El agente se instala e inicia.

Instalación con SCCM

Instalar Cyber Crucible con SCCM no es diferente de cualquier otro paquete de software. Los puntos clave para la implementación mediante SCCM son:

1. Implemente con el script PS1 previamente creado, descargado desde https://dashboard.cybercrucible.com
2. Busque el servicio **Cyber Crucible Agent** en ejecución, o existente en el disco, como método de detección. La ubicación predeterminada del servicio del agente es **C:\Program Files\CyberCrucible\service.exe**
    1. Opcionalmente, también puede buscar la existencia de la clave de registro **HKLM\Software\CyberCrucibleAgent**, pero tenga en cuenta que, después de una desinstalación, esta clave puede seguir presente.

Pasos de configuración predeterminados

1. Cree una Aplicación, **no** un paquete
2. Especifique la configuración manualmente

image-20250807-175116.png

3. Configure el nombre de la aplicación, el nombre del proveedor, la descripción, etc.
4. Configure el Tipo de implementación y especifique **Script Installer**

image-20250807-175303.pngimage-20250807-175332.png

5. Especifique la ubicación del script, probablemente un recurso compartido de red, por ejemplo, **\\cc-dc01\share**
6. Especifique el programa de instalación para ejecutar el archivo ps1 proporcionado, por ejemplo, `Powershell.exe -file “CC-Install-Script-2025-8-7T13-55.ps1`
    1. Observe la marca de fecha en el nombre del script y cámbiela por la suya
    2. No se recomienda anular las políticas de PowerShell, pero según su configuración, es posible que deba especificar `-executionpolicy Bypass` o similar
7. Agregue un método de detección haciendo clic en “Add Clause”
    1. Consulte los métodos de detección recomendados en la parte superior de esta página
8. Especifique la configuración de implementación de UX
    1. Dado que la implementación de Cyber Crucible no requiere reinicio, los requisitos de instalación y de inicio de sesión quedan a criterio de su organización

image-20250807-175906.png

9. Seleccione Siguiente / Finalizar hasta que pueda cerrar el asistente.