Wie man Cyber Crucible installiert

Firewalls blockieren den Zugriff auf CRL/OCSP-Zertifizierungsstellen (DMZ-Modus)

Wie installiert man Cyber Crucible

BODY:

Die Installation von Cyber Crucible ist unkompliziert. Melden Sie sich bei der Webanwendung unter https://dashboard.cybercrucible.com an

Gehen Sie zur Seite „Agents“ und klicken Sie auf die Schaltfläche „Agent herunterladen“.

85131265.png?width=680
Nachdem Sie auf die Schaltfläche geklickt haben, erscheint das folgende Modal:

85229569.png?width=340
Wählen Sie die Gruppe aus, in der die zu installierenden Agent(en) zunächst erscheinen sollen.

Wenn die Gruppe nicht in der Liste angezeigt wird, müssen Sie entweder die Gruppe erstellen oder den Gruppenadministrator bitten, Sie der vorhandenen Gruppe hinzuzufügen.

Nach der Installation können Sie jederzeit die Gruppe ändern, in der sich ein Agent befindet, oder mehrere Agents gleichzeitig. Es ist in der Regel einfacher, die Gruppenzugehörigkeit vor der Massenbereitstellung zu konfigurieren, als die Agents nach der Installation zu organisieren.

Erforderliche Berechtigungen

Für die Installation und das Laden des Cyber Crucible-Dienstes und -Treibers ist administrativer Zugriff auf einen Rechner erforderlich.

Die Skriptinstallation lädt den Installer speziell herunter und konfiguriert ihn im Standardverzeichnis C:\. Das Skript muss als Benutzer oder mit einer Rolle ausgeführt werden, die über die Berechtigung für den Download- und Ausführungsort verfügt.

Daher wird entweder ein Benutzer mit Berechtigung zur Nutzung von C:\ während der Installation benötigt, oder das Skript (nachfolgend beschrieben) muss angepasst werden, um an einem anderen Speicherort herunterzuladen und auszuführen.

GUI-Installation

Diese Installationsmethode ermöglicht es dem Benutzer, eine Installation manuell zu konfigurieren und durchzuführen.

Diese Installationsmethode erfordert einen Benutzer mit Berechtigungen zur Installation in der angegebenen Gruppe, der sich anmelden kann.

Sie eignet sich am besten für 1 oder 2 Installationen durch einen einzelnen Benutzer.

Skriptinstallation

Dies ist mit Abstand die gebräuchlichste Installationsmethode.

Bei dieser Methode konfiguriert die Cyber Crucible-Webanwendung automatisch den Installationsprozess sowie das sichere Bootstrapping des Agents zur Webanwendung.

Es wird eine Windows-Batchdatei verwendet. Es gibt zwar auch andere, komplexere Installationsmethoden, doch diese Methode bietet die breiteste Kompatibilität mit Remote-Management-Tools.

Die Batchdatei kann von einem Benutzer mit den entsprechenden Berechtigungen (in der Regel Administrator) ausgeführt oder in Ihr bevorzugtes automatisches Bereitstellungstool kopiert und eingefügt werden.

Nachfolgend finden Sie eine technische Untersuchung des Inhalts der Batchdatei, die an Ihre Anforderungen angepasst werden kann.

Detaillierte Untersuchung des Installationsskripts

Die während der Skripterstellung ausgewählte Gruppenkennung wird in das Skript eingetragen, ebenso wie das oAuth-Token, das Agents zum Beitritt zur jeweiligen Gruppe benötigen.

47480849.png?width=680
Bitte beachten Sie, dass dieses oAuth-Authentifizierungstoken weder mit der Webanwendung noch mit einem Benutzer verknüpft ist. Es kann nicht verwendet werden, um REST-Aufrufe an die API der Webanwendung durchzuführen.

In manchen Umgebungen werden Berechtigungen automatisch erlangt. Dies ist typischerweise dann der Fall, wenn ein Benutzer das Installationsskript durch Anklicken ausführt, im Gegensatz zum programmatischen Zugriff. In Unternehmensumgebungen oder bei automatisierten Bereitstellungstools wird dies wahrscheinlich nicht ausgeführt.

47480857.png?width=680

An dieser nächsten Stelle im Skript kann der Speicherort, von dem der Installer heruntergeladen und ausgeführt werden kann, angepasst werden.

Es wird dringend empfohlen, diesen Speicherort lokal auf dem Rechner zu belassen, auf dem das Tool installiert wird. Wenn mehrere Rechner Installer an denselben Speicherort herunterladen, kommt es zu Fehlern und Überschreibungen.

Bitte beachten Sie, dass der automatische Neustart über das Installationsskript standardmäßig nicht verwendet wird. Dies liegt daran, dass der automatisierte Neustart in diesem Skript keine Verwaltungsfunktionen zur Planung von Installationen zu einem bestimmten Zeitpunkt, keine sauberen Herunterfahrmethoden zur Prüfung, ob der Benutzer aktuell angemeldet ist oder Anwendungen ausführt, sowie keine Warnung des Benutzers vor einem bevorstehenden Neustart bietet.

47513621.png?width=680
Dieser nächste Abschnitt führt den Download und die benutzerdefinierte Benennung des Installers auf dem Rechner durch. Bitte beachten Sie, dass Datum und Uhrzeit verwendet werden, um der Installationsdatei Eindeutigkeit zu verleihen, falls sie mehrmals mit unterschiedlichen Einstellungen oder Versionen heruntergeladen wird.

Bitsadmin ist ein Windows-Dienstprogramm, das versucht, Dateien herunterzuladen, ohne den Rechner negativ zu beeinträchtigen, falls das Betriebssystem gerade stark ausgelastet ist.

47448109.png?width=680
In manchen Umgebungen ist das Bits-Protokoll deaktiviert. Zudem kann sich Bits aufgrund eines Windows-Fehlers in einem nicht funktionsfähigen Zustand befinden. Falls der Download über Bits fehlschlägt, verwendet der nächste Abschnitt eine alternative Methode (.NET JSC) zum Herunterladen der Installer-Datei. Dieser Code wird nur ausgeführt, wenn der vorherige Bits-Downloader fehlgeschlagen ist.

47415316.png?width=680
Nachdem der Installer heruntergeladen wurde, führt dieser letzte Abschnitt des Skripts den Installer aus. Bitte beachten Sie, dass die Anpassung der Befehlszeilenargumente getestet werden sollte, um sicherzustellen, dass die Einstellungen und Schutzmechanismen von installer.exe mit den hier angegebenen Befehlszeilenargumenten übereinstimmen.

Bitte eröffnen Sie ein Support-Ticket, wenn zusätzliche Einstellungen erforderlich sind oder für erweiterte Umgebungen wie SSL-Man-in-the-Middle-Einstellungen.

47480877.png?width=680
Bitte beachten Sie, dass ein Neustart nicht erforderlich ist und in der Ausführung auskommentiert wurde. In seltenen Fällen, häufiger bei älteren Windows-Versionen, wurden Treiber trotz entsprechender Anweisung durch den Installer nicht im Betriebssystem registriert und geladen. In solchen Fällen ist die einfachste Methode zur Sicherstellung, dass der Treiber geladen ist, die Agents in ein Excel-Dokument zu exportieren und nach fehlenden Rechnernamen aus Ihrer Asset-Liste zu suchen. Wenn sich alle Installationen in einer neuen Gruppe befinden, können auch die Agent-Anzahlen herangezogen werden.

47480889.png?width=680
Dieser Abschnitt am Ende des Installationsskripts ist die Funktion, die zum Herunterladen des Installers mittels JSC verwendet wird, falls erforderlich. Er wird nur ausgeführt, wenn .NET JSC zum Herunterladen des Installers genutzt wird, etwa wenn Bits fehlschlägt.

47480895.png?width=680

Wie finde ich Installationsprotokolle?

Headless-CLI-Installationsprogramme geben ihren Status und ihre Protokolle sowohl an `stdout` als auch an eine Protokolldatei aus, die sich im lokalen Verzeichnis der Installer-exe befindet. Bei Verwendung eines vorgefertigten Skripts, wie z. B. der von https://dashboard.cybercrucible.com heruntergeladenen ps1- oder bat-Skripte, befindet sich die Protokolldatei standardmäßig im Stammverzeichnis des Laufwerks C:.

Die Installationsprotokolldateien werden `cc_installer.log` genannt.

GUI-Installationsprogramme erzeugen nicht dieselben Protokolldateien, da sie nicht headless sind und alle Protokolle im scrollbaren Textbereich des GUI-Fensters angezeigt werden.

Installer erzwungen an AD-Domäne verteilen

In manchen instabilen Umgebungen, insbesondere bei der Wiederherstellung nach einem kürzlichen Angriff oder Ausfall, sind normale RMM- und/oder SCCM-Bereitstellungen möglicherweise keine Option. Hier finden Sie ein Skript, das als Vorlage dienen kann, wie Sie eine CC-Installation erzwungen über eine Active-Directory-Umgebung verteilen können.

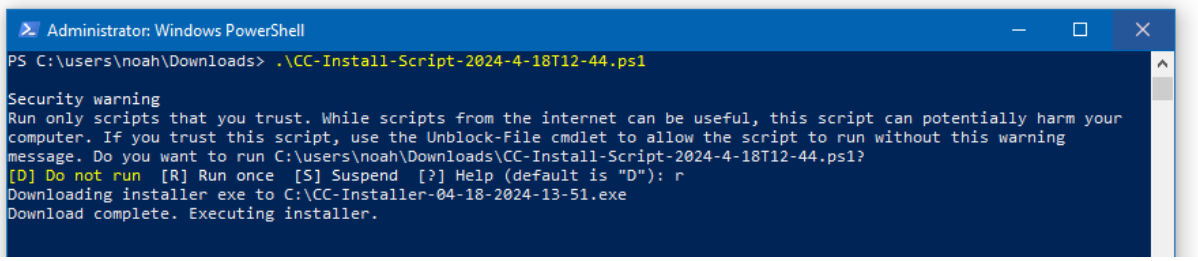
Hinweis: Dieses Skript muss wahrscheinlich für Ihren Anwendungsfall angepasst werden und erfordert Domänenanmeldeinformationen, um ausgeführt zu werden. Es wird erwartet, dass dieses Skript direkt auf einem (primären) Domänencontroller ausgeführt wird.

Ausführungsschritte

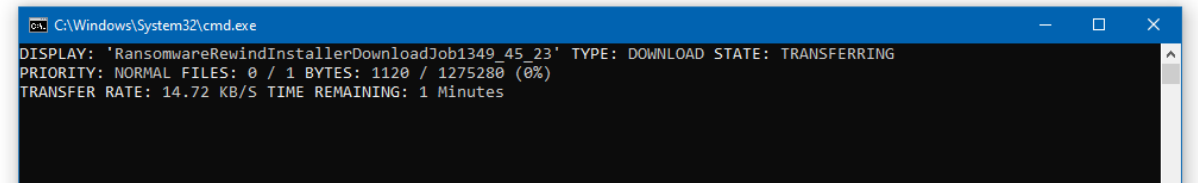
1. Aktualisieren Sie die Variable `$install_targets` mit einer Liste von Rechnernamen (NETBIOS- oder ähnliche Hostnamen)
2. Laden Sie ein „normales“ Installer-ps1-Skript von dem Cyber Crucible Dashboard herunter
3. Aktualisieren Sie die Variablen im Skript push_installer_ad.ps1, sodass sie mit den gruppenspezifischen Variablen aus dem Dashboard-Skript übereinstimmen
    1. `${GroupId}`
    2. `${ClientAuth}`
    3. alle `--rest-pub-key`-Variablen
4. Laden Sie eine native CLI-ausführbare Datei von dem Cyber Crucible Dashboard herunter
    1. Platzieren Sie die CLI auf einer Netzwerkfreigabe oder an einem Ort, der für alle zu installierenden Rechner zugänglich ist
        1. Dies verhindert, dass jeder Rechner Zeit und Bandbreite damit verschwendet, dieselbe exe erneut herunterzuladen
        2. Dieselbe exe kann für unterschiedliche Betriebssysteme ausgeführt werden, da der Installer die relevanten Dienst-/Treiber-/Installationsdateien für das erkannte Betriebssystem und die Rolle des Rechners herunterlädt.
    2. Setzen Sie `${OutputFilePath` auf den Pfad der CLI auf einer Netzwerkfreigabe
5. Entfernen Sie gegebenenfalls die ICMP-Online-Prüfung (falls nicht benötigt / für Ihre Umgebung ungültig)
6. Führen Sie das Skript mit `-credential` aus
    1. z. B. `./push_installer_ad.ps1 -credential ad1\kyle`

Übersicht über das Installationsskript

1. Der neueste Installer wird von `https://installerfiles.rpp.cybercrucible.com/installers/64/installer-cli.exe` herunterladen
    1. PowerShell (PS1)-Installationsskripte verwenden eine WebClient-Instanz.



    2. Batch (BAT)-Installationsskripte verwenden BitsAdmin oder, falls BitsAdmin fehlschlägt, JScript.



2. Der Installer wird ausgeführt, wobei ihm die Gruppen-ID und die Client-Authentifizierung aus Ihrem Skript übergeben werden.
    1. Optional kann bei der Ausführung der .exe der Parameter `--reuse-agent-by-machine-name` angehängt werden, damit der Installer das Agentenobjekt und die Lizenz eines bereits installierten Agenten mit demselben NetBIOS-Namen wiederverwendet.
3. Der Installer prüft die erforderlichen Installationsbedingungen
    1. Ausführung mit Administratorrechten.
    2. Der Computer läuft mit einer unterstützten Windows-Version.
    3. Es läuft nicht bereits ein anderer Installer.
    4. Der Agent ist noch nicht installiert.
4. Der Installer prüft, ob der Computer mit den erforderlichen Servern kommunizieren kann.
    1. Amazon oAuth 2.0 unter `ransomwarerewind-agents.auth.us-west-2.amazoncognito.com`
    2. Cyber Crucible-Backend unter `agent.tasking.rpp.cybercrucible.com`
5. Die Agentendateien werden über HTTPS von `installerfiles.rpp.cybercrucible.com` herunterladen.
6. Der Agent wird installiert und gestartet.

Installation mit SCCM

Die Installation von Cyber Crucible mit SCCM unterscheidet sich nicht von der Installation anderer Softwarepakete. Die wichtigsten Punkte für die Bereitstellung über SCCM sind:

1. Bereitstellung mit dem vorgefertigten PS1-Skript, heruntergeladen von https://dashboard.cybercrucible.com
2. Suchen Sie nach dem laufenden oder auf der Festplatte vorhandenen Dienst **Cyber Crucible Agent** als Erkennungsmethode. Der Standardspeicherort für den Agent-Dienst ist **C:\Program Files\CyberCrucible\service.exe**
    1. Optional können Sie auch nach dem Vorhandensein des Registrierungsschlüssels **HKLM\Software\CyberCrucibleAgent** suchen, beachten Sie jedoch, dass dieser Schlüssel nach einer Deinstallation möglicherweise noch vorhanden ist.

Standardkonfigurationsschritte

1. Erstellen Sie eine Anwendung, **kein** Paket
2. Konfigurieren Sie die Konfiguration manuell

image-20250807-175116.png

3. Konfigurieren Sie den Anwendungsnamen, den Herstellernamen, die Beschreibung usw.
4. Konfigurieren Sie den Bereitstellungstyp und geben Sie **Skriptinstallationsprogramm** an

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

5. Geben Sie den Skriptspeicherort an, wahrscheinlich eine Netzwerkfreigabe, z. B. **\\cc-dc01\share**
6. Geben Sie das Installationsprogramm an, um das bereitgestellte ps1 auszuführen, z. B. `Powershell.exe -file „CC-Install-Script-2025-8-7T13-55.ps1`
    1. Beachten Sie den Datumsstempel im Skriptnamen und ändern Sie ihn entsprechend Ihrem eigenen
    2. Es wird nicht empfohlen, PowerShell-Richtlinien zu überschreiben, aber je nach Ihrer Konfiguration müssen Sie möglicherweise `-executionpolicy Bypass` oder Ähnliches angeben
7. Fügen Sie eine Erkennungsmethode hinzu, indem Sie auf „Klausel hinzufügen“ klicken
    1. Siehe die empfohlenen Erkennungsmethoden oben auf dieser Seite
8. Geben Sie die UX-Bereitstellungseinstellungen an
    1. Da die Cyber Crucible-Bereitstellung keinen Neustart erfordert, liegen die Installations- und Anmeldeanforderungen im Ermessen Ihrer Organisation

image-20250807-175906.png

9. Wählen Sie Weiter/Fertig stellen, bis Sie den Assistenten schließen können.