Bereitstellung & Agentenverwaltung

Installation, Konfiguration, Aktualisierung und Überprüfung des Cyber Crucible-Agenten, einschließlich Onboarding, Systemanforderungen und Netzwerkkonfiguration.

Wie kann ich die Verbindung zu diesen Domains testen?

Wie kann ich die Verbindung zu diesen Domains testen?

Überprüfung von Zertifikatsketten

Das folgende PowerShell-Skript kann verwendet werden, um die von einem bestimmten Rechner erhaltene Zertifikatskette auszugeben. Dies kann hilfreich sein, um SSL-Probleme zu debuggen oder die Auswirkungen einer SSL-Firewall-Konfiguration zu untersuchen.

Verwendung

Rufen Sie das Skript in der PowerShell-Kommandozeile mit dem Parameter -TargetHost auf. Zum Beispiel:

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

Am ergibt sich folgende Ausgabe:

```
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
```

Wie überwache ich den Agent-Status (Agent Health)?

Offline/Online-Agent-Überwachung

Seite „Agents“

Auf der Seite „Agents“ wird das Datum und die Uhrzeit der letzten Anmeldung **pro Aktivität** erfasst. Allgemein gesprochen sollte, wenn ein Software-Agent funktioniert und mit dem Internet verbunden ist, jedes Verhalten ein Datum aufweisen, das weniger als ein paar Stunden zurückliegt. Manche Aktivitäten werden durch Vorgänge auf dem Endpunkt ausgelöst, während andere zeitgesteuert erfolgen, jedoch mit einem „Jitter“-Versatz von bis zu 30 Sekunden, damit Kunden keine Spitzen bei der Netzwerkaktivität erleben.

85753879.png?width=680

Verwaltung der Offline-Benachrichtigungen

Um Benachrichtigungen für Offline-Agenten einzurichten, verwenden Sie die Seite „Security Notifications“.

Diese Benachrichtigungen sind für folgende Situationen vorgesehen:

1. Es liegt ein Netzwerkproblem zwischen einem Agenten und den Cyber Crucible-Servern vor. Dies kann entweder durch eine Firewall (durch einen Hacker verursacht oder durch normale IT-Vorgänge) bedingt sein, oder der Agent läuft, ist jedoch offline. Der Schutz bleibt während Offline-Zeiten bestehen, jedoch erfolgen Sicherheitsteam-Benachrichtigungen erst, wenn der Agent wieder online ist.

2. Es liegt ein Problem mit der Cyber Crucible-Software vor. Dies ist sehr, sehr selten. Bitte öffnen Sie unverzüglich ein Support-Ticket bei Cyber Crucible, falls dies auftritt.
3. Der Rechner ist ausgeschaltet. Dies ist das häufigste Szenario. Eine Erörterung bewährter Vorgehensweisen folgt als Nächstes.

85688410.png?width=680

Bewährte Vorgehensweisen für Offline-Benachrichtigungen

Ein wichtiger Aspekt bei Offline-Benachrichtigungen ist, dass ein ausgeschalteter Rechner den Cyber Crucible-Servern als offline erscheint. Arbeitsplatzrechner, die im normalen Geschäftsbetrieb häufig ein- und ausgeschaltet werden, würden während Mittagspausen, Reisen zwischen Standorten oder an Feiertagen Offline-Benachrichtigungen erzeugen.

Bewährte Vorgehensweisen für Gruppen trennen Server bereits von Arbeitsplatzrechnern. Server werden typischerweise am besten mit kürzeren Offline-Benachrichtigungszeiträumen bedient, falls ein Problem auftritt. Auf Arbeitsplatzrechner ausgerichtete Gruppen eignen sich am besten für längere Zeiträume, bevor sie als offline gemeldet werden.

Viele Cyber Crucible-Kunden halten es für am besten, automatisierte Benachrichtigungen nur für Servergruppen zu erstellen und regelmäßig eines der Datumsfelder auf der Seite „Manage Agents“ nach einem Datum zu filtern, beispielsweise „Zeige mir Agenten, deren Feld ‚Machine Data Update‘ in der vergangenen Woche nicht aktualisiert wurde“.

85688417.png?width=453

Agenten, die nicht vollständig aktualisiert sind

Cyber Crucible-Agenten erfordern einen Neustart, um aktualisiert zu werden. Weiterführende Informationen zu den Aktualisierungsalgorithmen finden Sie hier. Wenn ein Agent meldet, dass ein Neustart zu einer Aktualisierung führen wird, listet die Seite „Agents“ auf, welche Rechner eine Aktualisierung benötigen und bereit sind, beim Neustart zu aktualisieren. Manchmal stapeln Rechner, wenn sie nicht häufig neu gestartet werden (typischerweise Server), mehrere Aktualisierungen, bevor tatsächlich ein Upgrade erfolgt. Ein Beispiel dafür ist im Screenshot zu sehen. Die letzte Neustartzeit ist ebenfalls verfügbar.

Der wöchentliche Cyber Crucible-Führungsbericht weist die Anzahl der Agenten aus, die ein Upgrade benötigen, sowie wie viele davon bereit sind, sofort nach einem Neustart zu aktualisieren. Die zwei häufigsten Gründe, warum ein Rechner eine Aktualisierung benötigt, aber nicht bereit/vorbereitet ist, sind:

1. Der Rechner war offline, beispielsweise weil ein Mitarbeiter im Urlaub war.
2. Der Rechner hatte einen Hardware- oder größeren Softwareausfall/-austausch, und Cyber Crucible befindet sich tatsächlich nicht mehr auf diesem Rechner.

Abgesehen von diesen beiden Fällen erfolgen Aktualisierungen normalerweise sehr schnell und ohne Beteiligung von Administratoren, außer im Rahmen der üblichen Patch- und Neustartvorgänge.

85688423.png

Welche Windows-Versionen werden von Cyber Crucible unterstützt?

Desktop-Version	Server-Version	Unterstützung
11 10 8.1 8	2025 2022 2019 2016 2012 R2 2012 R1	Vollständig unterstützt.
7	2008 R2	Muss für die Unterstützung der SHA-2-Codesignierung gepatcht werden.
Vista und niedriger	2008 R1 und niedriger	Nicht unterstützt.

Was sind normale Ressourcenverbrauchsraten für RAM und CPU?

Die typische CPU-Auslastung liegt bei 1 % oder darunter (was in den meisten Überwachungstools, wie dem Task-Manager, als 0 % angezeigt wird).

Die typische RAM-Auslastung liegt unter 10 MB. Die meisten Desktop- und Servernutzungen liegen bei etwa 5 MB.

Wir überwachen zudem die Speichernutzung des Treibers im Kernel-Space, um etwaige Probleme zu erkennen.

Wie kann ich erkennen, dass Cyber Crucible auf dem System läuft?

Dienste

Öffnen Sie den Task-Manager.

Klicken Sie auf die Registerkarte Dienste.

Sortieren Sie bei Bedarf nach Namen und scrollen Sie zu CyberCrucibleAgent/ Cyber Crucible Agent

image-20250811-181519.png

Kernel-Treiber

Öffnen Sie eine Eingabeaufforderung als Administrator.

Führen Sie den im untenstehenden Screenshot gezeigten Befehl aus:

fltmc.exe | find „CCRRSecMon“

3047503.png?width=561
fltmc.exe listet geladene Treiber auf.

Es gibt wahrscheinlich mehrere, daher zeigt der find-Befehl nur den Cyber Crucible Treiber namens CCRRSecMon an.

Wenn der Treiber aufgeführt ist, ist er geladen und läuft ordnungsgemäß im Betriebssystem.

Woher weiß ich, wann ein Agent die Selbstkonfiguration nach der Installation abgeschlossen hat?

Auf der Seite „Agents“ im Dashboard verfügt jeder Agent über einige Zeitstempel, die den letzten Zeitpunkt angeben, zu dem er bestimmte Arten von Informationen erhalten hat. Ein Agent gilt als mit der Selbstkonfiguration fertig, wenn er zusätzlich zu einer gültigen zugewiesenen Lizenz Zeitstempel für die folgenden Spalten aufweist:

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

Wenn die Gruppe darüber hinaus über

Onboarding-Prozess

Gruppenverwaltung

Vor der Installation von Agents möchten Benutzer sich möglicherweise vorbereiten, indem sie ihre Gruppen einrichten. Folgen Sie den Anweisungen zur Gruppenverwaltung hier.

Einrichten von Agent-Sicherheitswarnungen

Benutzer können E-Mail-Benachrichtigungen für Sicherheitsereignisse einrichten, einschließlich Ransomware-Aktivitäten, abnormaler Identitätszugriffe und offline befindlicher Agents. Anweisungen finden Sie hier.

Best Practices für die Planung der Agent-Installation

Einige Umgebungen weisen im gesamten Unternehmen ähnliches Benutzer-, Anwendungs- und Systemverhalten sowie ähnliche Konfigurationen auf. Andere verfügen über spezialisierte Gruppen, die sich unterschiedlich verhalten, wie beispielsweise ein Vertriebsteam im Vergleich zu einer Abteilung von Softwareentwicklern.

Bereitstellung und Konfiguration erfolgen so schnell, dass es sich lohnt, ein paar Minuten für die Planung einer Installation auf einer Teilmenge von Desktops oder Servern mit denselben Geschäftsverhaltensweisen oder Anwendungen zu investieren, um zu beurteilen, ob Anwendungen berücksichtigt werden müssen.

Darüber hinaus stellt sich häufig heraus, dass Cyber Crucible während der ersten Einführung zuvor unbekannte (und nicht autorisierte) Verwaltungssoftware und VPNs, nicht autorisierte Admin-Skripte, fehlkonfigurierte Software oder sogar Infektionen entdeckt.

Installieren des Agents

Wenn Sie bereit sind, Ihre Agents zu installieren, finden Sie Anweisungen hier und hier

Update-Strategien für Gruppen und Agents

Um die Update-Strategien für Gruppen und Agents zu verwalten, folgen Sie den Anweisungen hier.

So untersuchen Sie die Grundursache einer Erpressungsreaktion

Die Seite „Erpressungsreaktion“ finden Sie im Reiter „Operations“ in der Seitenleiste. Anweisungen dazu, wie Sie die Grundursache einer Warnung untersuchen können, finden Sie hier.

Maßgeschneiderte Verhaltensweisen

Anweisungen zum Erstellen maßgeschneiderter Verhaltensweisen finden Sie hier.

Rest-Integration

Einige Benutzer möchten sich möglicherweise mit unserem Rest-Server integrieren. Die Seite zur Rest-Integration mit der zugehörigen Dokumentation finden Sie auf unserer Website im Reiter „Administration“ in der Seitenleiste.

Bereitstellung in einer bereits infizierten Umgebung

Hintergrund

Bei Cyber Crucible-Kundenbereitstellungen werden regelmäßig zuvor unbekannte Infektionen entdeckt. Netzwerke sind normalerweise nicht infektionsfrei, selbst wenn bestehende Cybersicherheits-Tools „alles klar“ gemeldet haben.

Ein Ransomware-Angriff bietet einen deutlich sichtbaren Abgrenzungspunkt bzw. einen entscheidenden Wendepunkt, an dem ein Unternehmen messen kann, wie oft Hacker erfolgreich erneut angreifen und wie erfolgreich sie dabei sind.

- Open-Source-Berichte und Bedrohungsanalysen zeigen eine Wiederangriffsrate von etwa 80 % bei Unternehmen, die keine Cyber Crucible-Kunden sind.
- Cyber Crucible beobachtete, dass bei etwa 10 % der Endpunkte pro 90-Tage-Zeitraum mindestens ein Versuch von Identitätsdiebstahl stattfand, etwa von Passwörtern, Schlüsseln oder Tokens.
- Cyber Crucible beobachtet, dass Angreifer ungefähr monatlich versuchen, wieder Fuß in einer Umgebung zu fassen.

Aus Sicht der Vorfallreaktion (Incident Response) bzw. Forensik ist Cyber Crucible ein hervorragendes Werkzeug, um die Kontrolle über das Netzwerk zurückzugewinnen. Insbesondere bei Opfern von Angriffen gehen wir davon aus, dass die Angreifer den Wiederherstellungs- und finanziellen Status der Opfer weiterhin im Blick behalten, um den richtigen Zeitpunkt für einen erneuten Angriff besser abschätzen zu können.

Was unmittelbar nach der Installation passiert

Cyber Crucible beginnt automatisch damit, laufende Programme zu suspendieren, die sich beobachtbar bösartig verhalten.

Der Rollout des Cyber Crucible-Produkts kann dazu führen, dass mehrere Programme auf mehreren Rechnern suspendiert werden, während die Umgebung bereinigt wird.

Mitunter kann ein teilweiser Rollout von Cyber Crucible dazu führen, dass der Hacker versucht, über die Rechner ohne Cyber Crucible-Schutz wieder Kontrolle zu erlangen.

So wurde Cyber Crucible beispielsweise bei einem kürzlichen Opfer einer Datenpanne nur auf einem Teil der Desktop-Rechner installiert. Die Hacker versuchten, Cyber Crucible zu deinstallieren, indem sie sich von den ungeschützten Rechnern aus verbanden, und begannen schließlich, die geschützten Rechner abzuschalten.

Was geschieht mit ruhender Malware, die auf zukünftige Aufgaben wartet?

Malware, die nicht im Auftrag von Angreifern aktiv wird, wird ausgelöst, sobald sie beginnt, auf Daten zuzugreifen.

Gehen wir ein Szenario durch:

Zwei Rechner sind mit Malware infiziert. Nennen wir sie Rechner A und Rechner B.

Beide Malware-Proben sind derzeit von Ihren bevorzugten Sicherheitstools nicht erkennbar.

Die Malware auf Rechner A tut nichts, sondern wartet auf Anweisungen. Cyber Crucible erkennt die Malware nicht. Die Malware ist auch von anderen Sicherheitstools noch nicht erkennbar.

Die Malware auf Rechner B versucht, auf Daten oder Identitätsdaten zuzugreifen. Unmittelbar nach einem erfolgreichen Angriff besteht das häufigste Verhalten, das wir beobachten, wenn Angreifer ihre Malware beauftragen, darin, sicherzustellen, dass sie über aktuelle Identitätsdaten wie Passwörter oder Tokens verfügen, sowie neue Daten zu erfassen. Also teils „die neuen Passwörter beschaffen, nachdem die Administratoren die Passwörter zurückgesetzt haben“ und teils „im Blick behalten, ob es neue Daten gibt“.

Auf Rechner B suspendiert Cyber Crucible die Anwendung sofort.

Nach einem Zeitraum von einem Monat bis zu einem Jahr wird die Malware auf Rechner A entdeckt, nachdem genügend Opfer die Malware an Sicherheitsanbieter-Datenbanken gemeldet haben. Je disziplinierter die Angreifer bei der Verbreitung dieser Probe vorgehen, desto länger bleibt diese

bestimmte Malware unentdeckt.

Die Malware auf Rechner B wurde neutralisiert und ist eingefroren.

Die Malware auf Rechner A sitzt in der Falle. In dem Moment (genauer: nach 100 Millisekunden), in dem sie versucht, auf Daten oder Identitätsinformationen zuzugreifen, wird die Malware auf Rechner A suspendiert. Der Kunde ist geschützt, selbst wenn die Malware Tage bis Jahre existiert, ohne von anderen Tools erkannt zu werden.

Zusätzliche Details – Neustarts können wertvoll sein

Einige unserer Analysen sind am genauesten, wenn der Lebenszyklus eines Prozesses vom Start der Anwendung bis zum aktuellen Zustand nachverfolgt werden kann.

Ein Neustart des Rechners nach der Installation kann von Vorteil sein.

Programme, die bereits vor der Installation liefen, werden von Cyber Crucible nicht vollständig analytisch überprüft. Ein Neustart erzwingt, dass diese Programme neu starten, wodurch eine vollständige Überprüfung aller Programme ermöglicht wird.

Wie teste ich die TLS-Verbindung zu diesen Domains?

Über das reine Anpingen der von Cyber Crucible verwendeten Domains hinaus, um sicherzustellen, dass Ihr Endpunkt alle korrekten Netzwerkadressen erreichen kann, enthält das Cyber Crucible Agent-Installationsprogramm ein Testargument, das sicherstellt, dass in beide Richtungen eine gültige TLS/SSL-Verbindung zu allen erforderlichen Servern hergestellt werden kann.

Untitled-20240410-185719.png
Fügen Sie einfach `--test-connection` zur Ausführung des Installationsprogramms hinzu und stellen Sie sicher, dass die für die Authentifizierung erforderlichen Gruppen-ID(s) und OAuth-Tokens weiterhin enthalten sind. Oben ist ein Screenshot zu sehen, der die einzige notwendige Änderung am bereitgestellten .bat-Skript sowie eine erfolgreiche Ausgabe zeigt.

Anhänge:

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

Warum benötige ich möglicherweise einen Proxy?

Obwohl die gesamte verhaltensbasierte Erkennung und der Schutz des Cyber Crucible-Agents am Endpunkt erfolgen, ohne dass Proben zur Analyse in die Cloud übermittelt werden müssen, benötigt der Endpunkt-Agent dennoch eine Verbindung zu einem Server, um Lizenzierungsinformationen, Konfigurationen, Software-Updates usw. zu erhalten.

Wenn Ihr Netzwerk so stark abgeriegelt ist, dass keine Verbindungen zu den IP-Bereichen zugelassen werden, in denen die Cyber Crucible-Server gehostet werden, benötigen Sie möglicherweise einen konfigurierten Proxy, damit (ausschließlich) der Agent seinen Server zur Installation erreichen kann. Informationen zur Konfiguration des Agents finden Sie unter How to Manage Proxy Configurations.

Welche Art von Proxy kann ich verwenden?

Ab Version 4.4.6.3 des Cyber Crucible-Agents unterstützen die Proxy-Konfigurationen Socks5. Es gibt keine Einschränkung hinsichtlich des Hosting-Standorts des Servers (vor Ort oder extern), solange die Netzwerkbeschränkungen den Agents das Erreichen des Servers ermöglichen. Nachfolgend ist ein Beispieldiagramm einer einfachen Proxy-Konfiguration dargestellt, bei der der Socks5-Server innerhalb des abgeriegelten Netzwerks gehostet wird und nur eine Verbindung zu einem externen Rechner herstellen darf, der den Datenverkehr tunnelt.

SOCKS5H.png

Dieses Setup ermöglicht es den Agents, sich mit ihrem/ihren Server(n) zu verbinden, während die Netzwerkrichtlinie eingehalten wird. Es ist nur eine Regel erforderlich, die es dem Socks5-Host erlaubt, seinen externen Proxy-Server über einen Port (SSH) zu erreichen. Dies stellt sicher, dass der gesamte Datenverkehr nicht nur über Port 443 läuft, sondern zusätzlich vor dem Verlassen des Netzwerks doppelt in SSH verpackt wird, und erfordert keine eingehende Portweiterleitung.

Wie viel Daten werden von Cyber Crucible erzeugt?

Die vom Cyber Crucible Agent erfassten Daten durchlaufen mehrere Filterebenen, um Rauschen durch zu viel Rohtelemetrie herauszufiltern. Die von den Kernel-Sensoren erzeugten Rohdaten werden reduziert [**Filter #1**], um sowohl den Speicherverbrauch am Endpunkt als auch die Netzwerkbandbreite pro Agent zu verringern. Anschließend ordnet die REST-API die empfangene Roh-Prozess-/Endpunkttelemetrie automatisierten Reaktionen zu, sodass der Analyst wählen kann, nur relevante Daten anzuzeigen [**Filter #2**].

Blank diagram-20240523-165941.png

Wie in der obigen Abbildung zu sehen ist, können die Workstation-Endpunkte eines durchschnittlichen Kunden über einen Zeitraum von 24 Stunden mehrere Gigabyte an Rohsensordaten erzeugen, während bei einem versuchten Angriff nur wenige Megabyte davon für einen SOC-Alarm relevant sind.

Wie deinstalliere ich mehrere Agenten gleichzeitig?

Die gleichzeitige Deinstallation mehrerer Agenten ist einfach.

Gehen Sie zur Seite Agenten.

Wir empfehlen die Verwendung von Filtern, wie z. B. Maschinenname, Gruppe, IP-Adresse oder Versionsfilter, um möglichst viele Agenten auf dem Bildschirm anzuzeigen. Dies ist besonders nützlich für Benutzer mit Hunderten oder Tausenden von Agenten in einer Gruppe.

85983282.png?width=680
Hier haben wir die Umschalttaste verwendet, während wir auf 3 Zeilen geklickt haben, um drei Agenten auszuwählen.

Die Schaltfläche „Alle ausgewählten Agenten deinstallieren“ befindet sich oben links über dem Raster.

Nachdem die Berechtigungen auf dem Server überprüft wurden, dass Sie über Berechtigungen in den Gruppen der Agenten verfügen, werden Deinstallationsbefehle ausgegeben.

Die Agenten erhalten einen digital signierten Deinstallationsbefehl. Die Signatur wird von den Agenten verwendet, um zu überprüfen, dass der Befehl tatsächlich von Cyber Crucible stammt und nicht von einem Kriminellen, der versucht, Ihre Schutzsoftware zu entfernen.

Sobald die Agenten die Validierung bestätigt haben, bereiten sie das System für die Deinstallation beim nächsten Neustart vor.

In der Spalte „Achtung“ erscheint der Eintrag „Deinstallation läuft“ und in der Zelle wird eine Schaltfläche „Deinstallation abbrechen“ angezeigt.

Sobald der Rechner neu gestartet wurde, überprüft der Agent, dass die Deinstallation durchgeführt wird, und entfernt alle Dateien.

Wichtig zu beachten ist, dass der Agent vor der vollständigen Deinstallation „ein letztes Mal grüßt“, sodass Agenten manchmal noch für kurze Zeit nach dem Neustart vorhanden sind. Dies liegt daran, dass einige Netzwerkumgebungen bis zu 30 Sekunden, nachdem der Desktop sichtbar ist, nicht ordnungsgemäß funktionieren. Beachten Sie, dass nach Abschluss der Deinstallationen Lizenzen automatisch von den Agenten entfernt werden.

Wie deinstalliere ich einen einzelnen Agenten?

Rufen Sie die Seite Agenten auf.

Suchen Sie den gewünschten Agenten und klicken Sie auf das Papierkorb-Symbol in der Spalte Agentenname:

86081562.png?width=680

Testen, ob die Cyber Crucible-Software „funktioniert“

Einführung

Cyber Crucible wurde so konzipiert, dass es läuft, ohne Endnutzer oder Mitarbeiter zu stören, während ausgewählte Dashboard-Nutzer (typischerweise ausgewählte Mitglieder der IT- und Sicherheitsteams) im Hintergrund über automatisierte Reaktionen informiert werden.

Viele Simulatoren für Ransomware oder Malware bilden das Verhalten eines Hackers nicht genau ab. Auch wenn dies für Tools wie Cyber Crucible, die die Simulation (korrekt) als Fehlalarm erkennen, Probleme verursacht, ist das nicht unbedingt schlecht.

Manche Anbieter bauen ihre Erkennungs-Engines für einen Teil ihrer Erkennungsfunktionen sogar gezielt auf diese Simulatoren auf, um sicherzustellen, dass alle Kundentests mit Bravour bestanden werden.

Reale Malware-Aktionen wie Ransomware-Verschlüsselung bergen das Risiko, Daten unwiederbringlich zu verschlüsseln oder zu beschädigen. Bei Cyber Crucible haben wir sogar erlebt, dass Ransomware heimlich andere Malware im Netzwerk aktiviert oder andere Aktionen ausführt, die dem Unternehmen schaden könnten, das versucht, Cyber Crucible zu testen.

Sie möchten also weder Malware verwenden, noch einen Simulator, der so realistisch ist, dass Sie versehentlich Ihre Daten beschädigen könnten.

Cyber Crucible testen

Es gibt eine einfache Möglichkeit, Cyber Crucible zu testen, ohne Malware oder eine Simulation zu verwenden, die so realistisch ist, dass Sie Ihre eigenen Daten oder die Ihres Unternehmens gefährden.

Cyber Crucible bewertet jede Millisekunde des Tages Zugriffe auf digitale Identitäten. Viele dieser digitalen Identitäten werden in Browsern gespeichert – deshalb setzen Angreifer Webbrowser bei ihrem automatisierten Targeting ganz oben auf die Liste.

Die Verhaltensanalyse von Cyber Crucible bei Identitätszugriffen führt zu einer von drei Reaktionen:

1. Nichts tun
2. Daten verbergen
    1. bekannte, legitime Anwendung, die alle Speicher- und Kernel-Prüfungen besteht, aber keinen Zugriff auf diese bestimmten Identitätsdaten benötigt – Beispiel: unausgenutzter Windows Explorer
3. Prozess anhalten
    1. bekannte, legitime Anwendung, die eigentlich Zugriff auf die Identitätsdaten haben sollte, aber gehackt wurde, oder
    2. eine ungewöhnliche Anwendung

Hier sind zwei Speicherorte, die bei Windows-Nutzern häufig vorkommen:

In diesem Fall lautet der Windows-Benutzername „denni“, und dies sind die Speicherorte, an denen Sitzungsdaten abgelegt werden. Möglicherweise funktioniert für Sie die Variable %LOCALAPPDATA%, wenn Sie den Benutzernamen nicht ermitteln möchten.

- 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

Die Ansicht ohne installiertes Cyber Crucible

Sehen wir uns zunächst an, wie einer dieser Ordner mit Explorer.exe aussieht, ohne dass Cyber Crucible installiert ist.

Screenshot 2025-05-14 103339.png
Hier sehen wir mehrere Chrome-Sitzungen unter dem „Standard“-Google-Chrome-Profil.

Diese Informationen enthalten typischerweise sensible Daten, mit denen ein Angreifer Sitzungen wichtiger Programme wie IT-Administrationsportale, Banking, E-Mail oder Speicherwerkzeuge wie Google Drive oder Dropbox kapern möchte.

Die Ansicht mit installiertem Cyber Crucible

Nach der Installation von Cyber Crucible kann ein schneller Test durchgeführt werden, ohne Malware oder irgendeine Art von kriminellen Techniken oder Missbrauch der IT-Ausrüstung zu verwenden.

In diesem Fall wird derselbe Speicherort für Browser-Sitzungen verwendet:

- 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 blockiert bereits unmittelbar nach der Installation den Zugriff auf die Daten in diesem Ordner.

Bitte beachten Sie, dass es sich um genau denselben Explorer-Prozess handelt, der bereits vor der Installation lief – dem laufenden Programm wurde also plötzlich der Zugriff auf der „Festplatten“- oder Kernel-Ebene entzogen. Selbst Programme, seien sie harmlos, ausgenutzt oder Malware, die bereits laufen, werden von Cyber Crucible korrekt bewertet.

Ihren Test im Cyber Crucible Dashboard einsehen

Es gibt jederzeit eine große Anzahl von Identitätsdatenzugriffen in einem laufenden System.

Software as a Service und cloudbasierte Programme haben dazu geführt, dass viele Websites und Anwendungen auf der Website selbst nur begrenzt Funktionen bieten, während der Browser (oder der eingebettete Browser bei Anwendungen) ständig mit Datenservern kommuniziert, um Tabellen, Diagramme und Social-Media-Inhalte zu befüllen.

Seite „Identitätszugriff“

Identitätszugriffe, bei denen es als angemessen erachtet wird, dass Cyber Crucible die betreffende Anwendung anhält, werden auf der Seite „Identitätszugriff“ aufgeführt.

Dies sind Situationen, in denen das auf die Identitätsdaten zugreifende Programm gestoppt werden sollte, statt nur die Daten zu verbergen.

In diesem Fall wurde Explorer nach der Vielzahl der von Cyber Crucible durchgeführten Prüfungen nicht gestoppt. Stattdessen wurden lediglich Daten verborgen.

Screenshot 2025-05-14 103741.png
Daher sind hier keine Verstöße gegen den Identitätszugriff aufgeführt.

Seite „Identitätszugriff verborgen“

Cyber Crucible bietet optional die Möglichkeit, Dashboard-Kunden Situationen anzuzeigen, in denen Identitätsdaten verborgen wurden, das zugreifende Programm jedoch nicht gestoppt wurde.

Explorer wurde in diesem Test nicht ausgenutzt oder war anderweitig bösartig, es griff lediglich auf sehr privilegierte Identitätsdaten der Browser Chrome und Edge zu.

Die meisten Nutzer haben aufgrund der zusätzlichen Belastung der Kundenrechner und -netzwerke bei der Übertragung dieser Daten an die Cyber Crucible-Server keinen Zugriff auf diese Informationen.

Bitte fragen Sie nach, wenn Sie Zugriff wünschen. Beachten Sie jedoch, dass die von Ihnen gesehene Aktivität keine bösartige Aktivität ist, sondern ein Verhalten zum Schutz der Privatsphäre von Identitätsdaten, das Cyber Crucible aus GRC- bzw. Richtliniendurchsetzungsperspektive durchführt.

Identity Hide Explorer.mp4
Hier sehen wir in diesem kurzen Video, dass Explorer daran gehindert wurde, die Browser-Sitzungsdaten einzusehen, obwohl Explorer selbst nicht unterbrochen wurde.

Verwaltung von Proxy-Konfigurationen

Beachten Sie, dass nur Agenten ab Version 4.4.6.3 über diese Fähigkeit verfügen

Wo Sie die aktuelle Proxy-Konfigurationseinstellung einer Gruppe finden

Benutzer können die aktuelle Proxy-Server-Konfigurationseinstellung einer Gruppe für die Agenten, die dieser Gruppe folgen, einsehen, indem sie zunächst zur Seite „Groups“ navigieren, die sich unter dem Tab „Administration“ in der Seitenleiste befindet.

Die aktuelle Proxy-Server-Konfigurationseinstellung einer Gruppe finden Sie in der Spalte „Proxy Server Config“ im Raster.

Wenn für die Gruppe keine Proxy-Server-Konfiguration aktiviert ist, wird der Text „Do Not Use Proxy“ angezeigt.

Proxy Server Config Column.png
Wenn für die Gruppe eine Proxy-Server-Konfiguration aktiviert ist, wird die URL der aktuellen Proxy-Konfiguration angezeigt

Proxy Server Config Enabled.png

Wie Sie eine Gruppe aktualisieren, um einen Proxy-Server zu aktivieren

Benutzer können Agenten in einer Gruppe so aktivieren, dass sie einen Proxy-Server verwenden, indem sie zunächst auf das Symbol „Manage Proxy Configurations“ in der Spalte „Proxy Server Config“ auf der Seite „Groups“ klicken. Durch Klicken auf dieses Symbol öffnet sich ein modales Fenster, in dem Benutzer die Proxy-Server-Konfigurationen für die Gruppe verwalten können.

Manage Proxy Server Config Icon.png
Das angezeigte modale Fenster „Manage Proxy Server Configuration“ dient dazu, die Proxy-Server-Konfigurationen für die Gruppe anzuzeigen und zu verwalten. Benutzer können mehrere Konfigurationen innerhalb einer Gruppe speichern, und alle gespeicherten Konfigurationen werden im Raster dieses modalen Fensters angezeigt. Beachten Sie, dass alle gespeicherten Proxy-Server-Konfigurationen einer Gruppe auch im modalen Fenster „Download Agent“ erscheinen.

Um eine Proxy-Server-Konfiguration für die Gruppe auszuwählen, muss die Konfiguration zunächst über das Formular „New Proxy Configuration“ übermittelt werden. Dieses Formular ist standardmäßig ausgeblendet, klicken Sie auf den Schalter, um es anzuzeigen.

Manage Proxy Server Configs Modal.pngNew Proxy Configuration Form.png
Nach dem Absenden des Formulars für die neue Konfiguration wird diese unten im Raster des modalen Fensters angezeigt.

Um eine Proxy-Konfiguration auszuwählen, die von Agenten in dieser Gruppe verwendet werden soll, wählen Sie zunächst die gewünschte Konfiguration aus und klicken Sie dann auf das Bearbeiten-Symbol oberhalb des Rasters.

Select Config for Group.png
Nachdem Sie auf das Bearbeiten-Symbol für die gewünschte Proxy-Konfiguration geklickt haben, ist die aktuelle Proxy-Server-Konfiguration der Gruppe nun aktualisiert und kann in diesem modalen Fenster sowie in der Spalte „Proxy Server Config“ eingesehen werden. Agenten in dieser Gruppe verwenden nun die aktualisierte Proxy-Konfiguration der Gruppe. Beachten Sie, dass ein Agent, der die Anweisung erhält, zu einem nicht erreichbaren Proxy-Server zu wechseln, erst wechselt, wenn dieser Server erreichbar wird.

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

Wie Sie eine Gruppe aktualisieren, damit kein Proxy verwendet wird

Wenn für eine Gruppe ein Proxy-Server aktiviert ist, den Agenten in dieser Gruppe verwenden sollen, und Benutzer die Gruppe so aktualisieren möchten, dass Agenten in dieser Gruppe keinen Proxy mehr verwenden, navigieren Sie zunächst zur Seite „Groups“ und suchen Sie die gewünschte Gruppe im Raster.

Klicken Sie dann auf das Symbol „Manage Proxy Configurations“ in der Spalte „Proxy Server Config“. Durch Klicken auf dieses Symbol öffnet sich das modale Fenster „Manage Proxy Server Configuration“.

Proxy Server Config Column 2.png
Klicken Sie in diesem modalen Fenster auf das x-Symbol, um Agenten in dieser Gruppe so zu aktualisieren, dass sie keinen Proxy-Server verwenden und normal mit unseren Servern kommunizieren. Beachten Sie, dass die aktuelle Proxy-Konfiguration dadurch nicht aus den gespeicherten Proxy-Konfigurationen der Gruppe entfernt wird; dies ist ein separater Schritt, der im folgenden Abschnitt beschrieben wird.

Do Not Use Proxy Icon.png
Nachdem Sie auf das x-Symbol geklickt haben, wird das modale Fenster aktualisiert, um diese Änderung widerzuspiegeln, und die Spalte „Proxy Server Config“ für diese Gruppe zeigt nun „Do Not Use Proxy“ an.

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

Wie Sie eine gespeicherte Proxy-Konfiguration in einer Gruppe entfernen

Um eine gespeicherte Proxy-Konfiguration einer Gruppe zu entfernen, navigieren Sie zunächst zur Seite „Groups“ und suchen Sie die gewünschte Gruppe im Raster.

Klicken Sie dann auf das Symbol „Manage Proxy Configurations“ in der Spalte „Proxy Server Config“. Durch Klicken auf dieses Symbol öffnet sich das modale Fenster „Manage Proxy Server Configuration“.

Manage Proxy Server Config Icon.png
Klicken Sie in diesem modalen Fenster auf die gewünschte gespeicherte Proxy-Konfiguration, die für diese Gruppe entfernt werden soll, und klicken Sie dann auf das Papierkorb-Symbol. Nach dem Klicken auf dieses Symbol erscheint die ausgewählte Proxy-Konfiguration nicht mehr im Raster als gespeicherte Proxy-Konfiguration für die Gruppe.

Remove Saved Config.png
Beachten Sie, dass, wenn Sie eine gespeicherte Proxy-Konfiguration für eine Gruppe entfernen und diese Konfiguration als aktuelle Proxy-Server-Konfiguration der Gruppe festgelegt ist, dies auch die aktuelle Proxy-Server-Konfiguration der Gruppe so aktualisiert, dass kein Proxy verwendet wird.

Wie Sie einen Agenten unter Verwendung eines Proxys installieren

Navigieren Sie zunächst zur Seite „Agents“, die sich unter dem Tab „Operations“ in der Seitenleiste befindet. Klicken Sie dann auf die Schaltfläche „Download Agent“. Durch Klicken auf diese Schaltfläche öffnet sich das modale Fenster „Download Agent“.

Download Agent Button.png
Wenn Sie in diesem modalen Fenster eine Gruppe auswählen, die über gespeicherte Proxy-Konfigurationen verfügt, erscheint die Option „Select Proxy Configuration for Installer“, wobei die aktuelle Einstellung der Gruppe als Standardwert ausgewählt ist. Alle gespeicherten Proxy-Konfigurationen der Gruppe erscheinen ebenfalls als Optionen, einschließlich einer Option „Do Not Use Proxy“.

Download Agent Modal.pngDownload Agent Modal Proxy Config Options.png
Wenn Sie sich dafür entscheiden, einen Proxy für das Installationsprogramm zu verwenden, ist als einziger Installationsprogrammtyp der Command Line Installer möglich.

Wenn Sie die Option „Do Not Use Proxy“ auswählen, erscheinen unsere normalen Installationsprogrammtyp-Optionen.

Download Agent Modal Do Not Use Proxy.png
Beachten Sie, dass, wenn Sie für das Installationsprogramm eine Proxy-Konfiguration auswählen, die nicht der aktuellen Einstellung der Gruppe entspricht, das Installationsprogramm mit der ausgewählten Einstellung ausgeführt wird und nach der Installation zur aktuellen Proxy-Konfigurationseinstellung der Gruppe wechselt.

Wo Sie sehen können, ob ein Agent in der Lage ist, den Proxy zu umgehen

Benutzer können einsehen, ob Agenten sich ohne Verwendung eines Proxys mit unseren Servern verbinden können, indem sie zunächst zur Seite „Agents“ navigieren, die sich unter dem Tab „Operations“ in der Seitenleiste befindet. Suchen Sie dann die Spalte „Agent is Able to Bypass Proxy“ im Raster.

Beachten Sie, dass die Spalte „Agent is Able to Bypass Proxy“ nur sichtbar ist, wenn der Benutzer Mitglied einer Gruppe ist, in der Agenten für die Verwendung eines Proxys aktiviert wurden.

Wenn sich der Agent in einer Gruppe befindet, in der die Verwendung eines Proxys aktiviert wurde, und der Agent den Proxy nicht umgehen kann, um sich mit unseren Servern zu verbinden, wird das rote x-Symbol in der Spalte angezeigt. Ein Beispiel hierfür finden Sie unten:

Agent Cannot Bypass Proxy.png
Wenn sich der Agent in einer Gruppe befindet, in der die Verwendung eines Proxys aktiviert wurde, und der Agent in der Lage ist, den Proxy zu umgehen und sich normal mit unseren Servern zu verbinden, wird das grüne Häkchen in der Spalte angezeigt. Ein Beispiel hierfür finden Sie unten:

Agent Can Bypass Proxy.png