Versionen & Updates

Softwareveröffentlichungen, Upgrade-Hinweise, Wartungsmitteilungen und Qualitätssicherung.

Was ist das Qualitätssicherungsprogramm von Cyber Crucible?

Cyber Crucible durchläuft zahlreiche Phasen interner Tests sowie externer Validierung, einschließlich der Tests des Microsoft Windows Hardware Certification Program, um die Funktionsfähigkeit auf allen Microsoft-Betriebssystemen bis zurück zu Server 2008 R2 sicherzustellen.

Dies lässt sich anhand des Windows Server Catalog nachvollziehen, in dem ausschließlich Treiber aufgeführt sind, die die WHCP-Validierung bestanden haben. Ebenso kann dies durch eine Suche in der Microsoft-Altitude-Liste überprüft werden, die die Altitude aller registrierten Treiber anzeigt.

- https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/allocated-altitudes
- Windows Server Catalog - Cyber Crucible

69369886.png

06. März 2024

Zusammenfassung des Vorfalls

Ein Netzwerkausfall am 6MAR2024 beeinträchtigte den Zugriff über das Frontend auf das Cyber Crucible
Dashboard sowie den Telemetriezugriff über die API. Dieses Problem wurde inzwischen am 7MAR2024 behoben.

Ursache

Um 0400 UTC am 6MAR2024 begann der Telemetrieverkehr eskalierend anzusteigen und erreichte schließlich 1600 % des normalen
Agenten-Datenverkehrs. Zusätzlich begann sich die Netzwerkbandbreite zwischen den AWS-Instanzen auf
begrenzte Geschwindigkeiten zwischen den AWS-gehosteten Load Balancern, Servern und Datenbanken zu drosseln. In
mehreren Zonen waren die Bandbreitenbeschränkungen unterschiedlich stark ausgeprägt und reichten von vollständigem Übertragungsverlust
(0 % der Kapazität) bis zu 50 % der Kapazität. Auch die Verfügbarkeit des AWS-DNS war beeinträchtigt.
Es wurde bestätigt, dass der eingehende Netzwerkverkehr zu Cyber Crucible gültiger Agenten-Datenverkehr bestehender
Kunden war. Der Bot-Datenverkehr zu den Load Balancern nahm im Volumen nicht zu.
Die zusätzliche Bandbreite war nicht die Hauptursache für die Nichtverfügbarkeit der Server, verschärfte jedoch
die Bandbreitenprobleme bei Middleware und Datenbank.
Der Anstieg des Agenten-Datenverkehrs in diesem Zeitraum hat sich teilweise wieder gelegt.
Zum aktuellen Zeitpunkt kommuniziert Cyber Crucible keinen Zusammenhang zwischen den am 6MAR2024 gemeldeten Cloud-Ausfällen und den AWS-Problemen bzw. dem Anstieg des Datenverkehrs.

Auswirkung

Der Zugriff auf das Cyber Crucible Dashboard und die APIs wäre verzögert oder nicht verfügbar gewesen.
Die Telemetrie von installierten Agenten blieb vollständig erhalten und konnte bei der Übermittlung an die Datenbank verzögert sein, es ging jedoch keine Telemetrie verloren. Die Endpunktschutzfunktionen der Agenten waren vollständig
unbeeinträchtigt und funktionierten normal, da keine Analyse- oder Schutzfunktionen von einer Netzwerkverbindung zu
vorgelagerten APIs abhängen. Zum aktuellen Zeitpunkt hat die gesamte Telemetrie im Dashboard „aufgeholt“.

Behebung

Cyber Crucible hat mehrere Server sowohl innerhalb als auch außerhalb von AWS eingerichtet. Die Netzwerkstabilität innerhalb von
AWS scheint sich über Nacht (7MAR2024) verbessert zu haben, wobei bereits ab
0200 UTC Verbesserungen beobachtet wurden. Cyber Crucible arbeitet derzeit mit 500 % der Serverkapazität, berechnet auf Basis
der Spitzenbandbreite des Datenverkehrs, die inzwischen zurückgegangen ist. Das Team hat AWS-gehostete
Server ersetzt, sobald diese die Netzwerkverbindung verloren.

Um es klar zu sagen: Eine zusätzliche Serverskalierung war in diesem Fall keine wirksame Lösung. Cyber Crucible hat begonnen, sich von AWS als alleinigem Cloud-Hosting-Anbieter zu lösen. Arbeiten
zur Unterstützung einer Cloud-Plattform-unabhängigen Architektur laufen bereits seit Monaten, mit ursprünglichen
Plänen, sich im zweiten Quartal 2024 von AWS als alleinigem Anbieter zu lösen. End-to-End-Tests, einschließlich aller

erforderlichen Doppelverschlüsselungs- und x509-Authentifizierungsschemata für unsere verschiedenen Server und
Dienste, wurden Ende Februar 2024 abgeschlossen. Die Netzwerkprobleme, die wir
mit AWS erlebt haben, haben die ursprünglich für Q2 geplante Umstellung beschleunigt, sodass sie nun einen Monat früher als
geplant beginnt.

Wie kann ich Update-Strategien für Gruppen und Agenten verwalten?

Gruppen-Update-Einstellungen verwalten

Bei Gruppen ist die automatische Aktualisierung standardmäßig aktiviert, und Agenten folgen standardmäßig den Update-Einstellungen ihrer Gruppe. Die Gruppen-Update-Einstellungen finden Sie auf der Seite „Groups“:

85295158.png?width=680
Die erste Spalte zeigt an, ob die automatische Aktualisierung für die Gruppe ein- oder ausgeschaltet ist. Die zweite Spalte zeigt, welche Version für Updates bei Agenten in dieser Gruppe freigegeben ist, sofern diese ihre Gruppen-Update-Einstellungen nicht überschreiben.

Wenn bei Gruppen die automatische Aktualisierung eingeschaltet ist, zeigt die Spalte „Approved Agent Version“ die zuletzt veröffentlichte Agentenversion an und ist nicht bearbeitbar.

Wenn bei Gruppen die automatische Aktualisierung ausgeschaltet ist, ist die Spalte „Approved Agent Version“ bearbeitbar: Durch Doppelklick auf die Zelle kann die gewünschte freizugebende Version ausgewählt werden. Es gibt außerdem die Option, Updates vollständig zu deaktivieren (die Option „Do Not Update“). Beachten Sie, dass Agenten keine Downgrades auf frühere Versionen durchführen.

Beachten Sie, dass die Gruppen-Update-Einstellungen bei der Installation eines Agenten herangezogen werden, um zu entscheiden, mit welcher Version der Agent installiert werden soll. Wenn bei der Gruppe die automatische Aktualisierung ausgeschaltet und „Do Not Update“ ausgewählt ist, wird der Agent standardmäßig mit der neuesten verfügbaren Agentenversion installiert.

Agenten-Update-Einstellungen verwalten

Agenten folgen standardmäßig den Update-Einstellungen ihrer Gruppe, können jedoch so konfiguriert werden, dass sie die Gruppen-Update-Einstellungen überschreiben und stattdessen ihren eigenen Einstellungen folgen. Die Agenten-Update-Einstellungen finden Sie auf der Seite „Agents“:

85131315.png?width=680
Wenn ein Agent die Gruppen-Update-Einstellungen überschreibt, sind die Spalten für automatische Aktualisierung und freigegebene Agentenversion bearbeitbar, sodass Benutzer die Update-Einstellungen des Agenten konfigurieren können, denen dieser dann statt den Gruppen-Update-Einstellungen folgt.

Wenn ein Agent den Gruppen-Update-Einstellungen folgt, sind die Spalten für automatische Aktualisierung und freigegebene Agentenversion nicht bearbeitbar und zeigen die Gruppen-Update-Einstellungen an.

Was bedeutet "Update Staged"?

Das Aktualisieren von Cyber Crucible ist ein automatisierter, mehrstufiger, geschützter Prozess.

Das Update erfordert einen Neustart, um wirksam zu werden, nachdem es von den Cyber Crucible-Servern abgerufen wurde.

Version	Attention
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)
4.4.0.6	Update Staged (4.4.0.7)

Während einige Updates von sehr alten Versionen aus mehrere Schritte erfordern, können Updates bei Bedarf mehrere Versionen überspringen.

Zum Beispiel haben die folgenden Rechner 4.4.0.6 heruntergeladen, aber vor der Veröffentlichung von 4.4.0.7 keinen Neustart durchgeführt.

Sie werden nun 4.4.0.7 ausführen, sobald sie neu gestartet werden.

Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

Im Detail erfordert die Aktualisierung von Cyber Crucible die folgenden Schritte:

1. Die Cyber Crucible-Software erhält die Benachrichtigung, dass ein Update verfügbar ist.
2. Diese Update-Benachrichtigung ist RSA-signiert, um sicherzustellen, dass ein Angreifer kein bösartiges Update erzwingen kann. Diese Update-Benachrichtigung wird auf ihre Echtheit überprüft. Dies ist Teil des Zero-Trust-Produktdesigns von Cyber Crucible.
3. Das Update wird vom Agenten heruntergeladen.
4. Das Update wird validiert, um sicherzustellen, dass es nicht beschädigt oder anderweitig manipuliert wurde.
5. Das Update stellt die neue Software für die Installation bereit. Die Schutzmechanismen von Cyber Crucible im Arbeitsspeicher und auf der Festplatte verhindern, dass sie aktualisiert oder die Software ersetzt wird, außer während des Startvorgangs.
6. Nach der Verifizierung wird an die Cyber Crucible-Server eine Benachrichtigung gesendet, dass das Update bereit und ordnungsgemäß positioniert ist.
7. Nach einem Neustart wird das Update auf die Software angewendet, und die Cyber Crucible-Software meldet die neue Version zurück. Die Meldung "Update Staged" verschwindet.

Erfordert ein Update von Cyber Crucible einen Neustart?

Ja, es gibt verschiedene Speicher-, Dateisystem- und Betriebssystemschutzmechanismen, die die Cyber Crucible-Software nutzt, um sich selbst vor Manipulation oder Leistungsbeeinträchtigung durch Angreifer zu schützen.

Dies ist Teil des Zero-Trust-Produktdesigns von Cyber Crucible.

Ein Update erfordert das Ersetzen des Treibers und der Dienste.

Beim Neustart wird ein Zeitfenster geöffnet, in dem die Cyber Crucible-Software ein ordnungsgemäß verifiziertes Update zulässt.

Ein Update ist bereit für den Neustart, wenn Folgendes auf der Seite „Manage Agents“ zu sehen ist.

Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

Aktualisiert Cyber Crucible mehrere Versionen auf einmal?

Auch wenn beim Aktualisieren mehrerer Versionen selten mehrere Updates erforderlich sind, werden Updates normalerweise alle auf einmal durchgeführt, selbst wenn ein Agent mehrere Versionen hinter der neuesten Version zurückliegt.

Zum Beispiel haben die unten abgebildeten Agenten zunächst 4.4.0.6 heruntergeladen, um zu aktualisieren. Sie wurden nicht neu gestartet, um das Update anzuwenden, bevor 4.4.0.7 veröffentlicht wurde. Als 4.4.0.7 veröffentlicht wurde, luden die Agenten 4.4.0.7 herunter und bereiteten es vor.

Wenn die Systeme neu gestartet werden, läuft Cyber Crucible 4.4.0.7, und die Meldung „Staged Update“ wird verschwinden.

Version	Attention
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)
4.4.0.5	Update Staged (4.4.0.7)

Wie sieht Ihre Software-Update-Strategie aus?

Die Software von Cyber Crucible ist nicht auf kontinuierliche Signatur-Updates angewiesen, um Angreifern hinterherzujagen.

Etwa einmal pro Monat werden neue Funktionen, Erweiterungen der Zero-Trust-Methodik sowie Verbesserungen der Verhaltensanalyse-Module veröffentlicht.

Alle Software-Releases von Cyber Crucible werden zudem getestet, freigegeben und nach unseren eigenen strengen Tests vom Microsoft Hardware Compatibility Program zertifiziert.

Für ein Upgrade ist ein Neustart erforderlich, bevor ein Update wirksam wird.

Gruppen-Update-Einstellungen verwalten

Für Gruppen ist die automatische Aktualisierung standardmäßig aktiviert, und Agenten folgen standardmäßig den Update-Einstellungen ihrer Gruppe. Die Gruppen-Update-Einstellungen finden Sie auf der Seite „Gruppen“:

85426272.png?width=680
Die erste Spalte zeigt an, ob für die Gruppe die automatische Aktualisierung aktiviert oder deaktiviert ist. Die zweite Spalte zeigt, welche Version für Updates von Agenten in dieser Gruppe freigegeben ist, sofern diese ihre Gruppen-Update-Einstellungen nicht überschreiben.

Wenn für Gruppen die automatische Aktualisierung aktiviert ist, zeigt die Spalte „Freigegebene Agentenversion“ die zuletzt veröffentlichte Agentenversion an und ist nicht bearbeitbar.

Wenn für Gruppen die automatische Aktualisierung deaktiviert ist, ist die Spalte „Freigegebene Agentenversion“ bearbeitbar, indem Sie die Zelle doppelklicken und die gewünschte Version auswählen. Es gibt außerdem die Option, Updates vollständig zu deaktivieren (die Option „Nicht aktualisieren“). Beachten Sie, dass Agenten keine Downgrades auf ältere Versionen durchführen.

Beachten Sie, dass die Gruppen-Update-Einstellungen bei der Installation eines Agenten angewendet werden, um zu bestimmen, mit welcher Version der Agent installiert werden soll. Wenn für die Gruppe die automatische Aktualisierung deaktiviert ist und „Nicht aktualisieren“ ausgewählt wurde, installiert der Agent standardmäßig die neueste verfügbare Agentenversion.

Agenten-Update-Einstellungen verwalten

Agenten folgen standardmäßig den Update-Einstellungen ihrer Gruppe, können jedoch so konfiguriert werden, dass sie die Gruppen-Update-Einstellungen überschreiben und stattdessen ihre eigenen Einstellungen verwenden. Die Agenten-Update-Einstellungen finden Sie auf der Seite „Agenten“:

85557298.png?width=680
Wenn ein Agent die Gruppen-Update-Einstellungen überschreibt, sind die Spalten „Automatische Aktualisierung“ und „Freigegebene Agentenversion“ bearbeitbar, sodass Benutzer die Update-Einstellungen des Agenten konfigurieren können, denen dieser dann folgt, anstatt den Gruppen-Update-Einstellungen zu folgen.

Wenn ein Agent den Gruppen-Update-Einstellungen folgt, sind die Spalten „Automatische Aktualisierung“ und „Freigegebene Agentenversion“ nicht bearbeitbar und zeigen die Gruppen-Update-Einstellungen an.