Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

Veröffentlicht: 2023-11-13

ExtraHop Cloud Services bietet über eine verschlüsselte Verbindung Zugriff auf Cloud-basierte Dienste von ExtraHop. Die Dienste, mit denen Sie verbunden sind, werden durch Ihre Systemlizenz bestimmt.

Nachdem die Verbindung hergestellt wurde, werden Informationen zu den verfügbaren Diensten auf der Seite ExtraHop Cloud Services angezeigt.

- Der ExtraHop Machine Learning Service ermöglicht Erkennungen für Ihr ExtraHop-System. In Reveal (x) Enterprise können Sie reine Sicherheitserkennungen oder Sicherheits- und Leistungserkennungen aktivieren.
- Reveal (x) Enterprise-Benutzer können Daten an den Machine Learning Service senden, indem sie ExtraHop Cloud Services in den Administrationseinstellungen aktivieren. Das System kann beispielsweise externe Klartext-IP-Adressen, Domainnamen und Hostnamen senden, die mit dem erkannten verdächtigen Verhalten in Verbindung stehen. Diese Einstellung ist in Reveal (x) 360 standardmäßig aktiviert und kann nicht deaktiviert werden. Sehen Sie die Häufig gestellte Fragen zur gemeinsamen Bedrohungsanalyse für weitere Informationen. Eine vollständige Liste der Datentypen, die an den ExtraHop Machine Learning Service gesendet werden, und Informationen darüber, wie die Daten zur Verbesserung der Bedrohungserkennung verwendet werden, finden Sie im Abschnitt Machine Learning der Überblick über Sicherheit, Datenschutz und Vertrauen bei ExtraHop.
- Der ExtraHop Update Service ermöglicht automatische Updates von Ressourcen für das ExtraHop-System, z. B. von Ransomware-Paketen.
- Mit ExtraHop Remote Access können Sie es Mitgliedern des ExtraHop-Kontoteams, ExtraHop Atlas-Analysten und dem ExtraHop-Support ermöglichen, sich mit Ihrem ExtraHop-System zu verbinden, um Hilfe bei der Konfiguration zu erhalten. Wenn Sie sich für den Atlas Remote Analysis Service angemeldet haben, können die Analysten von ExtraHop eine unvoreingenommene Analyse Ihrer Netzwerkdaten durchführen und über Bereiche in Ihrer IT-Infrastruktur berichten, in denen Verbesserungen vorgenommen werden können. Sehen Sie die Häufig gestellte Fragen zum Fernzugriff für weitere Informationen über Benutzer mit Fernzugriff.

Bevor Sie beginnen

- Reveal (x) 360-Systeme werden automatisch mit ExtraHop Cloud Services verbunden. Möglicherweise müssen Sie jedoch den Zugriff über Netzwerk-Firewalls zulassen.
- Sie müssen die entsprechende Lizenz auf dem ExtraHop-System anwenden, bevor Sie eine Verbindung zu den ExtraHop Cloud Services herstellen können. Sehen Sie die Häufig gestellte Fragen zur Lizenz für weitere Informationen.
- Sie müssen eingerichtet haben oder System- und Zugriffsadministrationsrechte um auf die Administrationseinstellungen zuzugreifen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Netzwerkeinstellungen auf **ExtraHop Cloud-Dienste** .
3. klicken **Allgemeine Geschäftsbedingungen** um den Inhalt zu lesen.
4. Lesen Sie die Allgemeinen Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen.
5. klicken **Stellen Sie eine Verbindung zu ExtraHop Cloud Services her**.

   Nachdem Sie eine Verbindung hergestellt haben, wird die Seite aktualisiert und zeigt Status- und Verbindungsinformationen für jeden Dienst an.
6. Optional: Aktivieren Sie im Bereich Machine Learning Service das Kontrollkästchen für **Tragen Sie zum Machine Learning Service zur kollektiven Bedrohungsanalyse bei** und wählen Sie dann eine der folgenden Optionen:

© 2023ExtraHop Networks, Inc. Alle Rechte vorbehalten.

- Externe IP-Adressen
- Externe IP-Adressen, Domains und Hostnamen

Wenn die Verbindung fehlschlägt, liegt möglicherweise ein Problem mit Ihren Firewallregeln vor.

Konfigurieren Sie Ihre Firewall-Regeln

Wenn Ihr ExtraHop-System in einer Umgebung mit einer Firewall eingesetzt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen. Für Reveal (x) 360-Systeme, die mit selbstverwalteten Systemen verbunden sind Sensoren, müssen Sie auch den Zugang zum ExtraHop Cloud Recordstore öffnen.

Offener Zugang zu Cloud-Diensten

Für den Zugriff auf ExtraHop Cloud Services benötigen Sie Sensoren muss in der Lage sein, DNS-Abfragen für *.extrahop.com aufzulösen und über die IP-Adresse, die Ihrer entspricht, auf TCP 443 (HTTPS) zuzugreifen Sensor Lizenz:

- 35.161.154.247 (Portland, Vereinigte Staaten von Amerika)
- 54.66.242.25 (Sydney, Australien)
- 52.59.110.168 (Frankfurt, Deutschland)

Offener Zugang zu Cloud Recordstore

Für den Zugriff auf den ExtraHop Cloud Recordstore benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) zu diesen vollqualifizierten Domainnamen zuzugreifen:

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Sie können auch die öffentlichen Leitlinien von Google zu folgenden Themen lesen Berechnung möglicher IP-Adressbereiche für googleapis.com.

Zusätzlich zur Konfiguration des Zugriffs auf diese Domänen müssen Sie auch die globale Proxyserver-Einstellungen.

Stellen Sie über einen Proxy eine Verbindung zu ExtraHop Cloud Services her

Wenn Sie keine direkte Internetverbindung haben, können Sie versuchen, über einen expliziten Proxy eine Verbindung zu ExtraHop Cloud Services herzustellen.

Bevor Sie beginnen
Überprüfen Sie, ob Ihr Proxyanbieter so konfiguriert ist, dass er Machine-in-the-Middle (MITM) ausführt, wenn SSH über HTTP CONNECT zu localhost:22 getunnelt wird. ExtraHop Cloud Services stellt einen verschlüsselten inneren SSH-Tunnel bereit, sodass der Datenverkehr für die MITM-Inspektion nicht sichtbar ist. Es wird empfohlen, eine Sicherheitsausnahme zu erstellen und die MITM-Prüfung für diesen Datenverkehr zu deaktivieren.

Wichtig: Wenn Sie MITM auf Ihrem Proxy nicht deaktivieren können, müssen Sie die Zertifikatsvalidierung in der Konfigurationsdatei des ExtraHop-Systems deaktivieren, in der das ExtraHop-System ausgeführt wird. Weitere Informationen finden Sie unter Zertifikatsvalidierung umgehen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
3. Klicken **ExtraHop Cloud-Proxy aktivieren**.
4. Geben Sie den Hostnamen für Ihren Proxyserver ein, z. B. `Proxyhost`.
5. Geben Sie den Port für Ihren Proxyserver ein, z. B. `8080`.
6. Optional: Geben Sie bei Bedarf einen Benutzernamen und ein Passwort für Ihren Proxyserver ein.
7. Klicken **Speichern**.

Zertifikatsvalidierung umgehen

Einige Umgebungen sind so konfiguriert, dass verschlüsselter Datenverkehr das Netzwerk nicht ohne Überprüfung durch ein Gerät eines Drittanbieters verlassen kann. Dieses Gerät kann als SSL/TLS-Endpunkt fungieren, der den Datenverkehr entschlüsselt und erneut verschlüsselt, bevor die Pakete an ExtraHop Cloud Services gesendet werden.

Wenn eine Appliance über einen Proxyserver eine Verbindung zu ExtraHop Cloud Services herstellt und die Zertifikatsvalidierung fehlschlägt, deaktivieren Sie die Zertifikatsvalidierung und versuchen Sie erneut, die Verbindung herzustellen. Die durch die Authentifizierung und Verschlüsselung des ExtraHop-Systems gebotene Sicherheit stellt sicher, dass die Kommunikation zwischen Geräten und ExtraHop Cloud-Diensten nicht abgefangen werden kann.

Hinweis: Das folgende Verfahren setzt Vertrautheit mit der Änderung der laufenden ExtraHop-Konfigurationsdatei voraus.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Geräteeinstellungen Abschnitt, klicken **Config ausführen**.
3. Klicken **Konfiguration bearbeiten**.
4. Fügen Sie die folgende Zeile am Ende der laufenden Konfigurationsdatei hinzu:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Klicken **Aktualisieren**.
6. Klicken **Änderungen anzeigen und speichern**.
7. Überprüfen Sie die Änderungen und klicken Sie auf **Speichern**.
8. Klicken **Erledigt**.