Leitfaden zur technischen Implementierung von RevealX Enterprise Secure

Veröffentlicht: 2025-03-28

Die folgenden Abschnitte enthalten Informationen und Empfehlungen zur Konfiguration Ihres ExtraHop RevealX Enterprise-Systems mit optimalen Sicherheitskontrollen.

Datenschutz

Die folgenden Abschnitte enthalten Anleitungen zu Einstellungen, die sicherstellen, dass Ihre Daten geschützt sind.

Erstellen Sie eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System

Eine Certificate Signing Request (CSR) ist ein verschlüsselter Textblock, der Ihrer Zertifizierungsstelle (CA) zur Verfügung gestellt wird, wenn Sie ein TLS-Zertifikat beantragen. Die CSR wird auf dem ExtraHop-System generiert, auf dem das TLS-Zertifikat installiert wird, und enthält Informationen , die in das Zertifikat aufgenommen werden, wie z. B. den allgemeinen Namen (Domänenname), die Organisation, den Ort und das Land. Die CSR enthält auch den öffentlichen Schlüssel, der im Zertifikat enthalten sein wird. Die CSR wird mit dem privaten Schlüssel aus dem ExtraHop-System erstellt, wodurch ein Schlüsselpaar entsteht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** und klicken Sie dann **Eine Zertifikatsignieranforderung (CSR) exportieren**.
4. In der Betreff Alternative Namen Abschnitt, geben Sie den DNS-Namen des ExtraHop-Systems ein.

   Sie können mehrere DNS-Namen und IP-Adressen hinzufügen, die durch ein einziges TLS-Zertifikat geschützt werden sollen.
5. In der Betreff Abschnitt, füllen Sie die folgenden Felder aus.

   Nur die **Allgemeiner Name** Feld ist erforderlich.

Feld	Beschreibung	Beispiele
Allgemeiner Name	Der vollqualifizierte Domänenname (FQDN) des ExtraHop-Systems . Der FQDN muss mit einem der alternativen Betreffnamen übereinstimmen.	*.example.com discover.example.com
E-mail-Adresse	Die E-Mail-Adresse des Hauptansprechpartners für Ihre Organisation.	webmaster@example.com
Organisatorische Einheit	Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.	IT-Abteilung
Organisation	Der offizielle Name Ihrer Organisation. Dieser Eintrag darf nicht abgekürzt werden und sollte Suffixe wie Inc, Corp oder LLC enthalten.	Beispiel, Inc.

Feld	Beschreibung	Beispiele
Ort/Stadt	Die Stadt, in der sich Ihre Organisation befindet.	Seattle
Bundesstaat/Provinz	Das Bundesland oder die Provinz, in der sich Ihre Organisation befindet. Dieser Eintrag sollte nicht abgekürzt werden.	Washington
Landeskennzahl	Der zweibuchstabige ISO-Code für das Land, in dem sich Ihre Organisation befindet.	UNS

6. Klicken Sie **Exportieren**.
   Die CSR-Datei wird automatisch auf Ihren Computer heruntergeladen.

Nächste Schritte
Senden Sie die CSR-Datei an Ihre Zertifizierungsstelle (CA), um die CSR signieren zu lassen. Wenn Sie das TLS-Zertifikat von der CA erhalten haben, kehren Sie zur TLS-Zertifikat Seite in den Administrationseinstellungen und laden Sie das Zertifikat in das ExtraHop-System hoch.

Hinweis Wenn Ihre Organisation verlangt, dass der CSR einen neuen öffentlichen Schlüssel enthält, ein selbstsigniertes Zertifikat generieren um neue Schlüsselpaare zu erstellen, bevor die CSR erstellt wird.

Verschlüsselungssteuerungen

Die folgenden Abschnitte enthalten Anleitungen zu Einstellungen, die die Verschlüsselung steuern.

Verschlüsselung im Ruhezustand

Auf Daten auf einer gestohlenen unverschlüsselten Festplatte kann immer noch zugegriffen werden. Eine Verschlüsselung im Ruhezustand schützt Ihre Daten jedoch weiter, da für den Zugriff auf Festplattendaten ein Verschlüsselungsschlüssel erforderlich ist.

Verschlüsselung im Ruhezustand kann auf unterstützten Appliances konfiguriert.

Verschlüsselung während der Übertragung

Die folgenden Einstellungen in der Konfigurationsdatei wird ausgeführt helfen Sie dabei, Ihre verschlüsselten Daten während der Übertragung zu sichern.

Einige der folgenden Einstellungen werden möglicherweise nicht standardmäßig in der Datei „Laufende Konfiguration“ angezeigt. Wenn sie jedoch von einem Administrator hinzugefügt wurden, sollten Sie sicherstellen, dass diese Einstellungen für die sicherste Option konfiguriert sind.

Die meisten dieser Einstellungen sind standardmäßig auf den sichersten Modus konfiguriert, aber hier ist eine Liste der Einstellungen.

Ersetzen Sie den DNS-Lizenzverkehr durch HTTPS über ExtraHop Cloud Services

Diese Einstellung ermöglicht es Lizenz-Check-Ins, sich über HTTPS mit ExtraHop Cloud Services zu verbinden, anstatt über DNS. Einstellung `use_dns` zu `false` stellt sicher, dass die Firmware über einen verschlüsselten Tunnel eine Verbindung zu den ExtraHop Cloud Services herstellt, um Lizenzen einzuchecken. Die Einstellung ist gesetzt auf `true` standardmäßig, sollte aber geändert werden in `false` um die Sicherheit zu maximieren:

```
"license_server": {
    "use_dns": false
```

```
}
```

Beachten Sie, dass, wenn dieser Wert auf gesetzt ist `false`, wenn die Appliance keine Verbindung zu ExtraHop Cloud Services über HTTPS herstellen kann, werden alle Funktionen angehalten.

FIPS-Modus aktivieren

Diese Einstellung konfiguriert die Appliance so, dass die Verschlüsselung für die Datenübertragung auf FIPS-validierte Algorithmen beschränkt wird. Diese Einstellung ist gesetzt auf `false` standardmäßig, sollte aber gesetzt sein auf `true` für Kunden, die FIPS-validierte Algorithmen einhalten müssen.

Die Einstellung sollte aus Gründen der FedRAMP-Konformität wie folgt aussehen:

```
"fips": {
    "enabled": true
}
```

Überprüfung des ExtraHop Cloud Services-Zertifikats

Wenn ein Kundenknoten ExtraHop Cloud Services beitritt, verifiziert ExtraHop standardmäßig das SSL-Zertifikat. Dieses Zertifikat kann zwar deaktiviert werden, die inneren Tunnel validieren jedoch weiterhin Zertifikate. Die Einstellung sollte wie folgt aussehen:

```
"hopcloud": {
    "verify_outer_tunnel_cert": true
}
```

Strenge HTTP-Transportsicherheit (HSTS)

Aktiviert HTTP Strict Transport Security (HSTS), einen Mechanismus für Websicherheitsrichtlinien, der Websites vor Protokoll-Downgrade-Angriffen und Cookie-Hijacking schützt. Die Einstellung sollte wie folgt aussehen:

```
"webserver": {
    "hsts": true
}
```

Webserver-SSL-Profil

Ermittelt das für den Appliance-Webserver konfigurierte SSL-Profil. Das SSL-Profil sollte auf seinem Standardwert von belassen werden `modern`:

```
"webserver": {
    "ssl_profile": "modern"
}
```

Richtlinie zur Inhaltssicherheit (CSP)

Dieses Flag ermöglicht das Hinzufügen des Content-Security-Policy-Headers. Das Flag ist derzeit standardmäßig auf false gesetzt. Der CSP ist definiert als `default-src 'self' 'unsafe-inline'; img-src * data:`. Die Einstellung sollte wie folgt aussehen:

```
"webserver": {
    "enable_csp": true,
}
```

Weiterleitung von Sitzungsschlüsseln

Informationen zur Konfiguration der Sitzungsschlüsselweiterleitung finden Sie in den folgenden Anleitungen:

- Installieren Sie den ExtraHOP Session Key Forwarder auf einem Windows-Server
- Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server

- Laden Sie Sitzungsschlüssel mit Paket herunter

Wichtig: Stellen Sie sicher, dass der Zugriff für den TCP-Port 4873 auf dem ExtraHop-Sensor geöffnet ist.

TLS-Entschlüsselung

Informationen zur Konfiguration der TLS-Entschlüsselung finden Sie in den folgenden Anleitungen:

- Entschlüsseln Sie den TLS-Verkehr mit Zertifikaten und privaten Schlüsseln
- TLS-Entschlüsselung

PCAP konfigurieren

Mit der Paketerfassung können Sie Datenpakete aus Ihrem Netzwerkverkehr sammeln, speichern und abrufen. Sie können eine Paketerfassungsdatei zur Analyse in einem Drittanbieter-Tool wie Wireshark herunterladen. Pakete können überprüft werden, um Netzwerkprobleme zu diagnostizieren und zu lösen und um sicherzustellen , dass die Sicherheitsrichtlinien eingehalten werden.

Durch Hinzufügen einer Paketerfassungsdiskette zum ExtraHop Sensor, können Sie die an Ihr ExtraHop-System gesendeten Rohdaten speichern. Diese Festplatte kann zu Ihrer virtuellen Festplatte hinzugefügt werden Sensor oder eine SSD, die in Ihrem physischen Gerät installiert ist Sensor.

Diese Anweisungen gelten nur für ExtraHop-Systeme, die über eine Precision Paket Capture Disk verfügen. Informationen zum Speichern von Paketen auf einer ExtraHop PacketStore-Appliance finden Sie in der Anleitungen zur Bereitstellung von Packetstore.

Wichtig: Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

Päckchen schneiden

Standardmäßig speichert der Packetstore ganze Pakete. Wenn Pakete noch nicht in Scheiben geschnitten sind, können Sie den Sensor so konfigurieren, dass er Pakete speichert, die auf eine feste Anzahl von Byte aufgeteilt sind, um den Datenschutz und das Lookback zu verbessern.

Weitere Informationen zur Konfiguration dieser Funktion in Ihrer laufenden Konfigurationsdatei erhalten Sie vom ExtraHop-Support.

PCAP aktivieren

Ihr ExtraHop-System muss für die PCAP lizenziert und mit einer dedizierten Speicherplatte konfiguriert sein. Körperlich Sensoren benötigen eine SSD-Speicherfestplatte und virtuelle Sensoren benötigen eine Festplatte, die auf Ihrem Hypervisor konfiguriert ist.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr ExtraHop-System für Packet Capture lizenziert ist, indem Sie sich in den Administrationseinstellungen anmelden und auf **Lizenz**. Die Paketerfassung ist unter Funktionen aufgeführt und **Aktiviert** sollte erscheinen.

Wichtig: Der Erfassungsvorgang wird neu gestartet, wenn Sie die Paketerfassungsdiskette aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken **Festplatten**.
3. Abhängig von deinem Sensor Typ- und Menüoptionen, konfigurieren Sie die folgenden Einstellungen.
   - Für physische Sensoren klicken Sie auf **Aktiviere** neben SSD Assisted Packet Capture, und klicken Sie dann auf **OK**.
   - Stellen Sie für virtuelle Sensoren sicher, dass `running` wird in der Spalte Status angezeigt und die Festplattengröße, die Sie für die PCAP konfiguriert haben, wird in der Spalte Größe angezeigt.

Klicken Sie **Aktiviere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette, und klicken Sie dann auf **OK**.

Nächste Schritte
Ihre Paketerfassungsdiskette ist jetzt aktiviert und bereit, Pakete zu speichern. Klicken Sie **Konfiguriere** wenn Sie die Festplatte verschlüsseln oder konfigurieren möchten weltweite oder Präzisionspaket erfasst.

Verschlüsseln Sie die Paketerfassungsdiskette
Paketerfassungsfestplatten können mit einer 256-Bit-AES-Verschlüsselung gesichert werden.

Hier sind einige wichtige Überlegungen, bevor Sie eine Paketerfassungsdiskette verschlüsseln:

- Sie können eine Paketerfassungsdiskette nicht entschlüsseln, nachdem sie verschlüsselt wurde. Sie können die Verschlüsselung löschen, aber die Festplatte ist formatiert und alle Daten werden gelöscht.
- Sie können eine verschlüsselte Festplatte sperren, um jeglichen Lese- oder Schreibzugriff auf gespeicherte Paketerfassungsdateien zu verhindern. Wenn das ExtraHop-System neu gestartet wird, werden verschlüsselte Festplatten automatisch gesperrt und bleiben gesperrt, bis sie mit der Passphrase entsperrt werden. Unverschlüsselte Festplatten können nicht gesperrt werden.
- Sie können eine verschlüsselte Festplatte neu formatieren, aber alle Daten werden dauerhaft gelöscht. Sie können eine gesperrte Festplatte neu formatieren, ohne die Festplatte zuerst zu entsperren.
- Sie können eine sichere Löschung (oder Systemlöschung) aller Systemdaten durchführen. Anweisungen finden Sie in der Medienleitfaden für ExtraHop Rescue.

Warnung: Wenn Sie eine Paketerfassungsdiskette verschlüsseln, werden alle auf der Festplatte gespeicherten Pakete gelöscht.

Wichtig: Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

1. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Sensortyp eine der folgenden Optionen aus.
   - Für virtuelle Sensoren klicken Sie auf **Konfiguriere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette.
   - Für physische Sensoren klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.
3. Klicken Sie **Festplatte verschlüsseln**.
4. Geben Sie einen Festplattenverschlüsselungsschlüssel aus einer der folgenden Optionen an:
   - Geben Sie eine Passphrase in die Felder Passphrase und Bestätigen ein.
   - Klicken Sie **Wählen Sie Datei** und wählen Sie eine Verschlüsselungsschlüsseldatei aus.
5. Klicken Sie **Verschlüsseln**.

Nächste Schritte
Sie können den Festplattenverschlüsselungsschlüssel ändern, indem Sie zur Seite Festplatten zurückkehren und auf **Konfiguriere** und dann **Festplattenverschlüsselungsschlüssel ändern**.

Formatieren Sie die Paketerfassungsdiskette
Sie können eine verschlüsselte Paketerfassungsdiskette so formatieren, dass alle Paketerfassungen dauerhaft entfernt werden. Beim Formatieren einer verschlüsselten Festplatte wird die Verschlüsselung aufgehoben. Wenn Sie eine unverschlüsselte Paketerfassungsdiskette formatieren möchten, müssen Sie die Festplatte entfernen und die Festplatte dann erneut aktivieren.

Warnung: Diese Aktion kann nicht rückgängig gemacht werden.

1. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.

- Für virtuelle Sensoren klicken Sie auf **Konfiguriere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette.
- Für physische Sensoren klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.

3. Klicken Sie **Festplattenverschlüsselung löschen**.
4. Klicken Sie **Format**.

Entfernen Sie die Paketerfassungsdiskette
Wenn Sie eine Paketerfassungsdiskette austauschen möchten, müssen Sie die Festplatte zuerst aus dem System entfernen. Wenn eine Paketerfassungsdiskette aus dem System entfernt wird, werden alle Daten auf der Festplatte dauerhaft gelöscht.

Zum Entfernen des Datenträgers muss eine Formatoption ausgewählt werden. Bei physischen Geräten können Sie die Festplatte nach Abschluss dieses Vorgangs sicher aus der Appliance entfernen.

1. In der Appliance-Einstellungen Abschnitt, klicken **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.
   - Für virtuelle Appliances klicken Sie auf **Konfiguriere** neben Triggered Packet Capture.
   - Für physische Geräte klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.
3. Klicken Sie **Festplatte entfernen**.
4. Wählen Sie eine der folgenden Formatoptionen aus:
   - **Schnelles Format**
   - **Sicheres Löschen**
5. Klicken Sie **entfernen**.

Konfigurieren Sie eine globale PCAP
Eine globale PCAP erfasst jedes Paket, das an das ExtraHop-System gesendet wird, für die Dauer, die den Kriterien entspricht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Paketerfassung Abschnitt, klicken **Globale Paketerfassung**.
   Bei der Konfiguration der PCAP müssen Sie nur die gewünschten Kriterien für die Paketerfassung angeben.
3. In der Name Feld, geben Sie einen Namen ein, um die Paketerfassung zu identifizieren.
4. In der Max. Pakete Feld, geben Sie die maximale Anzahl der zu erfassenden Pakete ein.
5. In der Max. Byte Feld, geben Sie die maximale Anzahl der zu erfassenden Byte ein.
6. In der Max. Dauer (Millisekunden) Feld, geben Sie die maximale Dauer der PCAP in Millisekunden ein.
   ExtraHop empfiehlt den Standardwert 1000 (1 Sekunde). Der Maximalwert beträgt bis zu 60000 Millisekunden (1 Minute).
7. In der Schnappschuss Feld, geben Sie die maximale Anzahl der pro Frame kopierten Byte ein.
   Der Standardwert ist 96 Byte, aber Sie können diesen Wert auf eine Zahl zwischen 1 und 65535 setzen.
8. Klicken Sie **Starten**.

   Hinweis: Notieren Sie sich den Zeitpunkt, zu dem Sie mit der Erfassung beginnen, um das Auffinden der Pakete zu erleichtern.
9. Klicken Sie **Stopp** um die Paketerfassung zu stoppen, bevor eine der Höchstgrenzen erreicht wird.

Laden Sie Ihre PCAP herunter.

- Klicken Sie auf RevealX Enterprise-Systemen auf **Pakete** aus dem Hauptmenü und dann auf **PCAP herunterladen**.

Um das Auffinden Ihrer PCAP zu erleichtern, klicken und ziehen Sie auf die Zeitleiste der Paketabfrage, um den Zeitraum auszuwählen, in dem Sie die PCAP gestartet haben.

- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen, klicken **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Paketerfassung.

Konfigurieren Sie eine präzise PCAP
Für präzise Paketerfassungen sind ExtraHop-Trigger erforderlich, mit denen Sie nur die Pakete erfassen können, die Ihren Spezifikationen entsprechen. Trigger sind hochgradig anpassbarer benutzerdefinierter Code, der bei definierten Systemereignissen ausgeführt wird.

Bevor Sie beginnen
Die Paketerfassung muss auf Ihrem ExtraHop-System lizenziert und aktiviert sein.

Es wird empfohlen, dass Sie sich mit dem Schreiben von Triggern vertraut machen, bevor Sie eine präzise PCAP konfigurieren. Hier sind einige Ressourcen, die Ihnen helfen, mehr über ExtraHop Triggers zu erfahren:

- Triggerkonzepte
- Einen Auslöser erstellen
- Trigger-API-Referenz
- Gehen Sie durch: Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren

Im folgenden Beispiel erfasst der Auslöser einen HTTP-Flow mit dem Namen `HTTP host <hostname>` und stoppt die Erfassung, nachdem maximal 10 Pakete gesammelt wurden.

1. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Trigger**.
2. klicken **Erstellen**.
3. Geben Sie einen Namen für den Auslöser ein und wählen Sie die Ereignisse HTTP_REQUEST und HTTP_RESPONSE aus.
4. Geben Sie den folgenden Triggercode in den rechten Bereich ein oder fügen Sie ihn ein.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Weisen Sie den Auslöser einem Gerät oder einer Gruppe von Geräten zu.

   Warnung: Das Ausführen von Triggern auf unnötigen Geräten und Netzwerken erschöpft die Systemressourcen. Minimieren Sie die Auswirkungen auf die Leistung, indem Sie einen Auslöser nur den spezifischen Quellen zuweisen, aus denen Sie Daten erheben müssen.
6. Wählen **Auslöser aktivieren**.
7. Klicken Sie **Speichern**.

Nächste Schritte
Laden Sie die Paketerfassungsdatei herunter.

- Klicken Sie auf RevealX Enterprise-Systemen auf **Rekorde** aus dem oberen Menü. Wählen **Paketerfassung** aus dem Typ des Datensatzes Drop-down-Menü. Nachdem die mit Ihrer PCAP verknüpften Datensätze angezeigt werden, klicken Sie auf das Symbol Pakete, und klicken Sie dann auf **PCAP herunterladen**.
- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen, klicken **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Paketerfassung.

Paketerfassungen anzeigen und herunterladen
Wenn Sie Paketerfassungen auf einer virtuellen Festplatte oder auf einer SSD-Festplatte in Ihrem gespeichert haben Sensor, Sie können diese Dateien auf der Seite „Paketerfassung anzeigen“ in den

Administrationseinstellungen verwalten. Sehen Sie sich für RevealX-Systeme und ExtraHop-Paketstores die Seite Pakete an.

Der Abschnitt Paketerfassungen anzeigen und herunterladen wird nur auf ExtraHop Performance-Systemen angezeigt. Auf RevealX-Systemen werden Precision-Paketerfassungsdateien gefunden, indem Datensätze nach dem Datensatztyp für die PCAP durchsucht werden.

- klicken **Einstellungen für die PCAP konfigurieren** um gespeicherte Paketerfassungen nach der angegebenen Dauer (in Minuten) automatisch zu löschen.
- Sehen Sie sich Statistiken über Ihre Paketerfassungsdiskette an.
- Geben Sie Kriterien zum Filtern von Paketerfassungen an und begrenzen Sie die Anzahl der in der Paketerfassungsliste angezeigten Dateien.
- Wählen Sie eine Datei aus der Paketerfassungsliste aus und laden Sie die Datei dann herunter oder löschen Sie sie.

  Hinweis Sie können keine einzelnen Paketerfassungsdateien von RevealX-Systemen löschen.

Sicherheit der Infrastruktur

Platzieren Sie Verwaltungsschnittstellen immer in sicheren internen Netzwerken, nicht in nicht vertrauenswürdigen Netzwerken, einschließlich des öffentlichen Internets.

Wir empfehlen die folgenden Best Practices:

- Achten Sie darauf Beschränken Sie die ausgehende Konnektivität zu den ExtraHop Cloud Services-IP-Adressen für die spezifische Region, die Ihrer Organisation zugewiesen ist, und erlauben Sie den Zugriff auf diese IP-Adressen nur über HTTPS (TCP 443). Wenn Sie über einen expliziten Proxy eine Verbindung zu ExtraHop Cloud Services herstellen, Sie können den an den Lizenzserver gesendeten Datenverkehr überwachen.
- Konfigurieren Sie Ihre Verwaltungsoberfläche und schränken Sie den Netzwerkzugriff so weit wie möglich ein.
- SSH-Zugriff deaktivieren von den Serviceseiten in den Administrationseinstellungen.

Stellen Sie sicher, dass ExtraHop Konsolen sind mit Sensoren verbunden über HTTPS auf Port 443.

Identitäts- und Zugriffsmanagement

Konfigurieren Sie Best Practices für Benutzer, die Zugriff auf das ExtraHop-System haben.

Authentifizierung

Wir empfehlen, Standardkonten zu deaktivieren oder komplexe Konten zu haben Passwörter nur für Administrator - oder Notfallzugriff und erzwingen Sie SSO-Regeln und LDAP-Gruppen für alle anderen Benutzer.

Konfigurieren Sie Sensoren mit einem Identitätsanbieter, der über starke Authentifizierungsfunktionen wie Zweifaktor- oder Multi-Faktor-Authentifizierung verfügt.

Sie können die sichere Remote-Authentifizierung für Benutzer mit den folgenden Methoden konfigurieren:

- SO SAML
- LDAP

Sie können auch strenger konfigurieren Passwortrichtlinien durch eine globale Richtlinieneinstellung.

Benutzersitzungen

Und es gibt eine Reihe von Optionen für die laufende Konfiguration, die Sie rund um den Ablauf der Sitzung konfigurieren können.

Konfiguration des Ablaufs der Sitzung

Konfigurieren Sie, wie lange ein lokaler Benutzer im ExtraHop-System angemeldet bleiben kann, indem Sie den `session` Abschnitt zur Running Configurations-Datei.

- Die Lebensdauer ist in Sekunden angegeben. Die Standardeinstellung ist `1209600` (2 Wochen).
- Lebenszeiten weniger als `3600` (1 Stunde) werden automatisch eingestellt auf `3600`.
- Die Sitzung kann für bis zu das Doppelte der konfigurierten Lebensdauer konfiguriert werden.

```
"session": {
    "lifetime": 654321
}
```

Ablauf der Remote-Authentifizierungssitzung

Stellen Sie in Sekunden ein, wie lange ein Benutzer mit Fernauthentifizierung am ExtraHop-System angemeldet bleiben kann. Der Standardwert ist `43200` (12 Stunden); mindestens ist `3600` (1 Stunde), maximal ist `86400` (1 Tag).

```
"session": {
    "remote_lifetime": 4800
}
```

Ablauf einer Sitzung im Leerlauf

Konfigurieren Sie die Dauer, für die ein Benutzer angemeldet und inaktiv sein kann, dargestellt durch einen Ganzzahlwert in Sekunden. Wenn die Zeit abgelaufen ist, wird der Benutzer abgemeldet. Wann `idle_lifetime` ist nicht gesetzt, der Standardwert ist `-1`, was auf keinen Timeout im Leerlauf hinweist und unsicher ist.

Wir empfehlen, diesen Wert auf einzustellen `900` Sekunden oder weniger.

```
"session": {
    "idle_lifetime": 900
}
```

API-Schlüssel

API-Schlüssel sind leistungsstark und laufen nie ab, was ein Sicherheitsrisiko darstellen kann. Wir empfehlen Ihnen, dies abzulehnen Generierung von API-Schlüsseln für Benutzer und beschränken Sie den Zugriff auf Administratoren.

Zutrittskontrolle

Privilegien sollten mit den minimalen Zugriffsanforderungen jedes Benutzers zugewiesen werden. Beachten Sie, dass Benutzer mit Administratorrechten das System so neu konfigurieren können, dass es den Empfehlungen in diesem Handbuch nicht mehr entspricht.

Benutzer müssen zugewiesen werden Privilegien bevor sie auf das e+XtraHop-System zugreifen können.

Wirtschaftsprüfung

Die AU-11-Richtlinien schreiben vor, dass Daten 12 Monate lang aktiv und 18 Monate kalt aufbewahrt werden.

Das ExtraHop-System kann konfiguriert, um Audit-Log-Daten zu senden und Systembenachrichtigungen zu einem Remote-Syslog-Server sowie API-Interaktionen exportieren für den Machine Learning-Dienst. Wir empfehlen, einen externen Speicher zu konfigurieren, der es Ihnen ermöglicht, Daten für die erforderliche Zeit aufzubewahren.