Entschlüsseln Sie den Domänenverkehr mit einem Windows-Domänencontroller

Veröffentlicht: 2025-03-27

Das ExtraHop-System kann so konfiguriert werden, dass Domänenschlüssel von einem oder mehreren Domänencontrollern abgerufen und gespeichert werden. Wenn das System verschlüsselten Datenverkehr beobachtet, der den zwischengespeicherten Schlüsseln entspricht, wird der gesamte Kerberos-verschlüsselte Verkehr in der Domäne für unterstützte Protokolle entschlüsselt.

Active Directory ist ein häufiges Ziel von Angreifern, da eine erfolgreiche Angriffskampagne hochwertige Ziele hervorbringt. Kritische Angriffe wie Golden Ticket, PrintNightmare und Bloodhound können durch Kerberos- oder NTLM-Entschlüsselung verdeckt werden. Die Entschlüsselung dieser Art von Datenverkehr kann tiefere Einblicke in Sicherheitserkennungen liefern.

Sie können die Entschlüsselung für eine Person aktivieren Sensor oder durch eine Integration auf RevealX 360. Sie können mehr als eine Domänencontroller-Verbindung von einem Sensor hinzufügen, um den Datenverkehr von mehreren Domänen zu entschlüsseln.

Das System synchronisiert nur Kerberos- und NTLM-Entschlüsselungsschlüssel. Sensoren arbeiten im schreibgeschützten Modus und ändern keine Eigenschaften in der Domäne. Entschlüsselungsschlüssel werden im Sensorspeicher zwischengespeichert und können nicht vom Sensor entfernt werden.

Für die Entschlüsselung müssen die folgenden Anforderungen erfüllt sein:

- Sie müssen über einen Active Directory Directory-Domänencontroller (DC) verfügen, der nicht als schreibgeschützter Domänencontroller (RODC) konfiguriert ist.
- Nur Windows Server 2016, Windows Server 2019 und Windows Server 2022 werden unterstützt.
- Das ExtraHop-System synchronisiert Schlüssel für bis zu 50.000 Konten in einer konfigurierten Domain. Wenn Ihr DC mehr als 50.000 Konten hat, wird ein Teil des Datenverkehrs nicht entschlüsselt.
- Das ExtraHop-System muss den Netzwerkverkehr zwischen dem DC und den angeschlossenen Clients und Servern beobachten.
- Das ExtraHop-System muss über die folgenden Ports auf den Domänencontroller zugreifen können: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC) und TCP-Ports 49152-65535 (RPC-Dynamikbereich).

  ⚠ **Warnung:** Wenn Sie diese Einstellungen aktivieren, erhält das ExtraHop-System Zugriff auf alle Kontoschlüssel in der Windows-Domäne; weitere Informationen finden Sie unter Erforderliche Rechte für die Entschlüsselung. Das ExtraHop-System sollte auf derselben Sicherheitsstufe wie der Domänencontroller bereitgestellt werden. Hier sind einige bewährte Methoden, die Sie berücksichtigen sollten:

  - Beschränken Sie den Endbenutzerzugriff strikt auf Sensoren die mit Zugriff auf den Domänencontroller konfiguriert sind. Erlauben Sie im Idealfall nur Endbenutzern den Zugriff auf ein verbundenes Konsole.
  - Konfiguriere Sensoren mit einem Identitätsanbieter, der über starke Authentifizierungsfunktionen wie Zweifaktor- oder Multi-Faktor-Authentifizierung verfügt.
  - Beschränken Sie den eingehenden und ausgehenden Verkehr zum und vom Sensor nur auf das, was benötigt wird.
  - Beschränken Sie in Active Directory die Logon-Workstations für das Konto so, dass sie nur mit dem Domänencontroller kommunizieren, mit dem das ExtraHop-System konfiguriert ist.

Erforderliche Rechte für die Entschlüsselung

Wir empfehlen, dass Sie in Ihrem Domain-Controller einen dedizierten Benutzer für das ExtraHop-System erstellen. Dieser Benutzer sollte Mitglied der integrierten Administratorgruppe sein. Dadurch wird sichergestellt, dass Administratoren leicht erkennen können, welche Rechte dem ExtraHop-System gewährt wurden.

Wenn das Erstellen eines Benutzers in der Gruppe Administratoren nicht möglich ist, können Sie alternativ einen Benutzer mit den folgenden Rechten auf Domänenebene erstellen:

- Änderungen im Replikationsverzeichnis
- Alle Änderungen im Replikationsverzeichnis
- Änderungen des Replikationsverzeichnisses im gefilterten Satz

Es ist wichtig zu verstehen, dass ein Benutzer mit diesen Rechtestufen im Wesentlichen genauso mächtig ist wie ein Mitglied der integrierten Administratorgruppe für die Domäne. Diese Rechte gewähren Zugriff auf alle Kontoschlüssel in der Windows-Domäne, einschließlich Administratorkonten. Der Besitz eines Kontoschlüssels gewährt dem Eigentümer die Kontrolle über dieses Konto. Daher ist der Zugriff auf Administratorkontoschlüssel praktisch gleichbedeutend damit, ein Administrator zu sein.

Einen Domänencontroller an einen Sensor anschließen

Bevor Sie beginnen
Sie benötigen ein Benutzerkonto bei Setup oder System- und Zugriffsadministrationsrechte auf dem Sensor.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Domänencontroller**.
4. Klicken Sie **Domänencontroller-Verbindung hinzufügen**.
5. Füllen Sie die folgenden Felder aus, um Anmeldedaten für den Microsoft Active Directory-Domänencontroller anzugeben, den Sie mit diesem Sensor verbinden möchten:
   - **Gastgeber:** Der vollqualifizierte Domänenname des Domänencontroller.
   - **Computername (sAMAccountName):** Der Name des Domänencontroller.
   - **Bereichsname:** Der Name des Kerberos-Bereichs, in dem der Domänencontroller autorisiert ist .
   - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domänen-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
   - **Passwort:** Das Passwort des privilegierten Benutzers.
6. Klicken Sie **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
7. Klicken Sie **Speichern**.
   Der Verbindungsstatus und ein Zeitstempel der letzten erfolgreichen Synchronisierung werden angezeigt.

Nächste Schritte

- Klicken Sie **Domänencontroller-Verbindung hinzufügen** um eine Verbindung zu einem anderen Domänencontroller herzustellen.
- Klicken Sie **Benutzeranmeldedaten ändern** von einer gespeicherten Verbindung, um die mit der Verbindung verknüpften Anmeldedaten zu ändern.

- Klicken Sie **Verbindung entfernen** um alle mit der Verbindung verknüpften Anmeldedaten zu löschen und den Domänencontroller vom Sensor zu trennen.

Verbinden Sie einen Domänencontroller mit einem RevealX 360-Sensor

Bevor Sie beginnen
Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf **Entschlüsselung des Microsoft-Protokolls** Kachel.
4. klicken **Anmeldeinformationen hinzufügen**.
5. Füllen Sie die folgenden Felder aus, um Anmeldedaten für den Microsoft Active Directory-Domänencontroller anzugeben, den Sie mit einem RevealX 360-Sensor verbinden möchten:
   - **Gastgeber:** Der vollqualifizierte Domänenname des Domänencontroller.
   - **Computername (sAMAccountName):** Der Name des Domänencontroller.
   - **Bereichsname:** Der Name des Kerberos-Bereichs, in dem der Domänencontroller autorisiert ist .
   - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domänen-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
   - **Passwort:** Das Passwort des privilegierten Benutzers.
6. Wählen Sie im Drop-down-Menü den RevealX 360-Sensor aus, mit dem der Domänencontroller eine Verbindung herstellen soll.
7. klicken **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
8. klicken **Verbinde**.
   Der Verbindungsstatus und ein Zeitstempel der letzten erfolgreichen Synchronisierung werden angezeigt.

Nächste Schritte

- klicken **Domänencontroller-Verbindung hinzufügen** um eine Verbindung zu einem anderen Domänencontroller herzustellen.
- klicken **Benutzeranmeldedaten ändern** von einer gespeicherten Verbindung, um die mit der Verbindung verknüpften Anmeldedaten zu ändern.
- klicken **Anmeldeinformationen löschen** um alle mit der Verbindung verknüpften Anmeldedaten zu löschen und den Domänencontroller vom Sensor zu trennen.

Überprüfen Sie die Konfigurationseinstellungen

Um zu überprüfen, ob das ExtraHop-System in der Lage ist, Datenverkehr mit konfigurierten Domänencontrollern zu entschlüsseln, rufen Sie das integrierte Microsoft Protocol Decryption Dashboard auf, um erfolgreiche Entschlüsselungsversuche zu identifizieren.

Jedes Diagramm im Microsoft Protocol Decryption-Dashboard enthält Visualisierungen der Kerberos-Entschlüsselungsdaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Das Microsoft Protocol Decryption-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsam genutzten Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Microsoft Protocol Decryption-Dashboard und fügen Sie es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Hinweis: Das Microsoft Protocol Decryption-Dashboard kann nur auf einer Konsole angezeigt werden.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Kerberos-Entschlüsselungsversuche

Beachten Sie die Anzahl der Kerberos-Entschlüsselungsversuche in Ihrer Umgebung in den folgenden Diagrammen:

- **Erfolgreiche Kerberos-Entschlüsselungsversuche:** Gesamtzahl der erfolgreichen Kerberos-Entschlüsselungsversuche und deren Zeitpunkt.
- **Gesamtzahl erfolgreicher Versuche:** Gesamtzahl der erfolgreichen Kerberos-Entschlüsselungsversuche.
- **Erfolglose Kerberos-Entschlüsselungsversuche:** Gesamtzahl der erfolglosen Kerberos-Entschlüsselungsversuche und deren Zeitpunkt, aufgeführt nach dem Grund, warum der Versuch fehlgeschlagen ist.
- **Gesamtzahl erfolgloser Versuche:** Gesamtzahl der erfolglosen Kerberos-Entschlüsselungsversuche, aufgelistet nach dem Grund, warum der Versuch fehlgeschlagen ist.

Details zur erfolglosen Kerberos-Entschlüsselung

Beachten Sie die Details zu erfolglosen Kerberos-Entschlüsselungsversuchen in den folgenden Diagrammen:

- **Unbekannte Serverprinzipalnamen:** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines unbekannten Serverprinzipalnamens (SPN) fehlgeschlagen sind, aufgeführt im SPN. Wird als Balkendiagramm und Listendiagramm angezeigt.
- **Ungültige Kerberos-Schlüssel:** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines ungültigen Kerberos-Schlüssels fehlgeschlagen sind, aufgeführt im SPN, der den Versuch unternommen hat. Wird als Balkendiagramm und Listendiagramm angezeigt.
- **Kerberos-Entschlüsselungsfehler :** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines Fehlers fehlgeschlagen sind, aufgeführt im SPN, der den Versuch unternommen hat. Wird als Balkendiagramm und Listendiagramm angezeigt.

Einzelheiten zum Serverprinzipalnamen

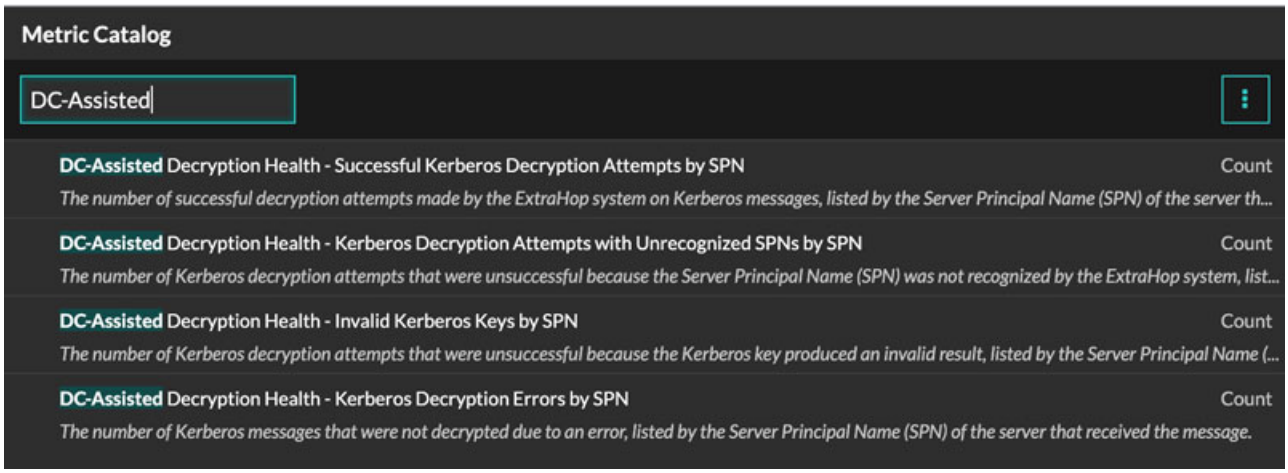
Beachten Sie in den folgenden Diagrammen den wichtigsten SPN, der Kerberos-Entschlüsselungsversuche unternommen hat:

- **Die wichtigsten Serverprinzipalnamen:** Die 50 wichtigsten SPNs, die Kerberos-Entschlüsselungsversuche unternommen haben, und die folgenden Details:
  - Die Anzahl erfolgreicher Entschlüsselungsversuche.
  - Die Anzahl der erfolglosen Versuche aufgrund eines ungültigen Kerberos-Schlüssels.
  - Die Anzahl der erfolglosen Versuche aufgrund eines Fehlers.
  - Die Anzahl der erfolglosen Versuche aufgrund eines unbekannten SPN.

Zusätzliche Metriken zur Systemintegrität

Das ExtraHop-System bietet Metriken, die Sie einem Dashboard hinzufügen können, um den Zustand und die Funktionalität der DC-gestützten Entschlüsselung zu überwachen.

Um eine Liste der verfügbaren Metriken anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Metrischer Katalog**. Typ `DC-unterstützt` im Filterfeld, um alle verfügbaren DC-unterstützten Entschlüsselungsmetriken anzuzeigen.


Metric Catalog
DC-Assisted
DC-Assisted Decryption Health - Successful Kerberos Decryption Attempts by SPN
Count
The number of successful decryption attempts made by the ExtraHop system on Kerberos messages, listed by the Server Principal Name (SPN) of the server th...
DC-Assisted Decryption Health - Kerberos Decryption Attempts with Unrecognized SPNs by SPN
Count
The number of Kerberos decryption attempts that were unsuccessful because the Server Principal Name (SPN) was not recognized by the ExtraHop system, list...
DC-Assisted Decryption Health - Invalid Kerberos Keys by SPN
Count
The number of Kerberos decryption attempts that were unsuccessful because the Kerberos key produced an invalid result, listed by the Server Principal Name (...
DC-Assisted Decryption Health - Kerberos Decryption Errors by SPN
Count
The number of Kerberos messages that were not decrypted due to an error, listed by the Server Principal Name (SPN) of the server that received the message.