Déchiffrez le trafic de domaine à l'aide d'un contrôleur de domaine Windows

Publié: 2024-10-26

Le système ExtraHop peut être configuré pour récupérer et stocker les clés de domaine d'un ou de plusieurs contrôleurs de domaine. Lorsque le système observe un trafic chiffré correspondant aux clés stockées, tout le trafic crypté Kerberos du domaine est déchiffré pour les protocoles pris en charge. Le système synchronise uniquement les clés de déchiffrement Kerberos et NTLM et ne modifie aucune autre propriété du domaine.

Un contrôleur de domaine tel qu'Active Directory est une cible fréquente pour les attaquants, car une campagne d'attaque réussie génère des cibles de grande valeur. Les attaques critiques peuvent être masquées par le déchiffrement Kerberos ou NTLM, comme Golden Ticket, PrintNightmare et Bloodhound. Le déchiffrement de ce type de trafic peut fournir des informations plus détaillées pour les détections de sécurité.

Vous pouvez activer le déchiffrement sur un individu sonde ou via une intégration sur RevealX 360. Vous pouvez ajouter plusieurs connexions de contrôleur de domaine à partir d'une sonde pour déchiffrer le trafic provenant de plusieurs domaines.

Les conditions suivantes doivent être remplies pour le déchiffrement :

- Vous devez disposer d'un contrôleur de domaine Active Directory (DC) qui n'est pas configuré en tant que contrôleur de domaine en lecture seule (RODC).
- Seuls Windows Server 2016, Windows Server 2019 et Windows Server 2022 sont pris en charge.
- Le système ExtraHop synchronise les clés d'un maximum de 50 000 comptes dans un domaine configuré. Si votre DC possède plus de 50 000 comptes, une partie du trafic ne sera pas déchiffrée.
- Le système ExtraHop doit observer le trafic réseau entre le contrôleur de domaine et les clients et serveurs connectés.
- Le système ExtraHop doit pouvoir accéder au contrôleur de domaine via les ports suivants : TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC) et ports TCP 49152-65535 (plage dynamique RPC).

Avertissement Si vous activez ces paramètres, le système ExtraHop a accès à toutes les clés de compte du domaine Windows. Le système ExtraHop doit être déployé au même niveau de sécurité que le contrôleur de domaine. Voici quelques bonnes pratiques à prendre en compte :

- Limiter strictement l'accès des utilisateurs finaux à capteurs qui sont configurés avec un accès au contrôleur de domaine. Idéalement, autorisez uniquement l'accès de l'utilisateur final à un console.
- Configurez capteurs avec un fournisseur d'identité doté de fonctionnalités d'authentification robustes, telles que l'authentification à deux facteurs ou multifacteurs.
- Restreignez le trafic entrant et sortant à destination et en provenance du sonde uniquement pour ce qui est nécessaire.
- Dans Active Directory, limitez le nombre de postes de travail d'ouverture de session pour que le compte communique uniquement avec le contrôleur de domaine avec lequel le système ExtraHop est configuré.

Connecter un contrôleur de domaine à une sonde

Avant de commencer
Vous devez disposer d'un compte utilisateur configuré ou privilèges d'administration du système et des accès sur la sonde.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Contrôleur de domaine**.
4. Cliquez **Ajouter une connexion au contrôleur de domaine**.
5. Renseignez les champs suivants pour spécifier les informations d'identification du contrôleur de domaine Microsoft Active Directory que vous souhaitez connecter à cette sonde :
   - **Hôte:** Le nom de domaine complet du contrôleur de domaine.
   - **Nom de l'ordinateur (SAMAccountName):** Le nom du contrôleur de domaine.
   - **Nom du domaine:** Le nom de domaine Kerberos du contrôleur de domaine.
   - **Nom d'utilisateur:** Nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs du domaine). Pour éviter d' éventuelles erreurs de connexion, spécifiez un compte utilisateur créé après la création du contrôleur de domaine.
   - **Mot de passe:** Le mot de passe de l'utilisateur privilégié.
6. Cliquez **Connexion de test** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
7. Cliquez **Enregistrer**.
   L'état de la connexion et un horodateur de la dernière synchronisation réussie sont affichés.

Prochaines étapes

- Cliquez **Ajouter une connexion au contrôleur de domaine** pour vous connecter à un autre contrôleur de domaine.
- Cliquez **Modifier les informations d'identification des utilisateurs** à partir d'une connexion enregistrée pour modifier les informations dcessaires associées à la connexion.
- Cliquez **Supprimer la connexion** pour supprimer toutes les informations dcessaires associées à la connexion et déconnecter le contrôleur de domaine de la sonde.

Connecter un contrôleur de domaine à une sonde RevealX 360

Avant de commencer
Votre compte utilisateur doit avoir privilèges sur RevealX 360 pour l'administration des systèmes et des accès.

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Intégrations**.
3. Cliquez sur **Décryptage du protocole Microsoft** tuile.
4. Cliquez **Ajouter des informations d'identification**.
5. Renseignez les champs suivants pour spécifier les informations d'identification du contrôleur de domaine Microsoft Active Directory que vous souhaitez connecter à une sonde RevealX 360 :
   - **Hôte:** Le nom de domaine complet du contrôleur de domaine.
   - **Nom de l'ordinateur (SAMAccountName):** Le nom du contrôleur de domaine.
   - **Nom du domaine:** Le nom de domaine Kerberos du contrôleur de domaine.
   - **Nom d'utilisateur:** Nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs du domaine). Pour éviter d' éventuelles erreurs de connexion, spécifiez un compte utilisateur créé après la création du contrôleur de domaine.
   - **Mot de passe:** Le mot de passe de l'utilisateur privilégié.
6. Dans la liste déroulante, sélectionnez la sonde RevealX 360 à laquelle le contrôleur de domaine va se connecter.

7. Cliquez **Connexion de test** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
8. Cliquez **Connecter**.
   L'état de la connexion et un horodateur de la dernière synchronisation réussie sont affichés.

Prochaines étapes

- Cliquez **Ajouter une connexion au contrôleur de domaine** pour vous connecter à un autre contrôleur de domaine.
- Cliquez **Modifier les informations d'identification des utilisateurs** à partir d'une connexion enregistrée pour modifier les informations dcessaires associées à la connexion.
- Cliquez **Supprimer les informations d'identification** pour supprimer toutes les informations dcessaires associées à la connexion et déconnecter le contrôleur de domaine de la sonde.

Validez les paramètres de configuration

Pour vérifier que le système ExtraHop est capable de déchiffrer le trafic avec les contrôleurs de domaine configurés, accédez au tableau de bord intégré de Microsoft Protocol Decryption pour identifier les tentatives de déchiffrement réussies.

Chaque graphique du tableau de bord Microsoft Protocol Decryption contient des visualisations des données de déchiffrement Kerberos qui ont été générées via intervalle de temps sélectionné, organisé par région.

Le tableau de bord Microsoft Protocol Decryption est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord Microsoft Protocol Decryption et ajoutez-le à tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Note: Le tableau de bord Microsoft Protocol Decryption ne peut être consulté que sur une console.

Les informations suivantes résument chaque région et ses graphiques.

Tentatives de déchiffrement Kerberos

Observez le nombre de tentatives de déchiffrement Kerberos dans votre environnement dans les graphiques suivants :

- **Tentatives de déchiffrement de Kerberos réussies:** Nombre total de tentatives de déchiffrement Kerberos réussies et date à laquelle elles se sont produites.
- **Nombre total de tentatives réussies:** Nombre total de tentatives de déchiffrement Kerberos réussies.
- **Tentatives de déchiffrement Kerberos infructueuses:** Nombre total de tentatives de déchiffrement Kerberos infructueuses et date à laquelle elles se sont produites, répertoriées selon la raison de l'échec de la tentative.
- **Nombre total de tentatives infructueuses:** Nombre total de tentatives de déchiffrement Kerberos infructueuses, répertoriées selon la raison de l'échec de la tentative.

Détails du déchiffrement Kerberos ayant échoué

Consultez les graphiques suivants pour en savoir plus sur les tentatives infructueuses de déchiffrement de Kerberos :

- **Noms principaux de serveurs non reconnus:** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'un nom principal de serveur (SPN) non reconnu, répertorié par le SPN. Affiché sous forme de graphique en barres et de graphique en listes.

• **Clés Kerberos non valides:** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'une clé Kerberos non valide, répertorié par le SPN qui a effectué la tentative. Affiché sous forme de graphique en barres et de graphique en listes.

• **Erreurs de déchiffrement Kerberos :** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'une erreur, répertorié par le SPN qui a effectué la tentative. Affiché sous forme de graphique en barres et de graphique en listes.

Détails du nom principal du serveur

Dans les graphiques suivants, observez le SPN ayant effectué le plus de tentatives de déchiffrement avec Kerberos :

• **Principaux noms de serveurs:** Les 50 meilleurs SPN ayant effectué des tentatives de déchiffrement avec Kerberos et les informations suivantes :

- Le nombre de tentatives de déchiffrement réussies.
- Le nombre de tentatives infructueuses dues à une clé Kerberos non valide.
- Le nombre de tentatives infructueuses dues à une erreur.
- Le nombre de tentatives infructueuses dues à un SPN non reconnu.

Autres indicateurs de santé du système

Le système ExtraHop fournit des mesures que vous pouvez ajouter à un tableau de bord pour surveiller l'état et les fonctionnalités du déchiffrement assisté par courant continu.

Pour afficher la liste des mesures disponibles, cliquez sur l'icône Paramètres système puis cliquez sur **Catalogue métrique**. Tapez `Assisté par courant continu` dans le champ de filtre pour afficher toutes les mesures de déchiffrement assistées par courant continu disponibles.