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

Publié: 2024-04-10

Le système ExtraHop peut être configuré pour récupérer et stocker les clés de domaine à partir d'un contrôleur 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 Reveal (x) 360.

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 et Windows Server 2019 sont pris en charge.
- Un seul contrôleur de domaine peut être configuré sur sonde, ce qui signifie que vous pouvez déchiffrer le trafic d'un domaine par sonde.
- 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 DC 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'utilisateur final à accéder 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 **Capture**.
3. Cliquez **Contrôleur de domaine**.
4. Sélectionnez le **Activer la connexion au contrôleur de domaine** case à cocher.
5. Renseignez les champs suivants :
   - **Nom d'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:** Le nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs de 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 **Tester la connexion** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
7. Cliquez **Enregistrer**.

Connecter un contrôleur de domaine à une sonde Reveal (x) 360

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

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Intégrations**.
3. Cliquez sur le **Déchiffrement du protocole Microsoft** tuile.
4. Renseignez les champs suivants pour spécifier les informations dcredentialisation du contrôleur de domaine Microsoft Active Directory que vous souhaitez connecter à une sonde Reveal (x) 360 :
   - **Nom d'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:** Le nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs de 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.
5. Dans la liste déroulante, sélectionnez la sonde Reveal (x) 360 à laquelle le contrôleur de domaine doit se connecter. Un seul contrôleur de domaine peut être connecté à une sonde Reveal (x) 360.
6. Cliquez **Tester la connexion** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
7. Cliquez **Enregistrer**.

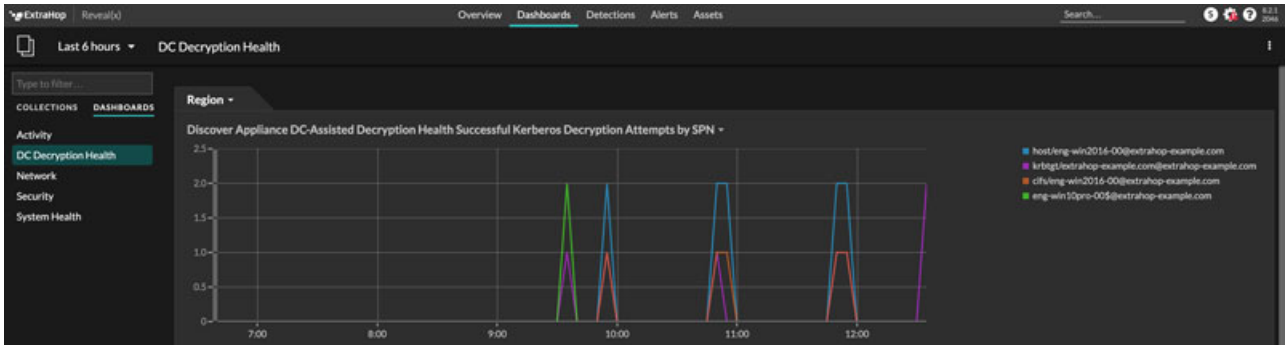
Valider les paramètres de configuration

Pour vérifier que le système ExtraHop est capable de déchiffrer le trafic avec le contrôleur de domaine, créez un tableau de bord qui identifie les tentatives de déchiffrement réussies.

1. Création d'un nouveau tableau de bord.
2. Cliquez sur le widget graphique pour ajouter la source métrique.

3. Cliquez **Ajouter une source**.
4. Dans le champ Sources, saisissez le nom du sonde en communiquant avec un contrôleur de domaine, puis en sélectionnant sonde depuis la liste.
5. Dans le champ Métriques, tapez DC dans le champ de recherche , puis sélectionnez **État du déchiffrement assisté par DC - Tentatives de déchiffrement Kerberos réussies par SPN** .
6. Cliquez **Enregistrer**.

Le graphique affiche le nombre de tentatives de déchiffrement réussies.



Indicateurs de santé supplémentaires du système

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

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