Configuration de l'analyse des fichiers

Publié: 2024-10-26

L'analyse de fichiers vous permet de spécifier les fichiers à hacher à l'aide de l'algorithme de hachage SHA-256. Les hachages de fichiers qui correspondent à une collecte des menaces génèrent une détection, et les données de hachage de fichiers peuvent être interrogées dans des enregistrements.

ExtraHop vous recommande de gérer ces paramètres à partir d'une console ExtraHop, qui est la configuration par défaut de RevealX 360. Pour RevealX Enterprise, les capteurs gèrent ces paramètres par défaut. Si vous préférez gérer les paramètres sur une console plutôt que sur une sonde, vous pouvez transférer la gestion vers une console.

Prérequis

- Vous devez disposer de l'administration du système et des accès ou de l'administration du système (RevealX 360 uniquement) privilèges d'utilisateur.

Configurer une limite de taille pour les filtres de fichiers

Vous pouvez spécifier une limite de taille qui s'applique globalement à tous les filtres de fichiers. Tout fichier dépassant cette limite ne sera pas haché.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Dans le Limite de taille (Mo) champ, spécifiez une taille de fichier, en Mo.
   La plage est comprise entre 1 et 1 000 000 Mo. La valeur par défaut est de 10 Mo.
4. Cliquez **Enregistrer**.

Création d'un filtre de fichiers

Vous pouvez créer des filtres de fichiers personnalisés qui déterminent quels fichiers sont hachés sur le système ExtraHop. Le filtre ExtraHop par défaut est automatiquement activé et configuré pour hacher les fichiers de type multimédia exécutable et les fichiers observés sur tous les protocoles, localités et extensions de fichiers pris en charge par l'analyse des fichiers. Vous pouvez désactiver le filtre par défaut, mais vous ne pouvez pas modifier la configuration du filtre.

Note: L'activation d'un grand nombre de filtres de fichiers personnalisés peut affecter les performances du système.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Dans le Filtres de fichiers section, cliquez sur **Ajouter un filtre**.
4. Dans le Nom champ, entrez un nom unique pour le filtre.
5. À partir du **Protocole** dans la liste déroulante, sélectionnez l'une des options de protocole suivantes :
   - N'importe quel protocole (par défaut)
   - HTTP
   - SMP
   - FTP

   Sélection **N'importe quel protocole** ne permet de hacher que les fichiers observés sur les protocoles HTTP, SMB ou FTP.

6. À partir du **Localité** dans la liste déroulante, sélectionnez l'une des options de direction de flux suivantes :
   - N'importe quelle localité (par défaut)
   - Entrant
   - Interne
   - Sortant
7. Dans le Format de fichier section, sélectionnez le type de fichiers à filtrer :
   - Pour filtrer par type de média, cliquez sur **Type de média**, puis sélectionnez l'une des options multimédia suivantes :
     - Archive
     - Document
     - Exécutable
   - Pour filtrer par extension de fichier, cliquez sur **Extension de fichier**, puis saisissez une ou plusieurs extensions de fichier, en les séparant par une virgule. Vous pouvez saisir des extensions dans l'un des formats suivants : `txt` ou `.txt`.
8. Dans la section Options, sélectionnez **Activer le filtre de fichiers** case à cocher pour activer le filtre et commencer à hacher les fichiers qui correspondent aux critères.
9. Optionnel : Si le filtre de fichiers est activé, vous pouvez sélectionner **Afficher les fichiers hachés dans le tableau Fichiers** case à cocher pour afficher les fichiers hachés et les métadonnées associées dans Tableau des fichiers disponible sur la page Actifs.
10. Cliquez **Enregistrer**.

Gestion du transfert des paramètres d'analyse des fichiers

Pour RevealX 360, les consoles ExtraHop gèrent les paramètres d'analyse des fichiers par défaut. Pour RevealX Enterprise, les capteurs ExtraHop gèrent ces paramètres.

Vous pouvez vous connecter à une console et transférer la gestion des paramètres d'analyse des fichiers vers une sonde, ou vous connecter à une sonde et transférer la gestion vers une console.

Note: Le transfert de la gestion de ces paramètres permet également de transférer la gestion de tous paramètres partagés.

1. Connectez-vous à la console ou à la sonde qui gère actuellement les paramètres d'analyse des fichiers via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Transférez la gestion de l'analyse des fichiers vers un autre système.

Option	Description
Transfert de la sonde à la console	1. Cliquez **Gestion des transferts**. 2. À partir du **Console de gestion** liste déroulante, sélectionnez un nom de console.
Transfert de la console à la sonde	1. Cliquez ***N* de *N* capteurs connectés**. La fenêtre Paramètres de gestion affiche la liste des capteurs dont la console gère les paramètres partagés et une liste des capteurs qui gèrent leurs propres paramètres. 2. Cliquez sur le nom de la sonde dont vous souhaitez gérer ses propres paramètres. 3. Connectez-vous à la sonde. 4. Cliquez **Gestion des transferts**.

Option	Description
	5. À partir du **Console de gestion** liste déroulante, sélectionnez **Appareil à capteur - Self**.