Masquer des détections à l'aide de règles de réglage

Publié: 2023-09-19

Les règles de réglage permettent de masquer les détections qui correspondent à des critères spécifiques.

Pour éviter de créer des règles redondantes, veillez à ajouter d'abord au système ExtraHop des informations sur votre environnement réseau en spécifiant des paramètres de réglage.

En savoir plus sur le réglage des détections.

Créer une règle de réglage

Créez des règles de réglage pour rationaliser votre liste de détection en spécifiant des critères qui masquent les détections passées, présentes et futures de faible valeur et qui ne nécessitent pas d'attention.

Avant de commencer
Les utilisateurs doivent disposer de privilèges d' écriture complets ou supérieurs pour créer une règle de réglage

Bonnes pratiques de réglage.

Ajout d'une règle de réglage à partir d'une carte de détection

Si vous rencontrez une détection de faible valeur, vous pouvez créer une règle de réglage directement à partir d'une carte de détection pour masquer les détections similaires dans le système ExtraHop.

Avant de commencer
Les utilisateurs doivent disposer de privilèges d' écriture complets ou supérieurs pour régler une détection

Bonnes pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez sur **Actions** dans le coin inférieur gauche de la carte de détection.
4. Cliquez sur **Ajuster la détection....**

   Si le type de détection est associé à un paramètre de réglage, vous verrez une option permettant de supprimer la détection. Si vous souhaitez toujours créer une règle de réglage, sélectionnez l'option Hide detections like these... (masquer les détections de ce type) et cliquez sur Save (enregistrer).
5. Spécifiez les critères de la règle de réglage et cliquez sur **Créer**.

   La règle est ajoutée à la page Règles de réglage. En savoir plus sur la gestion des règles de réglage.

Ajouter une règle de réglage à partir d'une détection de renforcement

Cliquez sur une détection de renforcement pour afficher un résumé de tous les actifs, propriétés de détection et localités du réseau associés à ce type de détection. Vous pouvez filtrer le résumé en cliquant sur l'une des valeurs associées, puis créer une règle de réglage pour masquer les détections en fonction des résultats affichés.

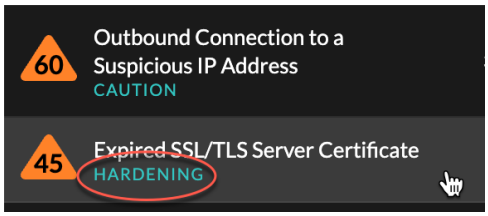
Avant de commencer
Les utilisateurs doivent disposer de privilèges d' écriture complets ou supérieurs pour régler une détection.En savoir plus sur

le filtrage et le réglage des détections de durcissement.

En savoir plus sur les meilleures pratiques de réglage

.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez sur une détection de durcissement dans la liste des détections.



4. Filtrez les résultats sur la page de résumé du durcissement.
   a) Cliquez sur un actif affecté pour afficher uniquement les détections dans lesquelles cet actif participe à une détection.
   b) Cliquez sur une valeur de propriété pour afficher uniquement les détections associées à la valeur de propriété de détection sélectionnée.
   c) Cliquez sur une localité du réseau pour afficher uniquement les détections dont le participant se trouve dans la localité du réseau sélectionnée.
5. Cliquez sur **Créer une règle de réglage**.

   Critères de la règle d'accord Les règles de réglage sont automatiquement remplies pour refléter les résultats filtrés de la page récapitulative du durcissement.
6. Cliquez sur **Créer**.

   La règle est ajoutée à la page Règles de réglage. En savoir plus sur la gestion des règles de réglage.

Ajouter une règle de réglage à partir de la page Règles de réglage

Créez des règles de réglage pour masquer les détections par type de détection, par participant ou par propriétés de détection spécifiques.

Avant de commencer

Les utilisateurs doivent disposer de privilèges d' écriture complets ou supérieurs pour configurer une

détection

Bonnes pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône System Settings (Paramètres système), puis sur **Tuning Rules (Règles d'**accord).
3. Cliquez sur **Create (Créer)**.
4. Spécifiez les critères de la règle de réglage et cliquez sur **Enregistrer**.

   La règle est ajoutée au tableau Règles de réglage. En savoir plus sur .
5. Spécifiez les critères de la règle d'accord et cliquez sur **Créer**.

   La règle est ajoutée à la page Règles de réglage. En savoir plus sur la gestion des règles de réglage.

Critères de la règle d'accord

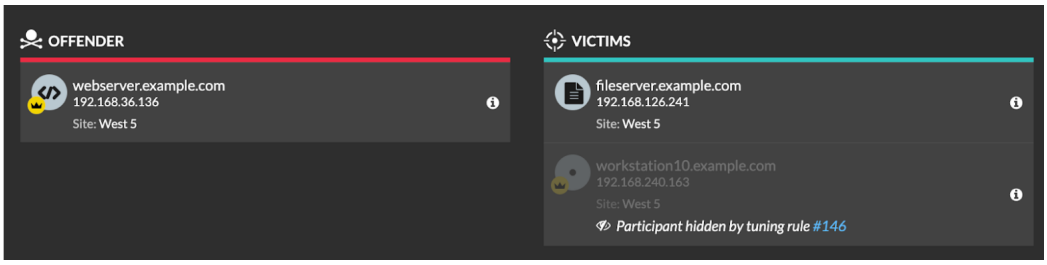
Sélectionnez l'un des critères suivants pour déterminer quelles détections sont masquées par une règle de réglage.

Type de détection

Vous pouvez créer une règle de réglage qui s'applique à un seul type de détection ou choisir d'appliquer la règle à tous les types de détection. Les règles qui englobent tous les types de détection sont généralement réservées aux activités associées aux scanners de vulnérabilité.

Participants

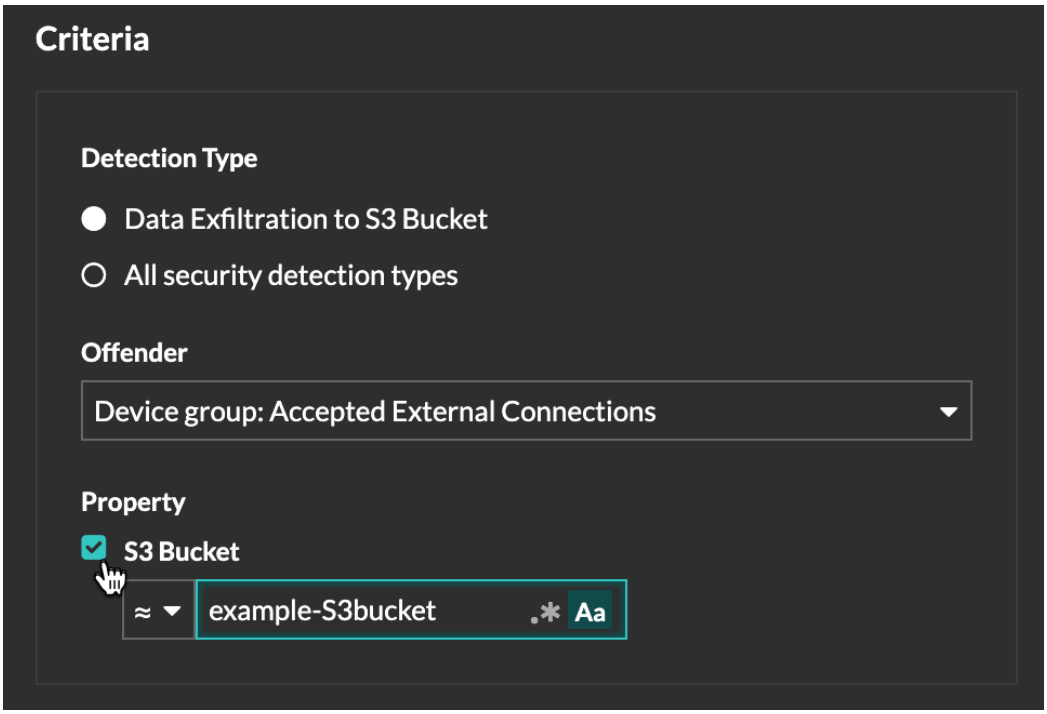
Identifiez les participants à une règle de réglage par adresse IP, nom de périphérique ou localité du réseau. Pour les détections avec plusieurs contrevenants, vous pouvez inclure une liste d'adresses IP ou de blocs CIDR, ou faire référence à un groupe de périphériques. Vous pouvez également créer des règles de réglage qui masquent un seul participant sans masquer l'ensemble de la détection.



Vous pouvez choisir de masquer tous les délinquants ou toutes les victimes. Par exemple, vous pouvez masquer l'auteur d'une détection de balayage bruyant sans tenir compte des participants victimes.

Propriétés de la détection

Créez une règle de réglage qui masque les détections en fonction d'une propriété spécifique. Par exemple, vous pouvez masquer les détections de ports SSH rares pour un seul numéro de port, ou les détections d'exfiltration de données vers un bac S3 pour un bac S3 spécifique.

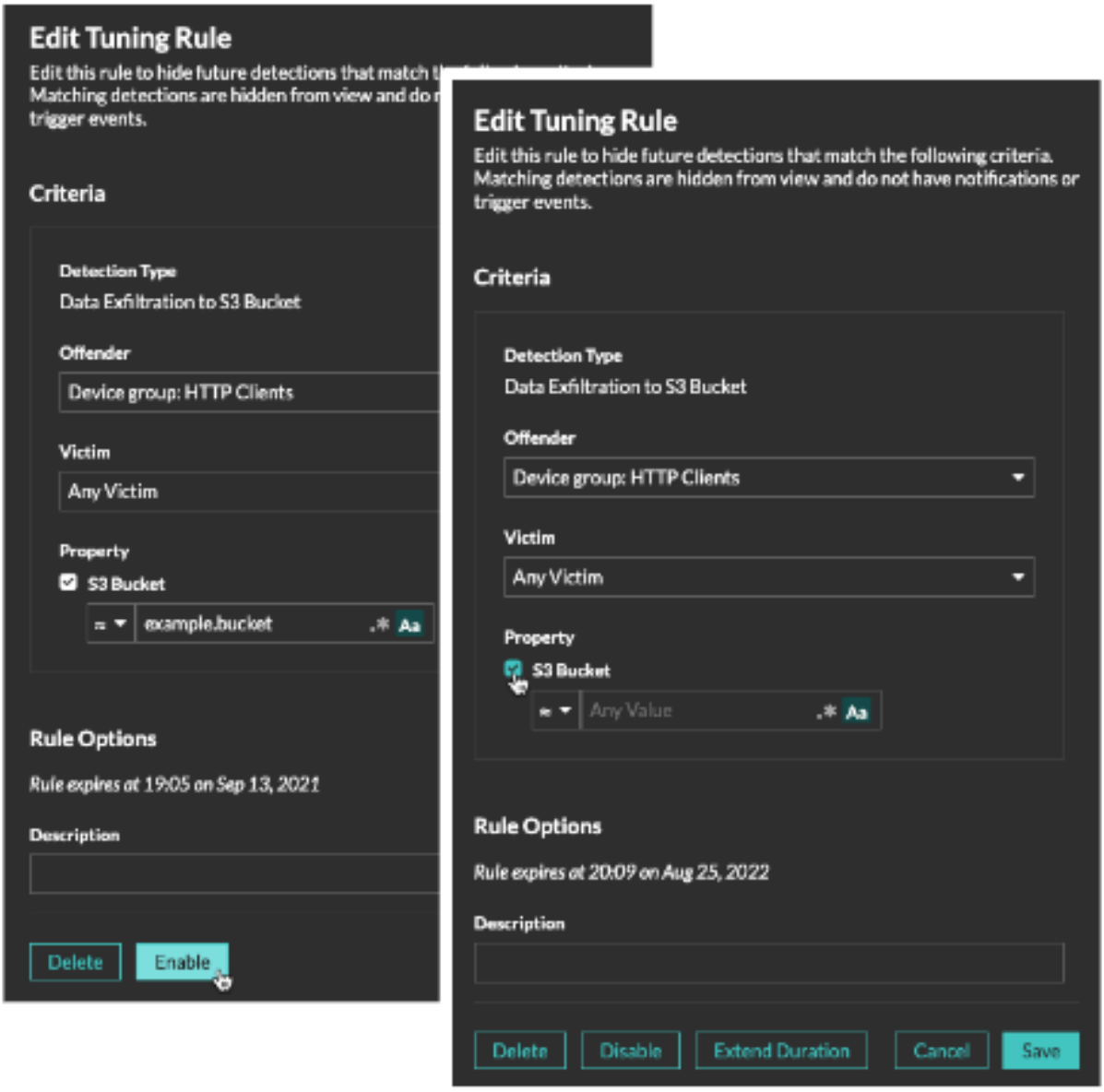


Gérer les règles de réglage

Vous pouvez modifier les critères ou prolonger la durée d'une règle, réactiver une règle et désactiver ou supprimer une règle.

En haut de la page, cliquez sur l'icône Systems Settings et sélectionnez **Tuning Rules**.

Cliquez sur une règle d'accord dans le tableau Règles d'accord pour ouvrir le panneau Modifier la règle d'accord. Mettez à jour les participants, les critères de la règle ou les propriétés pour ajuster la portée de la règle. Cliquez sur les boutons en bas du panneau pour supprimer, désactiver, activer ou prolonger la durée d'une règle.



- Lorsque vous désactivez ou supprimez une règle, celle-ci expire immédiatement et les déclencheurs et alertes associés reprennent.
- Après avoir désactivé une règle, les détections précédemment masquées restent masquées ; les détections en cours apparaissent.

- La suppression d'une règle affiche les détections précédemment masquées.

Vous pouvez afficher temporairement les détections et les participants masqués sur la page Détections en cochant la case **Afficher les détections masquées**, sans désactiver les règles de réglage. Chaque détection ou participant masqué comporte un lien vers la règle de réglage associée et affiche le nom d'utilisateur de l'utilisateur qui a créé la règle. Si la détection ou le participant est masqué par plusieurs règles, le nombre de règles applicables apparaît.