Masquer les détections à l'aide de règles d'exceptions

Publié: 2024-08-08

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

Pour éviter de créer des règles redondantes, assurez-vous d'abord d'ajouter des informations sur votre environnement réseau au système ExtraHop en spécification des paramètres de réglage.

En savoir plus sur détections de réglage.

Création d'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 qui sont de faible valeur et ne nécessitent pas d'attention.

Avant de commencer
Les utilisateurs doivent avoir une écriture complète ou supérieure privilèges pour créer une règle de réglage.

En savoir plus sur meilleures pratiques de réglage.

Ajouter 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 avoir une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur 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 **Actions** depuis le coin inférieur gauche de la carte de détection.
4. Cliquez **Détection des réglages...**.

   Si le type de détection est associé à un paramètre de réglage, vous verrez apparaître une option pour supprimer la détection. Si vous souhaitez toujours créer une règle de réglage, sélectionnez l'option Masquer les détections comme celles-ci... et cliquez sur Enregistrer.
5. Spécifiez le critères des règles de réglage et cliquez **Créez**.

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

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

Cliquez sur une détection renforcée pour afficher un résumé de tous les actifs, propriétés de détection et emplacements 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.

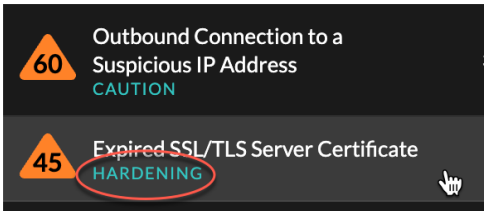
Avant de commencer
Les utilisateurs doivent avoir une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur filtrage et réglage des détections de durcissement.

En savoir plus sur 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 n'importe quelle détection de renforcement dans la liste de détection.



4. Filtrez les résultats sur la page récapitulative du durcissement.
   a) Cliquez sur un actif affecté pour afficher uniquement les détections où 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 où le participant se trouve dans la localité du réseau sélectionnée.
5. Cliquez **Création d'une règle de réglage**.

   Critères des règles de réglage sont automatiquement renseignés pour refléter les résultats filtrés de la page de résumé du durcissement.
6. Cliquez **Créez**.

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

Ajouter une règle de réglage depuis la page Règles de réglage

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

Avant de commencer
Les utilisateurs doivent disposer d'une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur bonnes pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de réglage**.
3. Cliquez **Créez**.
4. Spécifiez critères des règles de réglage et cliquez **Enregistrer**.

   La règle est ajoutée au tableau Règles de réglage.

Critères des règles de réglage

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

Type de détection

Créez une règle de réglage qui s'applique à un seul type de détection ou choisissez de l'appliquer à tous les types de détection de sécurité ou de performance, en fonction du module système. Les règles qui englobent tous les types de détection de sécurité sont généralement réservées aux activités associées aux scanners de vulnérabilités.

Les participants

Créez une règle de réglage qui masque les détections en fonction de participants spécifiques au délinquant et à la victime.

Spécifiez les participants à une règle de réglage à l'aide de l'une des sélections suivantes.

Tout délinquant ou victime

Vous pouvez spécifier N'importe quel délinquant ou N'importe quelle victime pour masquer tous les participants. Cette option est efficace pour masquer les détections lors de tests planifiés ou d'analyses de vulnérabilités.

Groupe d'appareils ou appareils

Vous pouvez spécifier un équipement découvert ou groupe d'équipements pour masquer les participants. Par exemple, vous pouvez spécifier le groupe déquipements intégré pour les scanners de vulnérabilité afin de masquer les détections auxquelles un scanner interne est participant.

Note: Les règles de réglage sont appliquées lorsque des détections ou des règles de réglage sont créées ou mises à jour. Les règles de réglage ne sont pas appliquées rétroactivement aux détections existantes lorsqu'un participant est ajouté ou retiré d'un groupe dequipments dynamique.

Service de numérisation externe

Vous pouvez spécifier un service de numérisation externe en tant que participant à une règle de réglage. Le système ExtraHop masque les services de numérisation externes en fonction de la plage d'adresses IP associée au service.

Adresse IP ou bloc CIDR

Vous pouvez spécifier une adresse IP unique ou un bloc d' adresses IP CIDR pour masquer tout participant compris dans cette plage. Par exemple, si une équipe effectue un test dintrusion sur un sous-réseau spécifique, vous pouvez créer une règle de réglage avec les adresses IP du sous-réseau afin d'éviter un pic de détections liées aux outils d'énumération et de piratage.

Note: Les détections sont masquées en fonction de l'adresse IP au moment de la détection. Étant donné que les adresses IP des appareils découverts et des points de terminaison externes peuvent changer de manière dynamique, la spécification d'une adresse IP unique n'est fiable que si le point de terminaison possède une adresse IP statique.

Nom d'hôte ou domaine

Vous pouvez spécifier un nom d'hôte, un nom de domaine ou une indication de nom de serveur (SNI) pour masquer un participant qui n'a pas été découvert par le système ExtraHop. Si vous spécifiez un nom de domaine, la règle de réglage masquera tous les sous-domaines. Par exemple, si vous créez une règle de réglage avec vendor.com comme délinquant, la règle de réglage masquera les détections avec example.vendor.com comme délinquant. Si vous spécifiez un sous-domaine tel que example.vendor.com, la règle de réglage masquera uniquement les détections où le participant se termine par ce sous-domaine exact. Dans cet exemple, test.example.vendor.com serait masqué mais pas test.vendor.com.

Note: Les règles de réglage ne masqueront pas les appareils découverts par nom d'hôte. Vous pouvez ajouter des appareils découverts en tant que critères de règle de réglage en spécifiant une adresse IP, un équipement ou un groupe déquipements.

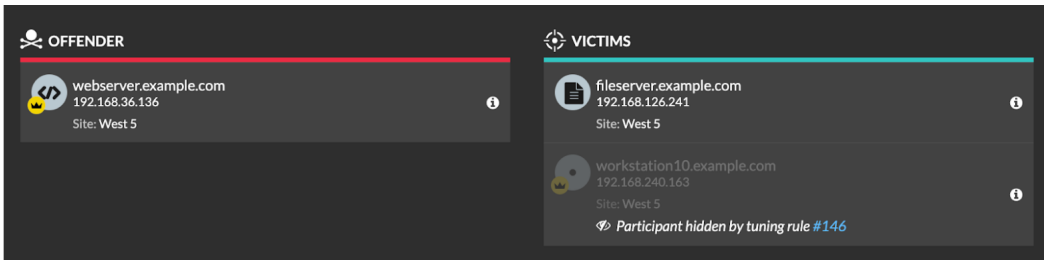
Localité du réseau

Vous pouvez spécifier localité du réseau pour masquer les participants à l'adresse IP de cette localité.

Note: Les règles de réglage masqueront uniquement les participants dont les adresses IP spécifiques sont incluses dans la localité du réseau. Si une autre adresse IP est attribuée à un équipement en dehors du bloc CIDR de localité du réseau, cet équipement ne sera pas masqué.

Voici quelques considérations importantes concernant le réglage des participants :

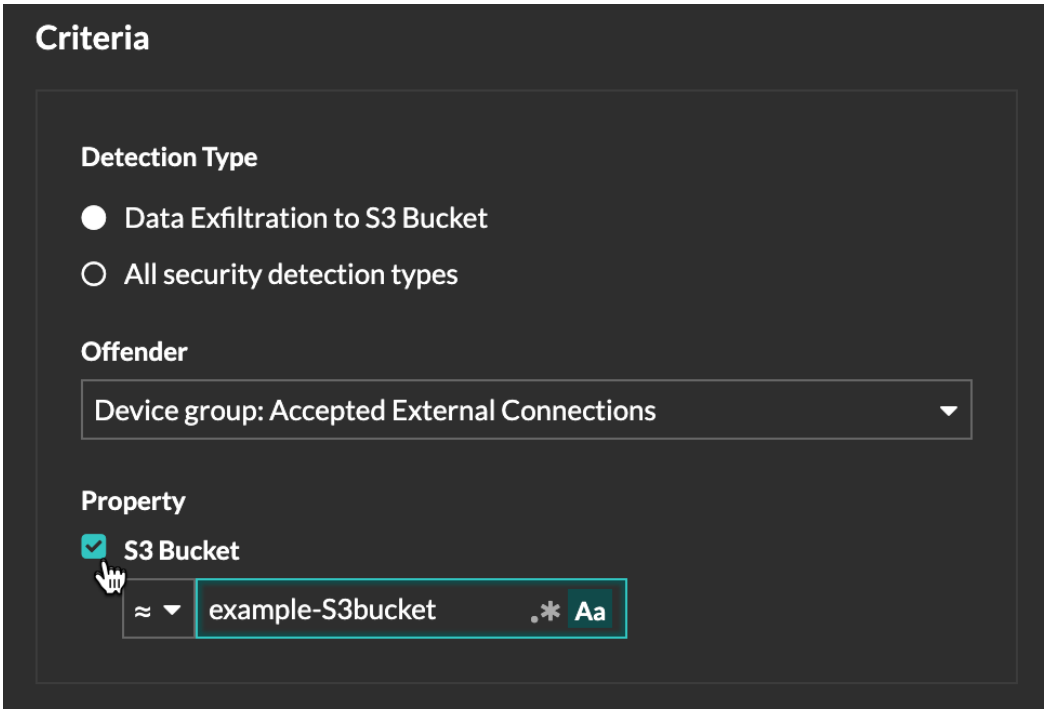
- Lorsque les critères de participation pour une règle de réglage ne correspondent qu'à une partie de la liste des participants d'une détection, le système masque les participants spécifiés dans la règle de réglage sans masquer la totalité de la détection.



- Les participants spécifiés comme critères de réglage, y compris les blocs CIDR et les services d'analyse externes, seront masqués même s'ils se connectent via une passerelle ou un équilibreur de charge.

Propriétés de détection

Créez une règle de réglage qui masque les détections par une propriété spécifique. Par exemple, vous pouvez masquer les détections de ports SSH rares pour un numéro de port unique, ou l'exfiltration de données vers les détections de compartiment S3 pour un compartiment S3 spécifique.



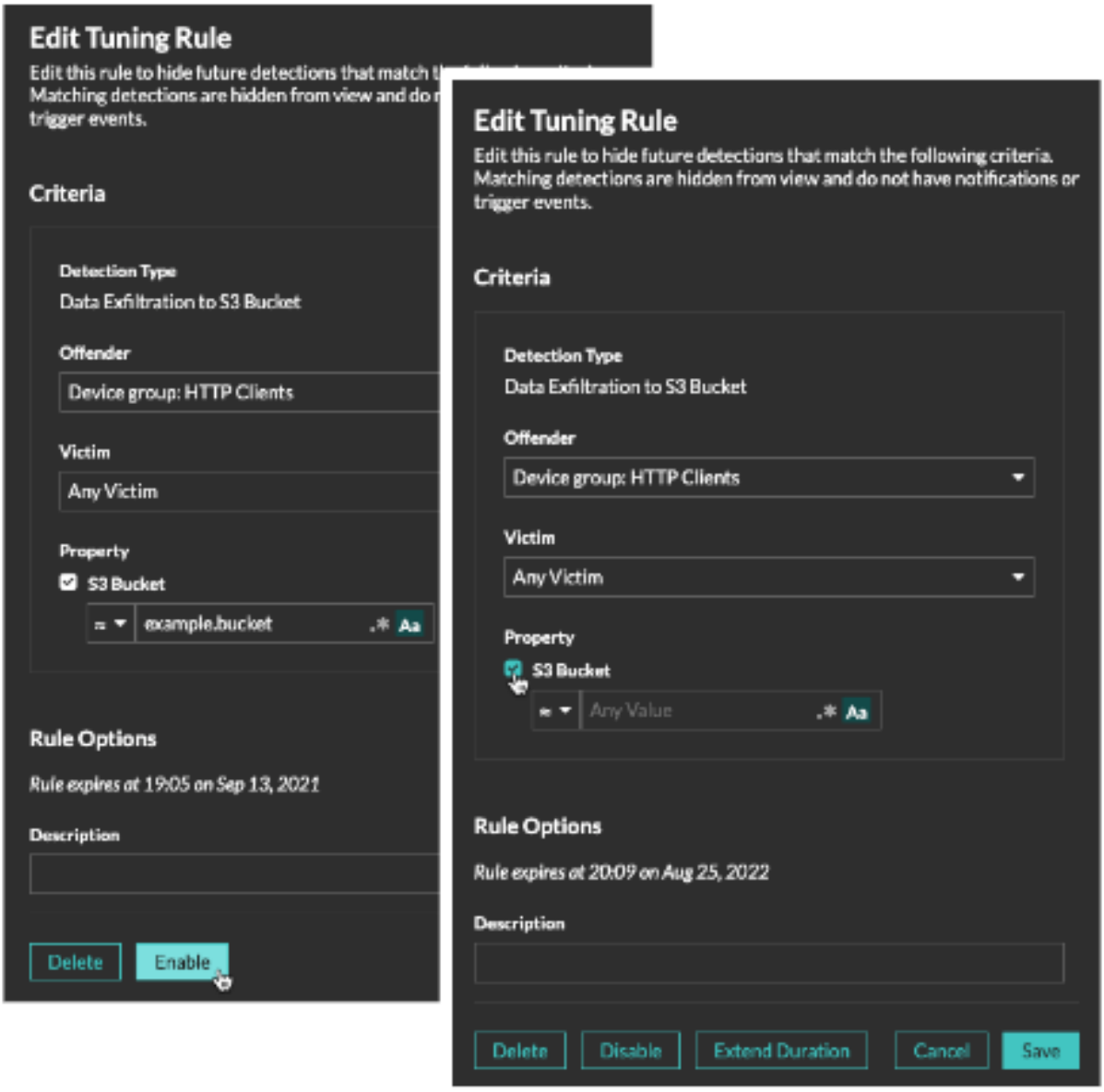
Gérer les règles de réglage

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 Paramètres du système et sélectionnez **Règles de réglage**.

Cliquez sur une règle de réglage dans Règles de réglage table pour ouvrir le Modifier la règle de réglage panneau. Mettez à jour les participants, les critères de règle ou les propriétés pour ajuster la portée de la

règle. Cliquez sur les boutons situés en bas du panneau pour supprimer, désactiver, activer ou prolonger la durée d'une règle.



- Une fois que vous avez désactivé ou supprimé une règle, celle-ci expire immédiatement et les déclencheurs et alertes associés reprennent.
- Une fois que vous avez désactivé une règle, les détections précédemment masquées restent masquées ; les détections en cours apparaissent.
- La suppression d'une règle affiche les détections précédemment masquées.
- Le système ExtraHop supprime automatiquement les détections présentes sur le système depuis 21 jours depuis le début de la détection, qui ne sont pas en cours et qui sont masquées. Si une règle de réglage nouvellement créée ou modifiée masque une détection répondant à ces critères, la détection concernée ne sera pas supprimée pendant 48 heures.

Vous pouvez appliquer le Statut masqué à la page Détections pour afficher uniquement les détections qui sont actuellement masqué par une règle de réglage.

Chaque détection ou participant masqué inclut 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.