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

Publié: 2024-04-10

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 Z.

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 Z.

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 Z.

- 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 Z. 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 Z.

En savoir plus sur meilleures pratiques de réglage Z.

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

En savoir plus sur bonnes pratiques de réglage 2.

- 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.

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.

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

Vous pouvez créer une règle de réglage qui s'applique à un seul type de détection ou choisir 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

Identifiez les participants à une règle de réglage par adresse IP, nom d'hôte ou de domaine, nom d' équipement ou localité du réseau . Vous pouvez également masquer les participants en fonction des rôles identifiés par le système ExtraHop. Par exemple, lorsque le système ExtraHop identifie un service d'analyse externe, vous pouvez masquer les détections pour ce service spécifique ou créer une règle de réglage qui masque tous les services d'analyse externes.

Pour les détections impliquant plusieurs contrevenants, vous pouvez inclure une liste d'adresses IP ou de blocs CIDR, ou référencer un groupe d'équipements. Vous pouvez également créer des règles d'exceptions qui masquent un seul participant sans masquer une détection complète.

		{ <mark>;</mark> → VICTIMS	
webserver.example.com 192.168.36.136 Site: West 5	0	fileserver.example.com 192.168.126.241 Site: West 5	6
		workstation10.example.com 192.168.240.163 Site: West 5 Ø Participant hidden by tuning rule #146	6

Vous pouvez choisir de masquer tous les agresseurs ou toutes les victimes. Par exemple, vous pouvez masquer le délinquant lors d'une détection par balayage bruyant, quels que soient les participants à la victime.

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.

Criteria				
Detection Type				
 Data Exfiltration to S3 Bucket 				
O All security detection types				
Offender				
Device group: Accepted External Connections -				
Property				
S3 Bucket				
≈ ▼ example-S3bucket .* Aa				

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.

Edit Tuning Rule Edit this rule to hide future detections that match the				
Matching detections are hidden from view and do r trigger events.	Edit Tuning Rule			
	Edit this rule to hide future detections that match the following criteria.			
Criteria	Matching detections are nidden from view and do not have notifications or trigger events.			
Detection Type Data Exfiltration to S3 Bucket	Criteria			
Offender	Detection Type			
Device group: HTTP Clients	Data Exfiltration to S3 Bucket			
Victim	Offender			
Any Victim	Device group: HTTP Clients -			
Descrite	Victim			
S S3 Bucket	Any Victim 👻			
a 🕶 example.bucket .* 🗛	Property			
	S3 Bucket			
Pula Online	Any Value .* 🗛			
Rule Options				
Kule expres at 197/9 on sep 13, 2021	Pule Ontions			
Description	Rule emires at 20:09 an Aue 25, 2022			
	Description			
Delete Enable	Description			
	Delete Disable Extend Duration Cancel Save			

- 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.

VPN Client Data Exfiltration EXFILTRATION, ACTIONS ON OBJECTIVE		May 24 08:36 lasting an hour	
🚔 OFFENDER	↔ viстiм		
VPN Client 192166 1845 Site West 5 © Participant hidden by tuning rule #147	0 proxy.example.co 192.168.230.45 Site: West 5 Ø Participant hid	inn Iden by tuning rule #147	
		(+) VICTIMS	
Actions webserver.example 192.168.36.136 Site: West 5	Loom	o fileserver.example.com 192.168.126.241 Site: West 5	0
		workstation 10. example.com 192.168.240.163 Site: West 5 60 Darticipant kiddan hy tuning nde #146	0
highvalue.example.com 192.168.221.82 Site: West 5 Ø Participant hidden by 2 rules	0	Participant moden by tuning rule ≠ 140	