

Détections de syntonisation

Publié: 2024-07-18

Le réglage de la détection vous permet de réduire le bruit et de détecter les détections critiques nécessitant une attention immédiate.

Il existe deux manières de régler les détections : vous pouvez ajouter des paramètres de réglage qui empêchent la génération de détections, ou vous pouvez créer des règles d'exceptions qui masquent les détections existantes en fonction du type de détection, des participants ou des propriétés de détection.

 Consultez la formation associée : [Configurer les règles de réglage](#)


Paramètres de réglage

Les paramètres de réglage vous permettent de spécifier des domaines connus et fiables, des serveurs DNS et des cibles HTTP CONNECT qui ne doivent pas générer de détection. Vous pouvez également activer des paramètres de réglage qui suppriment les détections fréquentes et redondantes associées aux périphériques de passerelle et aux nœuds Tor.

Les paramètres de réglage sont gérés à partir du [Paramètres de réglage](#) page.


Règles de réglage

Les règles de réglage vous permettent de spécifier des critères qui masquent les détections qui ont été générées, mais dont la valeur est faible et qui ne nécessitent aucune attention.

 **Note:** Les règles de réglage peuvent ne pas masquer certaines détections si vos capteurs de paquets n'utilisent pas la même version de microprogramme que celle de votre console.

Les règles de réglage masquent toutes les détections passées, en cours et futures et les participants qui correspondent aux critères spécifiés et affectent les zones système suivantes :

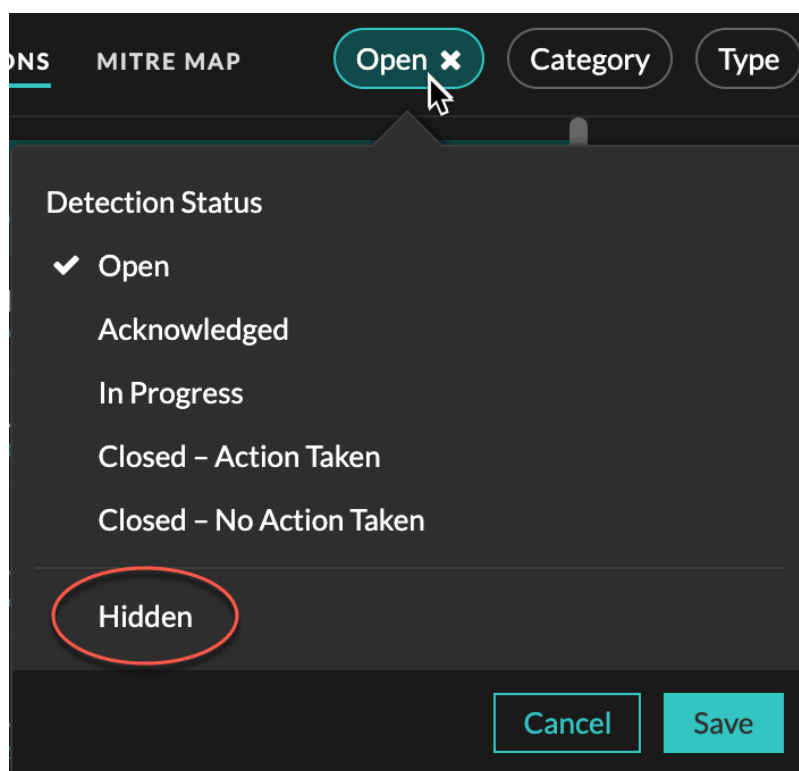
- Les détections masquées n'entraînent pas l'exécution de déclencheurs et d'alertes associés lorsque la règle est activée.
- Les détections masquées n'apparaissent pas en tant que marqueurs de détection dans les graphiques.
- Les détections masquées n'apparaissent pas sur les cartes d'activité, mais les participants cachés apparaîtront sur les cartes d'investigation.
- Les détections masquées n'apparaissent pas dans le nombre de détections sur les pages associées, telles que la page Aperçu de l'appareil ou la page Activité.
- Les détections et les participants masqués n'apparaissent pas dans le rapport sur les opérations de sécurité.
- Les détections masquées ne sont pas incluses dans les notifications par e-mail et par webhook.
- Les détections masquées ne sont pas exportées vers un SIEM ou un SOAR intégré.

 **Note:** Si vous ne voyez aucun marqueur de détection pour une détection, vérifiez que [marqueurs de détection](#) n'ont pas été désactivés.

Afficher les détections masquées

En appliquant le statut Masqué sur la page Détections, vous pouvez afficher les détections actuellement masquées par une règle de réglage.

Le filtre Ouvrir est sélectionné par défaut sur la page Détections. Cliquez sur le **Ouvert** filtre pour accéder à d'autres options de filtrage. Si le filtre Ouvrir n'est pas appliqué, cliquez sur **État** pour afficher les options de filtre, puis cliquez sur **Caché**. Le résumé des détections masquées s'affiche uniquement.



Le résumé identifie les règles de réglage qui masquent actuellement les détections sélectionnées, les participants masqués, les propriétés de détection et les localisations du réseau.

Cliquez sur une règle de réglage, un participant, une propriété ou une valeur de localité du réseau pour afficher un résumé des détections masquées associées à la valeur sélectionnée.

Les participants

Répertorie à la fois les délinquants et les victimes qui sont actuellement masqués. Les listes des délinquants et des victimes sont classées en fonction du nombre de détections où le participant est caché.

Valeurs des propriétés

Répertorie les valeurs des propriétés associées au type de détection masqué. La liste des valeurs de propriété est ordonnée en fonction du nombre de détections où la valeur de propriété est masquée.

Localités du réseau concernées

Répertorie les localités du réseau qui contiennent des détections masquées du type sélectionné . La liste des localités du réseau concernées est ordonnée en fonction du nombre de détections masquées dans la localité du réseau.

En filtrant les résultats pour une seule règle de réglage, un seul participant, une propriété ou une localité, vous pouvez afficher le nombre de détections masquées associées à la valeur spécifiée. Cliquez sur le **Afficher les détections** bouton pour afficher les cartes de détection individuelles.

Meilleures pratiques de réglage

Il est préférable de créer un paramètre ou une règle unique plus large au lieu de créer plusieurs paramètres et règles qui se chevauchent.

Voici quelques recommandations qui vous aideront à optimiser le réglage de votre détection :

- Commencez par ajouter des paramètres de réglage pour éviter les détections impliquant des agents connus ou fiables. N'oubliez pas de consulter le [Paramètres de réglage](#) et [Localités du réseau](#) pages pour les paramètres existants afin d'éviter la redondance.
- Déterminez si vous souhaitez masquer toutes les détections pour un participant spécifique, tel qu'un analyseur de vulnérabilités, et sélectionnez **Tous les types de détection**. Si vous souhaitez masquer les données par rôle d'équipement, augmentez la portée jusqu'à un groupe d'équipements.
- Quand un **Adresse IP ou bloc CIDR** est sélectionné dans la liste déroulante du délinquant ou de la victime, ajoutez ou supprimez des entrées de la liste dans le champ Adresses IP pour augmenter ou réduire la portée de la règle de réglage.
- Par défaut, les règles d'exceptions expirent au bout de 8 heures. Vous pouvez sélectionner un autre délai d'expiration dans la liste déroulante ou sélectionner un nouveau délai d'expiration après avoir réactivé une règle expirée dans le [Règles de réglage](#) page.
- Le système ExtraHop supprime automatiquement les détections qui sont dans le système depuis 21 jours depuis l'heure de début de la détection, qui ne sont pas en cours et qui sont masquées. Si une règle de réglage récemment créée ou modifiée masque une détection qui correspond à ce critère, la détection concernée ne sera pas supprimée pendant 48 heures.
- Lorsque vous ajoutez une règle de réglage, si vous identifiez un équipement qui n'est pas classé correctement, vous pouvez [modifier le rôle de l'équipement](#).
- Certaines détections peuvent nécessiter une règle de réglage précise basée sur une propriété spécifique de la détection. Sous l'en-tête Propriété, cliquez sur la case à cocher à côté d'une propriété pour spécifier une valeur ou une expression régulière et ajouter des critères pour une règle de réglage ciblée.
- Appliquez le **Caché** filtre d'état vers le Détections page pour afficher les détections qui sont **actuellement masqué** par des règles d'exceptions.

Apprenez comment [supprimer les détections à l'aide de paramètres de réglage](#) et [masquer les détections à l'aide de règles de réglage](#).