

Supprimez les détections à l'aide de paramètres de réglage

Publié: 2024-01-31

Fournissez des informations sur votre environnement réseau afin que le système ExtraHop puisse empêcher la génération de détections de faible valeur ou redondantes.

Vous pouvez ajouter des paramètres de réglage à partir du [Paramètres de réglage](#) ou [Localités du réseau](#) pages, ou vous pouvez les ajouter directement depuis une carte de détection. En outre, vous pouvez classer les plages d'adresses IP comme internes ou externes à votre réseau.

En savoir plus sur [détections de réglage](#).



Consultez la formation associée : [Configuration des paramètres de réglage](#)


Spécifier les paramètres de réglage pour les détections et les métriques

Spécifiez les paramètres de réglage pour améliorer les métriques et empêcher la génération de détections de faible valeur.

Si votre déploiement ExtraHop inclut une console, nous vous recommandons [gestion des transferts](#) de tous les capteurs connectés à la console.



Note: Les champs de cette page peuvent être ajoutés, supprimés ou modifiés au fil du temps par ExtraHop.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **Paramètres de réglage**.
3. Spécifiez des valeurs pour l'un des paramètres suivants disponibles sur la page.

Option

Description

Appareils de passerelle

Par défaut, les dispositifs de passerelle sont ignorés par les détections basées sur des règles, car elles peuvent entraîner des détections redondantes ou fréquentes.

Sélectionnez cette option pour identifier les problèmes potentiels liés aux périphériques de passerelle tels que vos pare-feux, routeurs et passerelles NAT.


Nœuds Tor sortants

Par défaut, les connexions sortantes vers des nœuds Tor connus sont ignorées par les détections basées sur des règles, car elles peuvent entraîner des détections de faible valeur dans des environnements où le trafic Tor est minimal.

Sélectionnez cette option pour identifier les détections sur les connexions sortantes vers des nœuds Tor connus si votre environnement observe un trafic Tor sortant important.

Nœuds Tor entrants

Par défaut, les connexions entrantes provenant de nœuds Tor connus sont ignorées par les détections basées sur des règles, car elles peuvent entraîner des détections de faible valeur dans des environnements où le trafic Tor est minimal.

Option	Description
Détection accélérée des balises	<p>Sélectionnez cette option pour identifier les détections sur les connexions entrantes provenant de nœuds Tor connus si votre environnement observe un trafic Tor entrant important.</p> <p>Par défaut, le système ExtraHop détecte les événements de balisage potentiels via HTTP et SSL.</p> <p>Sélectionnez cette option pour détecter les événements de balisage plus rapidement que la détection par défaut.</p> <p>Notez que l'activation de cette option peut augmenter la détection des événements de balisage qui ne sont pas malveillants.</p>
Détections IDS	<p>Par défaut, les systèmes ExtraHop sont connectés Capteurs du système de détection d'intrusion (IDS)  générer uniquement des détections pour le trafic à l'intérieur de votre réseau. Sélectionnez cette option pour générer des détections IDS pour le trafic entrant depuis un point de terminaison externe.</p> <p>Notez que l'activation de cette option peut augmenter considérablement le nombre de détections IDS.</p>
Comptes Active Directory privilégiés	<p>Spécifiez les expressions régulières (regex) qui correspondent aux comptes Active Directory privilégiés de votre environnement. La liste des paramètres inclut une liste par défaut d'expressions régulières pour les comptes privilégiés courants que vous pouvez modifier.</p> <p>Le système ExtraHop identifie les comptes privilégiés et suit l'activité des comptes dans les enregistrements et les statistiques Kerberos.</p>
Serveurs DNS publics autorisés	<p>Spécifiez les serveurs DNS publics autorisés dans votre environnement que vous souhaitez ignorer lors des détections basées sur des règles.</p> <p>Spécifiez une adresse IP ou un bloc CIDR valide.</p>
Cibles HTTP CONNECT autorisées	<p>Spécifiez les URI auxquels votre environnement peut accéder via la méthode HTTP CONNECT.</p> <p>Les URI doivent être formatés comme <code><hostname>: <port number></code>. Les Wildcards et les Regex ne sont pas pris en charge.</p> <p>Si vous ne spécifiez aucune valeur, les détections basées sur ce paramètre ne sont pas générées.</p>

4. Cliquez **Enregistrer**.

Prochaines étapes

Cliquez **Détections** depuis le menu de navigation supérieur vers [afficher les détections](#).

Ajouter un paramètre de réglage ou un domaine sécurisé à partir d'une carte de détection

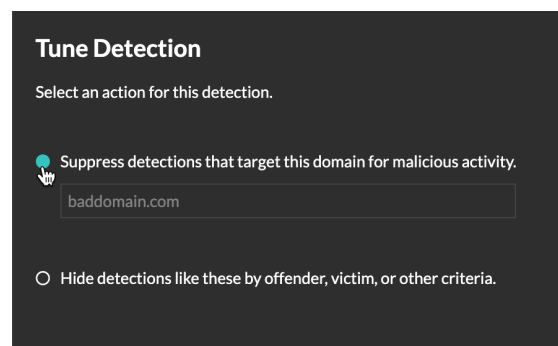
Si vous êtes confronté à une détection de faible valeur, vous pouvez ajouter des paramètres de réglage et des domaines fiables directement à partir d'une carte de détection pour éviter que des détections similaires ne se produisent.

Avant de commencer

Les utilisateurs doivent avoir une écriture complète ou supérieure [privilèges](#) pour régler une détection.

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 pouvez supprimer la détection en ajoutant un paramètre de réglage ou un domaine de confiance. Si aucun paramètre de réglage n'est associé à la détection, vous pouvez [masquer la détection à l'aide d'une règle de réglage](#).



5. Cliquez sur le **Supprimer les détections...** option et cliquez **Enregistrer**.

La confirmation de l'ajout du paramètre de réglage apparaît et le nouveau paramètre est ajouté au [Paramètres de réglage](#) page. Pour les domaines approuvés, le domaine est ajouté sous [Domaines de confiance](#) sur la page Localités du réseau.