

Suppression des détections à l'aide de paramètres de réglage

Publié: 2023-09-19

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

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

Pour en savoir plus sur l'[optimisation des détections](#).

Spécifier des paramètres de réglage pour les détections et les mesures


Spécifiez les paramètres de réglage pour améliorer les mesures et supprimer les détections de faible valeur qui ne sont jamais générées.

Si votre déploiement ExtraHop comprend une console, nous vous recommandons de [transférer la gestion 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 System Settings (Paramètres système) , puis sur **Tuning Parameters (Paramètres de réglage)**.
3. Spécifiez des valeurs pour l'un des paramètres suivants disponibles sur la page.

Option

Description

Périphériques de passerelle

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

. Sélectionnez cette option pour identifier les problèmes potentiels avec les dispositifs de passerelle tels que vos pare-feu, 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 minime

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

.

Option	Description
<p>Nœuds Tor entrants</p>	<p>Par défaut, les connexions entrantes provenant de nœuds Tor connus sont ignorées par les détections basées sur des règles, car elles peuvent donner lieu à des détections de faible valeur dans les environnements où le trafic Tor est minime</p> <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>Détection accélérée des balises</p>	<p>Par défaut, le système ExtraHop détecte les événements de balisage potentiels sur 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>
<p>Détections IDS</p>	<p>Par défaut, les systèmes ExtraHop dotés de capteurs IDS (Intrusion Detection System) connectés ne génèrent des détections que 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>
<p>Comptes Active Directory privilégiés</p>	<p>Spécifiez les expressions régulières (regex) qui correspondent aux comptes Active Directory privilégiés dans votre environnement. La liste des paramètres comprend 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 Kerberos et les métriques.</p>
<p>Serveurs DNS publics autorisés</p>	<p>Indiquez les serveurs DNS publics autorisés dans votre environnement que les détections basées sur des règles doivent ignorer.</p> <p>Indiquez une adresse IP ou un bloc CIDR valide.</p>
<p>Cibles HTTP CONNECT autorisées</p>	<p>Indiquez les URI auxquels votre environnement peut accéder via la méthode HTTP CONNECT.</p>

Option

Description

Les URI doivent être formatés sous la forme `<nom d'hôte>:<numéro de port>`.

Si vous n'indiquez pas de valeur, les détections qui reposent sur ce paramètre ne sont pas générées

4. Cliquez sur **Enregistrer**.

Prochaines étapes

Cliquez sur **Détections** dans le menu de navigation supérieur pour [afficher les détections](#).

Ajout d'un paramètre de réglage ou d'un domaine de confiance à partir d'une carte de détection

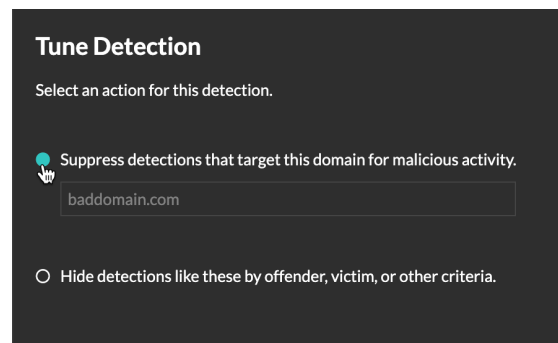
Si vous rencontrez une détection de faible valeur, vous pouvez ajouter des paramètres de réglage et des domaines de confiance directement à partir d'une carte de détection afin d'éviter que des détections similaires ne soient générées.

Avant de commencer

Les utilisateurs doivent disposer de [droits d'écriture complets](#) ou supérieurs 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 sur **Actions** dans le coin inférieur gauche de la fiche de détection.
4. Cliquez sur **Tune Detection...**

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



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

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