Supprimez les détections à l'aide de paramètres de réglage

Publié: 2024-08-09

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 critères à partir du Paramètres de réglage page ou directement depuis une carte de détection. De plus, vous pouvez spécifier les localités du réseau, qui classent les plages d'adresses IP comme internes ou externes à votre réseau.

En savoir plus sur détections de réglage.

Vidéos 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 de 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 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 Gateway	Par défaut, les périphériques 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. Ce paramètre n'affecte pas les détections par apprentissage automatique.
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 avec un trafic Tor 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.

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

Option	Description
	Si vous ne spécifiez aucune valeur, aucune détection basée sur ce paramètre n'est générée.
Domaines fiables	Ajoutez des domaines connus légitimes à la liste des domaines de confiance afin de supprimer les détections futures ciblant des activités malveillantes pour ce domaine. Tapez un seul nom de domaine par champ. Si vous spécifiez un nom de domaine, le paramètre de réglage supprime les détections pour tous les sous-domaines. Par exemple, si vous ajoutez exemple.com en tant que domaine sécurisé, les détections impliquant vendor.example.com comme étant le contrevenant sont également supprimées. Si vous ajoutez un sous-domaine tel que vendor.example.com, le paramètre supprime uniquement les détections où le participant se termine par ce sous-domaine exact. Dans cet exemple, test.vendor.example.com serait supprimé mais pas test.example.com. Les caractères génériques et Regex ne sont pas pris en charge. Pour ajouter plusieurs noms de domaine fiables, cliquez sur **Ajouter un domaine**. Pour les détections associées à un domaine, vous pouvez également ajouter un domaine de confiance directement à partir d'une carte de détection.

4. Cliquez **Enregistrer**.

Prochaines étapes
Cliquez **Détections** depuis le menu de navigation supérieur pour voir les détections.

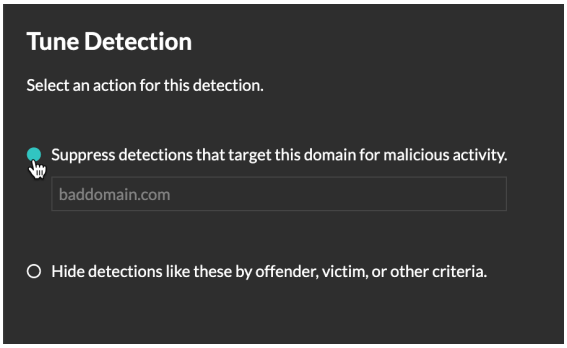
Ajouter un paramètre de réglage à partir d'une carte de détection

Si vous rencontrez une détection de faible valeur, vous pouvez ajouter des paramètres de réglage directement à partir d'une carte de détection pour empêcher la génération de détections similaires.

Avant de commencer
Les utilisateurs doivent disposer d'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, l' option permettant de supprimer la détection en ajoutant un paramètre de réglage s'affiche. 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 **Supprimer les détections...** option et cliquez **Enregistrer**.
   La confirmation de l'ajout d'un paramètre de réglage s'affiche et le nouveau paramètre est ajouté au Paramètres de réglage page.