Unterdrücken Sie Erkennungen mit Optimierungsparametern

Veröffentlicht: 2023-09-13

Stellen Sie Informationen über Ihre Netzwerkumgebung bereit, damit das ExtraHop-System verhindern kann, dass geringwertige oder redundante Erkennungen jemals generiert werden.

Sie können Tuning-Parameter aus dem hinzufügen Tuning-Parameter oder Netzwerk-Lortschaften Seiten, oder Sie können sie direkt von einer Erkennungskarte hinzufügen. Darüber hinaus können Sie IP-Adressbereiche als interne oder externe Bereiche Ihres Netzwerk klassifizieren.

Erfahre mehr über Erkennungen optimieren.

Geben Sie Optimierungsparameter für Erkennungen und Metriken an

Geben Sie Optimierungsparameter an, um die Metriken zu verbessern und zu verhindern, dass Erkennungen mit geringem Wert jemals generiert werden.

Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen Transfermanagement aller an die Konsole angeschlossenen Sensoren.

Hinweis: Die Felder auf dieser Seite können im Laufe der Zeit von ExtraHop hinzugefügt, gelöscht oder geändert werden.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Tuning-Parameter**.
3. Geben Sie Werte für einen der folgenden Parameter an, die auf der Seite verfügbar sind.

Option	Description
Gateway-Geräte	Standardmäßig werden Gateway-Geräte bei regelbasierten Erkennungen ignoriert, da sie zu redundanten oder häufigen Erkennungen führen können. Wählen Sie diese Option, um potenzielle Probleme mit Gateway-Geräten wie Firewalls, Routern und NAT-Gateways zu identifizieren.
Ausgehende Tor-Knoten	Standardmäßig werden ausgehende Verbindungen zu bekannten Tor-Knoten von regelbasierten Erkennungen ignoriert, da sie in Umgebungen mit minimalem Tor-Verkehr zu Erkennungen mit geringem Wert führen können. Wählen Sie diese Option, um Erkennungen bei ausgehenden Verbindungen zu bekannten Tor-Knoten zu identifizieren, wenn Ihre Umgebung erheblichen ausgehenden Tor-Traffic beobachtet.
Eingehende Tor-Knoten	Standardmäßig werden eingehende Verbindungen von bekannten Tor-Knoten von regelbasierten Erkennungen ignoriert, da sie in Umgebungen mit minimalem Tor-Verkehr zu Erkennungen mit geringem Wert führen können.

Option	Description
	Wählen Sie diese Option, um Erkennungen bei eingehenden Verbindungen von bekannten Tor-Knoten zu identifizieren, wenn Ihre Umgebung erheblichen eingehenden Tor-Traffic beobachtet.
Beschleunigte Beaconing-Erkennung	Standardmäßig erkennt das ExtraHop-System potenzielle Beaconing-Ereignisse über HTTP und SSL. Wählen Sie diese Option, um Beaconing-Ereignisse schneller als die Standarderkennung zu erkennen. Beachten Sie, dass die Aktivierung dieser Option die Erkennung von Beaconing-Ereignissen verbessern kann, die nicht böswillig sind.
IDS-Erkennungen	Standardmäßig sind ExtraHop-Systeme mit verbundenen Sensoren des Intrusion Detection Systems (Intrusion Detection System) generieren Sie nur Erkennungen für den Datenverkehr innerhalb Ihres Netzwerk. Wählen Sie diese Option, um IDS-Erkennungen für Datenverkehr zu generieren, der von einem Externer Endpunkt eingeht. Beachten Sie, dass die Aktivierung dieser Option die Anzahl der IDS-Erkennungen erheblich erhöhen kann.
Privilegierte Active Directory Directory-Konten	Geben Sie reguläre Ausdrücke (Regex) an, die privilegierten Active Directory-Konten in Ihrer Umgebung entsprechen. Die Parameterliste enthält eine Standardliste regulärer Ausdrücke für häufig verwendete privilegierte Konten, die Sie bearbeiten können. Das ExtraHop-System identifiziert privilegierte Konten und verfolgt die Kontoaktivitäten in Kerberos-Datensätzen und -Metriken.
Zulässige öffentliche DNS-Server	Geben Sie öffentliche DNS-Server an, die in Ihrer Umgebung zulässig sind und die von regelbasierten Erkennungen ignoriert werden sollen. Geben Sie eine gültige IP-Adresse oder einen gültigen CIDR-Block an.
Zulässige HTTP CONNECT-Ziele	Geben Sie URIs an, auf die Ihre Umgebung über die HTTP CONNECT-Methode zugreifen kann. URIs müssen formatiert sein als *<hostname>:<port number>*. Wildcards und Regex werden nicht unterstützt.

Option	Description
	Wenn Sie keinen Wert angeben, werden Erkennungen, die auf diesem Parameter basieren, nicht generiert.

4. klicken **Speichern**.

Nächste Schritte
klicken **Erkennungen** vom oberen Navigationsmenü zu Erkennungen anzeigen.

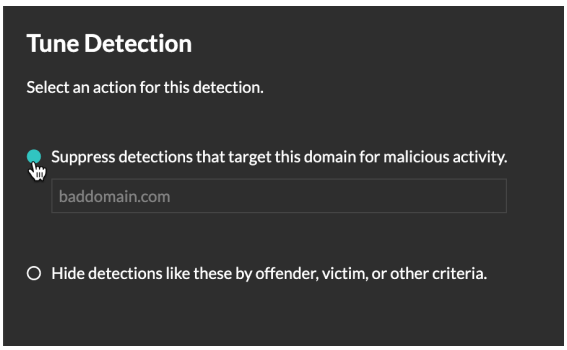
Fügen Sie einen Tuning-Parameter oder eine vertrauenswürdige Domain von einer Erkennungskarte hinzu

Wenn Sie auf eine Erkennung mit geringem Wert stoßen, können Sie Optimierungsparameter und vertrauenswürdige Domänen direkt von einer Erkennungskarte hinzufügen, um zu verhindern, dass ähnliche Erkennungen generiert werden.

Bevor Sie beginnen
Benutzer müssen über Vollschreibzugriff oder höher verfügen Privilegien um eine Erkennung zu optimieren.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. klicken **Erkennung abstimmen...**.

   Wenn der Erkennungstyp mit einem Optimierungsparameter verknüpft ist, wird die Option angezeigt, die Erkennung durch Hinzufügen eines Optimierungsparameters oder einer vertrauenswürdigen Domäne zu unterdrücken. Wenn der Erkennung kein Tuning-Parameter zugeordnet ist, können Sie die Erkennung mit einer Tuning-Regel ausblenden.



5. Klicken Sie auf **Erkennungen unterdrücken...** Option und klicken **Speichern**.

   Die Bestätigung „Tuning-Parameter hinzugefügt“ wird angezeigt und der neue Parameter wird dem Tuning-Parameter Seite. Für vertrauenswürdige Domänen wird die Domain hinzugefügt unter Vertrauenswürdige Domains auf der Seite Network Localities.