Unterdrücken Sie Erkennungen mit Tuning-Parametern

Veröffentlicht: 2024-08-08

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

Sie können Kriterien aus dem Tuning-Parameter Seite oder direkt von einer Erkennungskarte. Darüber hinaus können Sie Netzwerk angeben, die IP-Adressbereiche als interne oder externe Adressbereiche Ihres Netzwerk klassifizieren.

Erfahre mehr über Abstimmung von Erkennungen.

Video: Sehen Sie sich die entsprechende Schulung an: Tuning-Parameter konfigurieren

Geben Sie Optimierungsparameter für Erkennungen und Metriken an

Geben Sie Optimierungsparameter an, um Metriken zu verbessern und zu verhindern, dass Erkennungen mit niedrigen Werten überhaupt 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 klicken Sie dann **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 von regelbasierten Erkennungen ignoriert, da sie zu redundanten oder häufigen Erkennungen führen können. Wählen Sie diese Option, um potenzielle Probleme mit Gateway-Geräten wie Ihren Firewalls, Routern und NAT-Gateways zu identifizieren. Diese Einstellung wirkt sich nicht auf Erkennungen durch maschinelles Lernen aus.
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. Wähle diese Option, um Erkennungen bei ausgehenden Verbindungen zu bekannten Tor-Knoten zu identifizieren, falls deine Umgebung erheblichen ausgehenden Tor-Verkehr beobachtet.

Option	Description
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. Wähle diese Option, um Erkennungen bei eingehenden Verbindungen von bekannten Tor-Knoten zu identifizieren, falls deine Umgebung erheblichen eingehenden Tor-Verkehr 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 bei der Standarderkennung zu erkennen. Beachten Sie, dass die Aktivierung dieser Option die Erkennung von Beaconing-Ereignissen erhöhen kann, die nicht bösartig sind.
IDS-Erkennungen	Standardmäßig sind ExtraHop-Systeme mit verbundenen Sensoren des Intrusion Detection Systems (Intrusion Detection System) generiert nur Erkennungen für den Verkehr 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 allgemeine 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 in Ihrer Umgebung zulässige öffentliche DNS-Server an, die regelbasierte Erkennungen ignorieren sollen. Geben Sie eine gültige IP-Adresse oder einen CIDR-Block an.
Zulässige HTTP CONNECT-Ziele	Geben Sie URIs an, auf die Ihre Umgebung über die HTTP CONNECT-Methode zugreifen kann.

Option	Description
	URIs müssen formatiert sein als *<hostname>:<Portnummer>* . Wildcards und Regex werden nicht unterstützt. Wenn Sie keinen Wert angeben, werden keine Erkennungen generiert, die auf diesem Parameter basieren.
Vertrauenswürdige Domänen	Fügen Sie legitime bekannte Domänen zur Liste der vertrauenswürdigen Domänen hinzu, um zukünftige Erkennungen zu unterdrücken, die auf bösartige Domänenaktivitäten für diese Domain abzielen. Geben Sie einen einzelnen Domänenname pro Feld ein. Wenn Sie einen Domänenname angeben, unterdrückt der Tuning-Parameter Erkennungen für alle Subdomänen. Wenn Sie beispielsweise example.com als vertrauenswürdige Domain hinzufügen, werden Erkennungen mit vendor.example.com als Täter ebenfalls unterdrückt. Wenn Sie eine Subdomain wie vendor.example.com hinzufügen, unterdrückt der Parameter nur Erkennungen, bei denen der Teilnehmer mit genau dieser Subdomain endet. In diesem Beispiel würde test.vendor.example.com unterdrückt werden, test.example.com jedoch nicht. Wildcards und Regex werden nicht unterstützt. Um mehr als einen vertrauenswürdigen Domänenname hinzuzufügen, klicken Sie auf **Domain hinzufügen**. Für Erkennungen, denen eine Domain zugeordnet ist, können Sie auch Fügen Sie eine vertrauenswürdige Domain direkt von einer Erkennungskarte hinzu.

4. Klicken Sie **Speichern**.

Nächste Schritte
Klicken Sie **Erkennungen** vom oberen Navigationsmenü zu Erkennungen anzeigen.

Hinzufügen eines Tuning-Parameters von einer Erkennungskarte

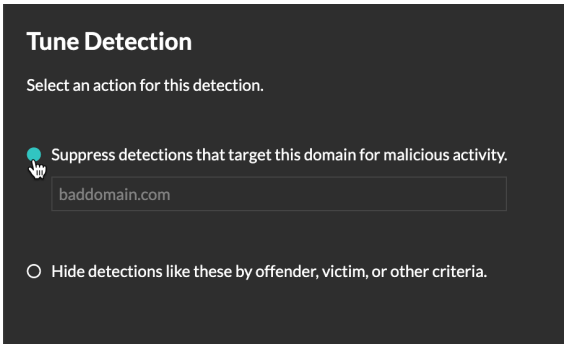
Wenn Sie auf eine Erkennung mit niedrigem Wert stoßen, können Sie direkt von einer Erkennungskarte aus Optimierungsparameter hinzufügen, um zu verhindern, dass ähnliche Erkennungen generiert werden.

Bevor Sie beginnen
Benutzer müssen Vollschreiben oder höher haben 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 Sie **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. Klicken Sie **Tune-Erkennung...**.

   Wenn der Erkennungstyp mit einem Tuning-Parameter verknüpft ist, wird die Option angezeigt, die Erkennung durch Hinzufügen eines Tuning-Parameters 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 klick **Speichern**.

   Die Bestätigung „Tuning-Parameter hinzugefügt“ wird angezeigt und der neue Parameter wird dem Tuning-Parameter Seite.