Erkennungen mit Optimierungsregeln ausblenden

Veröffentlicht: 2024-07-17

Mithilfe von Optimierungsregeln können Sie Erkennungen ausblenden, die bestimmten Kriterien entsprechen.

Um redundante Regeln zu vermeiden, stellen Sie sicher, dass Sie zuerst Informationen über Ihre Netzwerkumgebung zum ExtraHop-System hinzufügen, indem Sie Angeben von Tuning-Parametern.

Erfahre mehr über Abstimmung von Erkennungen.

Eine Optimierungsregel erstellen

Erstellen Sie Optimierungsregeln, um Ihre Erkennungsliste zu optimieren, indem Sie Kriterien angeben, die vergangene, aktuelle und zukünftige Erkennungen verbergen, die von geringem Wert sind und keine Aufmerksamkeit erfordern.

Bevor Sie beginnen
Benutzer müssen über Vollschreibzugriff oder höher verfügen Privilegien um eine Optimierungsregel zu erstellen.

Erfahre mehr über Abstimmung von Best Practices.

Eine Optimierungsregel von einer Erkennungskarte hinzufügen

Wenn Sie auf eine Erkennung mit niedrigem Wert stoßen, können Sie direkt von einer Erkennungskarte aus eine Optimierungsregel erstellen, um ähnliche Erkennungen im ExtraHop-System auszublenden.

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

Erfahre mehr über Abstimmung von Best Practices.

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 Tuning-Parameter verknüpft ist, sehen Sie eine Option zum unterdrücke die Erkennung. Wenn Sie dennoch eine Optimierungsregel erstellen möchten, wählen Sie die Option Erkennungen wie diese ausblenden... und klicken Sie auf Speichern.
5. Spezifizieren Sie die Kriterien Abstimmung Optimierungsregeln und klicken **Erstellen**.

   Die Regel wird der Seite Tuning-Regeln hinzugefügt. Erfahre mehr über Verwaltung von Tuning-Regeln.

Eine Optimierungsregel aus einer Härtungserkennung hinzufügen

Klicken Sie auf eine Hardening-Erkennung, um eine Zusammenfassung aller Ressourcen, Erkennungseigenschaften und Netzwerkstandorte anzuzeigen, die mit diesem Erkennungstyp verknüpft sind. Sie können die Zusammenfassung filtern, indem Sie auf einen der zugehörigen Werte klicken, und dann eine Optimierungsregel erstellen, um Erkennungen auf der Grundlage der angezeigten Ergebnisse auszublenden.

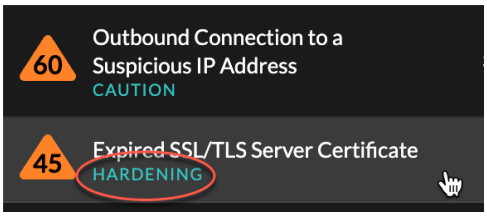
Bevor Sie beginnen

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

Erfahre mehr über Filterung und Abstimmung von Härtungserkennungen.

Erfahre mehr über Abstimmung von Best Practices.

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 in der Erkennungsliste auf eine beliebige Hardening-Erkennung.



4. Filtern Sie die Ergebnisse auf der Seite mit der Zusammenfassung der Härtung.
   a) Klicken Sie auf ein betroffenes Asset, um nur Erkennungen anzuzeigen, bei denen dieses Asset an einer Erkennung Teilnehmer ist.
   b) Klicken Sie auf einen Eigenschaftswert, um nur Erkennungen anzuzeigen, die mit dem ausgewählten Erkennungseigenschaftswert verknüpft sind.
   c) Klicken Sie auf eine Netzwerklokalität, um nur Erkennungen anzuzeigen, bei denen sich der Teilnehmer in der ausgewählten Netzwerklokalität befindet.
5. klicken **Eine Optimierungsregel erstellen**.

   Kriterien für Optimierungsregeln werden automatisch so gefüllt, dass sie die gefilterten Ergebnisse auf der Übersichtsseite zur Härtung widerspiegeln.
6. klicken **Erstellen**.

   Die Regel wird der Seite „Tuning-Regeln“ hinzugefügt. Erfahre mehr über Verwaltung von Tuning-Regeln.

Eine Tuning-Regel von der Seite „Tuning-Regeln“ hinzufügen

Erstellen Sie Optimierungsregeln, um Erkennungen nach Erkennungstyp, Teilnehmer oder bestimmten Erkennungseigenschaften auszublenden.

Bevor Sie beginnen
Benutzer müssen Vollschreiben oder höher haben Privilegien um eine Erkennung zu optimieren.

Erfahre mehr über Abstimmung von Best Practices.

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 auf **Tuning-Regeln**.
3. Klicken Sie **Erstellen**.
4. Spezifizieren Kriterien Abstimmung Optimierungsregeln und klicken Sie **Speichern**.

   Die Regel wird der Tabelle mit den Tuning-Regeln hinzugefügt.

Kriterien für Optimierungsregeln

Wählen Sie aus den folgenden Kriterien aus, um zu bestimmen, welche Erkennungen durch eine Optimierungsregel ausgeblendet werden.

Entdeckungstyp

Erstellen Sie eine Optimierungsregel, die für einen einzelnen Erkennungstyp gilt, oder legen Sie fest, dass die Regel je nach Systemmodul für alle Sicherheits- oder Leistungserkennungstypen gilt. Regeln, die alle Arten von Sicherheitserkennungen umfassen, sind in der Regel für Aktivitäten im Zusammenhang mit Schwachstellenscannern reserviert.

Teilnehmer

Erstellen Sie eine Optimierungsregel, die Erkennungen anhand bestimmter Täter- und Opferteilnehmer verbirgt.

Geben Sie die Teilnehmer an einer Optimierungsregel mit einer der folgenden Optionen an.

Jeder Täter oder Opfer

Sie können Any Offender oder Any Victim angeben, um alle Teilnehmer auszublenden. Diese Option ist effektiv, um Erkennungen während geplanter Tests oder beim Scannen von Schwachstelle auszublenden.

Gerätegruppe oder Gerät

Sie können ein erkanntes Gerät angeben oder Gerätegruppe um Teilnehmer zu verstecken. Sie können beispielsweise die integrierte Gerätegruppe für Vulnerability Scanner angeben, um Erkennungen auszublenden, an denen ein interner Scanner Teilnehmer ist.

Hinweis: Optimierungsregeln werden angewendet, wenn Erkennungen oder Optimierungsregeln erstellt oder aktualisiert werden. Optimierungsregeln werden nicht rückwirkend auf bestehende Erkennungen angewendet, wenn ein Teilnehmer zu einer dynamischen Gerätegruppe hinzugefügt oder daraus entfernt wird.

Externer Scan-Service

Sie können einen externen Scan-Service als Teilnehmer an einer Optimierungsregel angeben. Das ExtraHop-System verbirgt externe Scandienste basierend auf dem mit dem Dienst verknüpften IP-Adressbereich.

IP-Adresse oder CIDR-Block

Sie können eine einzelne IP-Adresse oder einen CIDR-Block von IP-Adressen angeben, um alle Teilnehmer innerhalb dieses Bereichs auszublenden. Wenn ein Team beispielsweise Penetrationstest in einem bestimmten Subnetz durchführt, können Sie eine Optimierungsregel mit den Subnetz-IP-Adressen erstellen, um einen Anstieg der Erkennungen im Zusammenhang mit Aufzählungs- und Hacking-Tools zu vermeiden.

Hinweis: Erkennungen werden basierend auf der IP-Adresse zum Zeitpunkt der Erkennung ausgeblendet. Da sich IP-Adressen für erkannte Geräte und externe Endpunkte dynamisch ändern können, ist die Angabe einer einzelnen IP-Adresse nur dann zuverlässig, wenn der Endpunkt eine statische IP-Adresse hat.

Hostname oder Domain

Sie können einen Hostnamen, Domainnamen oder Server Name Indication (SNI) angeben, um einen Teilnehmer auszublenden, der vom ExtraHop-System nicht erkannt wurde. Wenn Sie einen Domainnamen angeben, blendet die Tuning-Regel alle Subdomains aus. Wenn Sie beispielsweise eine Optimierungsregel mit vendor.com als Täter erstellen, blendet die Optimierungsregel Erkennungen mit example.vendor.com als Täter aus. Wenn Sie eine Subdomain wie example.vendor.com angeben, blendet die Tuning-Regel nur Erkennungen aus, bei denen der Teilnehmer mit genau dieser Subdomain endet. In diesem Beispiel wäre test.example.vendor.com versteckt, test.vendor.com jedoch nicht .

Hinweis: Tuning-Regeln verbergen erkannte Geräte nicht nach Hostnamen. Sie können erkannte Geräte als Optimierungsregelkriterien hinzufügen, indem Sie eine IP-Adresse, ein Gerät oder eine Gerätegruppe angeben.

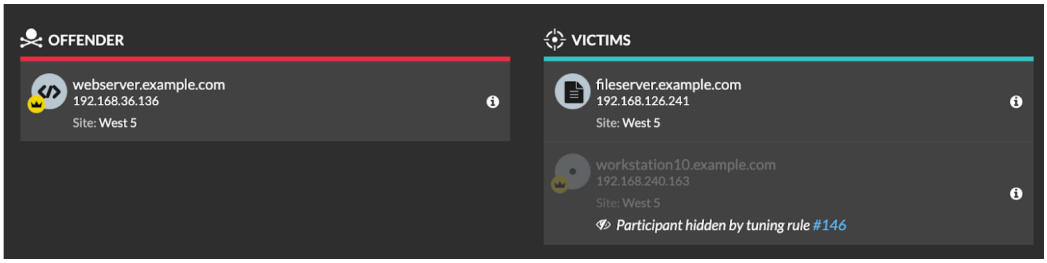
Netzwerk-Lokalität

Sie können eine angeben Netzwerklokalität um IP-Adressteilnehmer an diesem Ort zu verbergen.

Hinweis: Durch Tuning-Regeln werden nur Teilnehmer mit den spezifischen IP-Adressen ausgeblendet , die in der Netzwerklokalität enthalten sind. Wenn einem Gerät eine andere IP-Adresse außerhalb des CIDR-Blocks für den Netzwerkstandort zugewiesen wird, wird dieses Gerät nicht versteckt.

Hier sind einige wichtige Überlegungen zum Abstimmung von Teilnehmern:

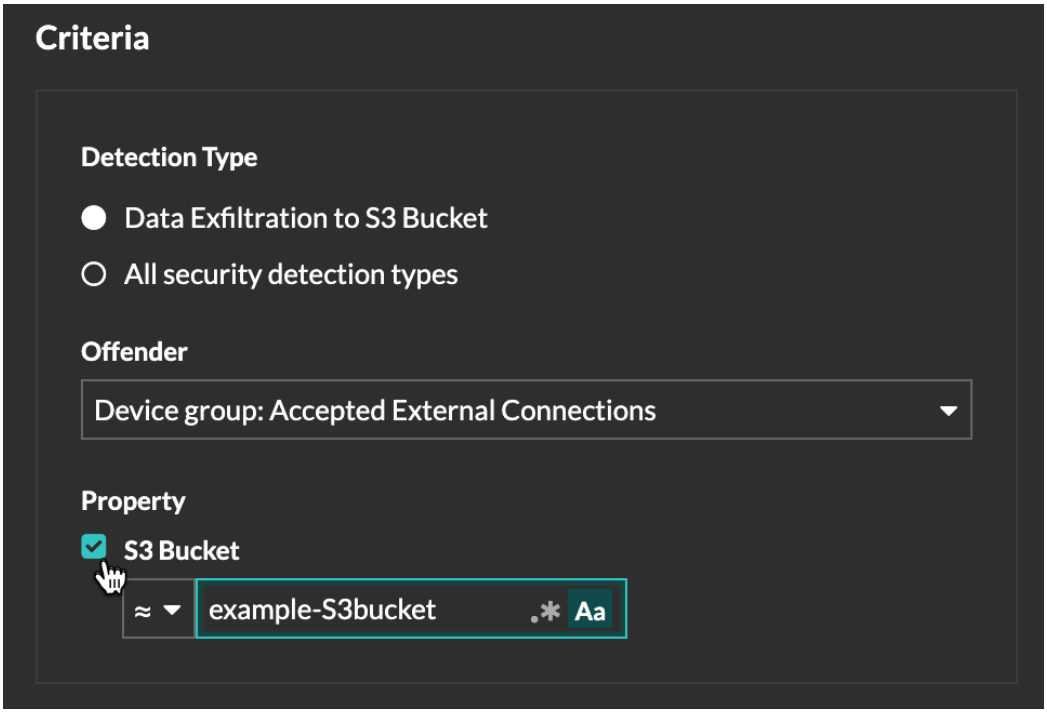
- Wenn die Teilnehmerkriterien für eine Optimierungsregel nur mit einem Teil der Teilnehmerliste einer Erkennung übereinstimmen, blendet das System die in der Optimierungsregel angegebenen Teilnehmer aus, ohne die gesamte Erkennung auszublenden.



- Teilnehmer, die als Optimierungskriterien angegeben sind, einschließlich CIDR-Blöcke und externe Scandienste, werden ausgeblendet, selbst wenn sie sich über ein Gateway oder einen Load Balancer verbinden.

Erkennungseigenschaften

Erstellen Sie eine Optimierungsregel, die Erkennungen anhand einer bestimmten Eigenschaft verbirgt. Sie können beispielsweise seltene SSH-Port-Erkennungen für eine einzelne Portnummer oder Erkennungen von Datenexfiltration in S3-Buckets für einen bestimmten S3-Bucket ausblenden.

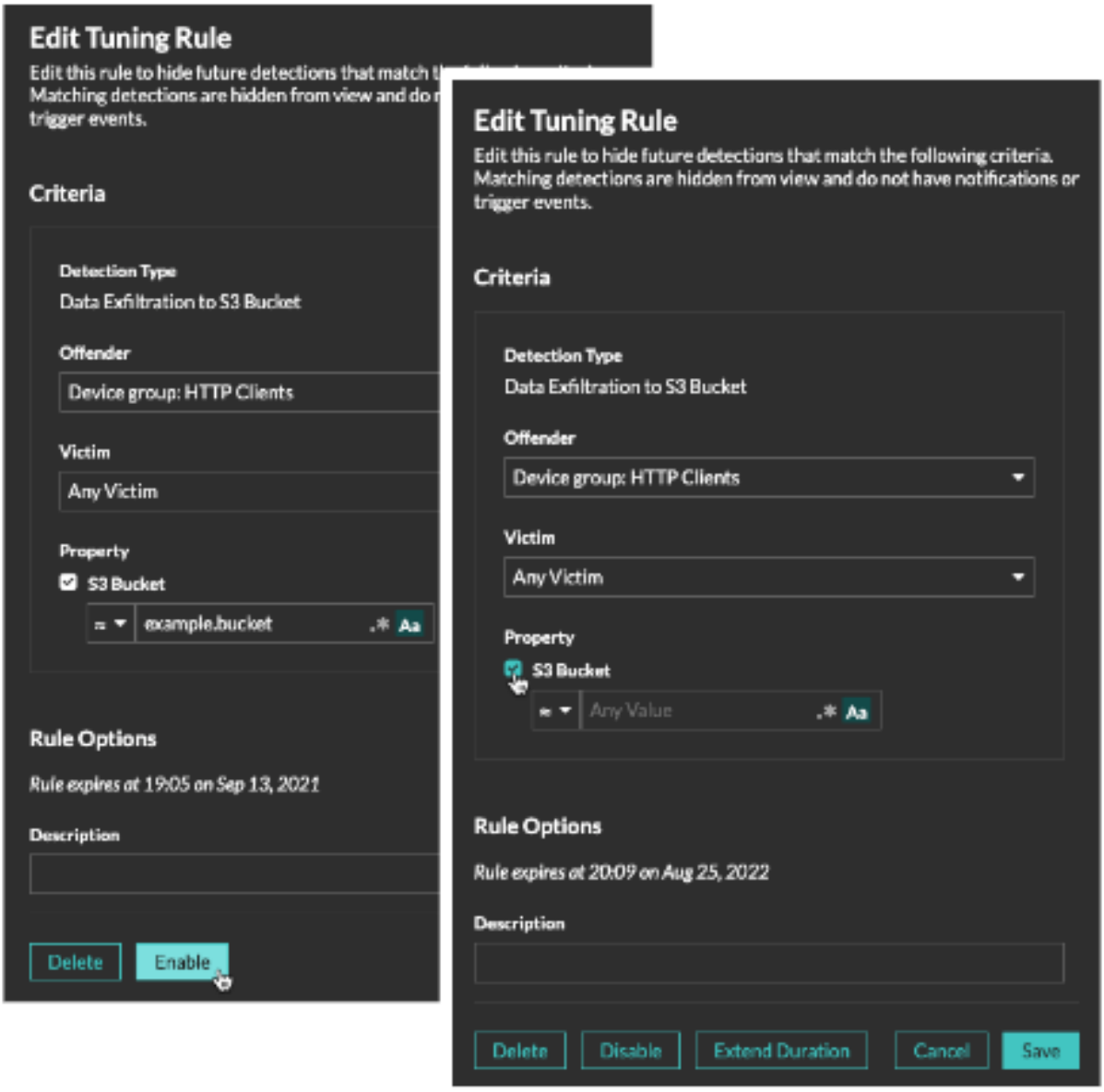


Tuning-Regeln verwalten

Sie können die Kriterien bearbeiten oder die Dauer einer Regel verlängern, eine Regel erneut aktivieren und eine Regel deaktivieren oder löschen.

Klicken Sie oben auf der Seite auf das Symbol Systemeinstellungen ⚙ und wähle **Tuning-Regeln**.

Klicken Sie auf eine Tuning-Regel in der Tuning-Regeln Tabelle zum Öffnen der Optimierungsregel bearbeiten tafel. Aktualisieren Sie Teilnehmer, Regelkriterien oder Eigenschaften, um den Geltungsbereich der Regel anzupassen. Klicken Sie auf die Schaltflächen am unteren Rand des Fensters, um eine Regel zu löschen, zu deaktivieren, zu aktivieren oder die Dauer einer Regel zu verlängern.



- Nachdem Sie eine Regel deaktiviert oder gelöscht haben, läuft die Regel sofort ab und die zugehörigen Auslöser und Benachrichtigungen werden fortgesetzt.
- Nachdem Sie eine Regel deaktiviert haben, bleiben zuvor ausgeblendete Erkennungen verborgen; laufende Erkennungen werden angezeigt.

- Beim Löschen einer Regel werden zuvor ausgeblendete Erkennungen angezeigt.
- Das ExtraHop-System löscht automatisch Erkennungen, die seit dem Startzeitpunkt der Erkennung 21 Tage lang auf dem System waren, die nicht andauern und die versteckt sind. Wenn eine neu erstellte oder bearbeitete Optimierungsregel eine Erkennung verbirgt, die diesen Kriterien entspricht, wird die betroffene Erkennung 48 Stunden lang nicht gelöscht.

Sie können das anwenden Versteckter Status zur Seite Erkennungen, um nur Erkennungen anzuzeigen, die derzeit versteckt durch eine Tuning-Regel.

Jede versteckte Erkennung oder jeder versteckte Teilnehmer enthält einen Link zur zugehörigen Optimierungsregel und zeigt den Benutzernamen des Benutzers an, der die Regel erstellt hat. Wenn die Erkennung oder der Teilnehmer durch mehrere Regeln verdeckt ist, wird die Anzahl der geltenden Regeln angezeigt.