Erkennungen mit Optimierungsregeln ausblenden

Veröffentlicht: 2024-04-10

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.

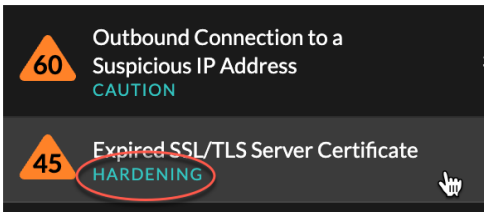
Bevor Sie beginnen

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.

Fügen Sie auf der Seite „Tuning-Regeln“ eine Tuning-Regel hinzu

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

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

Kriterien für Optimierungsregeln

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

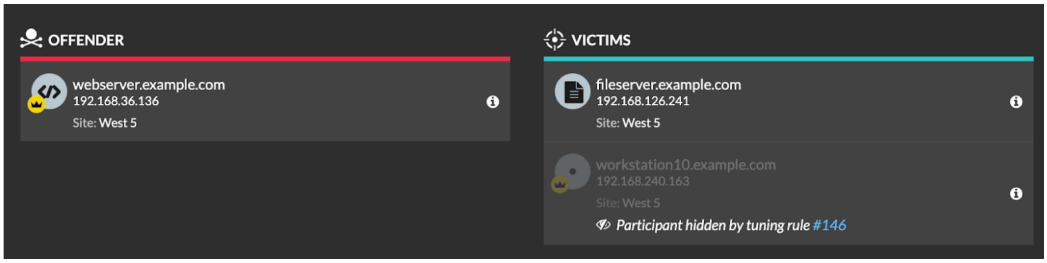
Entdeckungstyp

Sie können eine Optimierungsregel erstellen, die für einen einzelnen Erkennungstyp gilt, oder je nach Systemmodul festlegen, dass die Regel 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

Identifizieren Sie die Teilnehmer an einer Tuning-Regel anhand der IP-Adresse, des Hostnamens oder der Domain, Gerät Gerätenamens oder Netzwerklokalität. Sie können Teilnehmer auch anhand der vom ExtraHop-System identifizierten Rollen ausblenden. Wenn das ExtraHop-System beispielsweise einen externen Scandienst identifiziert, können Sie Erkennungen für diesen bestimmten Dienst ausblenden, oder Sie können eine Optimierungsregel erstellen, die alle externen Scandienste verbirgt.

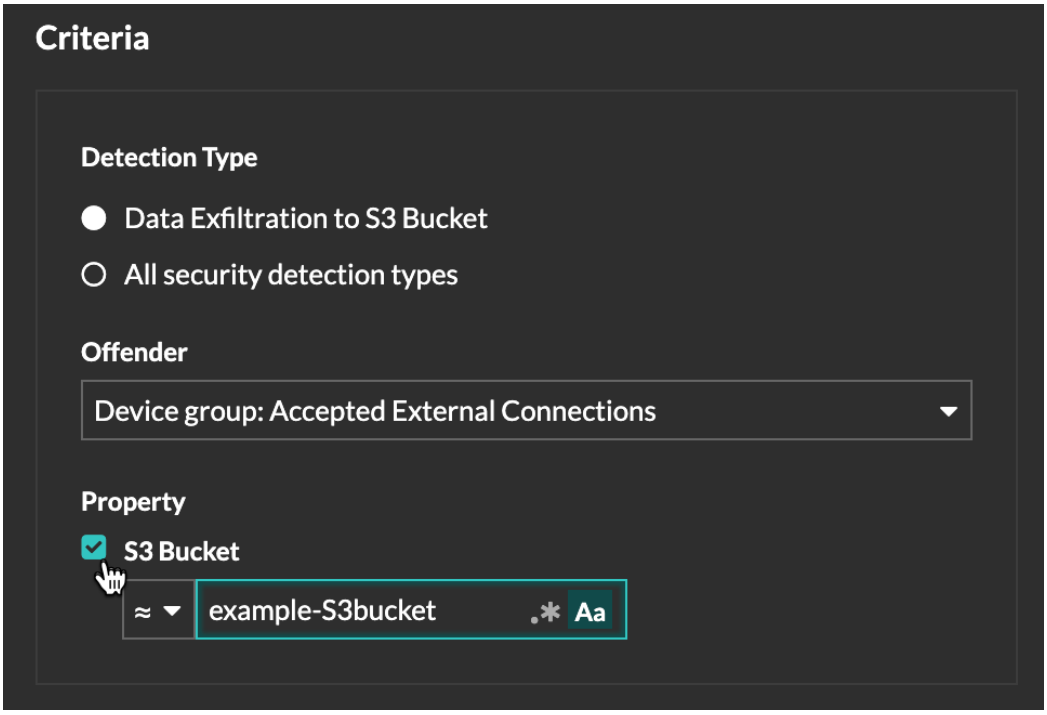
Bei Erkennungen mit mehreren Tätern können Sie eine Liste von IP-Adressen oder CIDR-Blöcken hinzufügen oder auf eine Gerätegruppe verweisen. Sie können auch Optimierungsregeln erstellen, die einen einzelnen Teilnehmer ausblenden, ohne eine gesamte Erkennung zu verbergen.



Sie können wählen, ob Sie alle Täter oder alle Opfer verstecken möchten. Beispielsweise können Sie den Täter bei einer Erkennung von lauten Scans unabhängig von den Teilnehmern des Opfers verstecken.

Erkennungseigenschaften

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

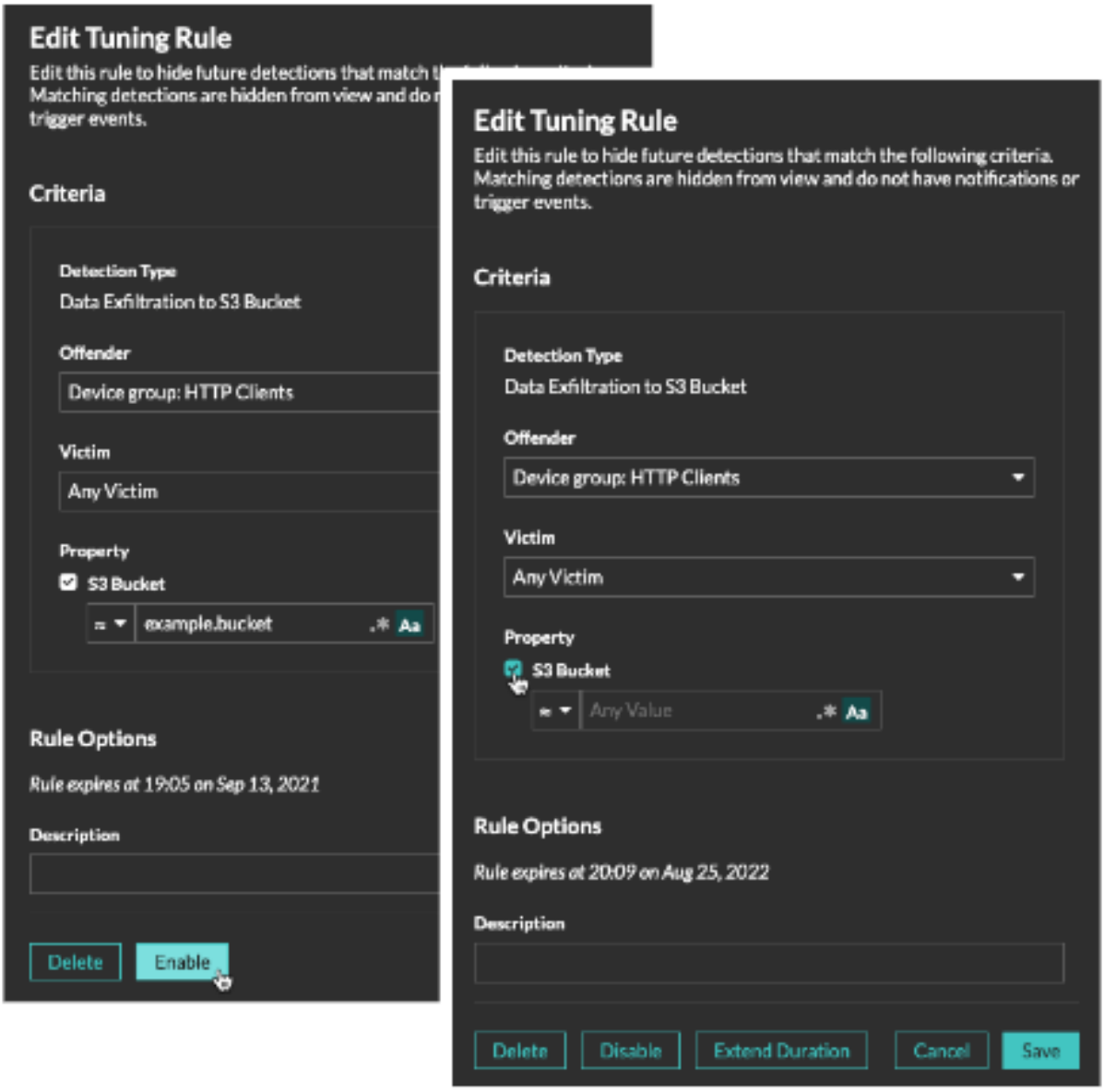


Tuning-Regeln verwalten

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**.

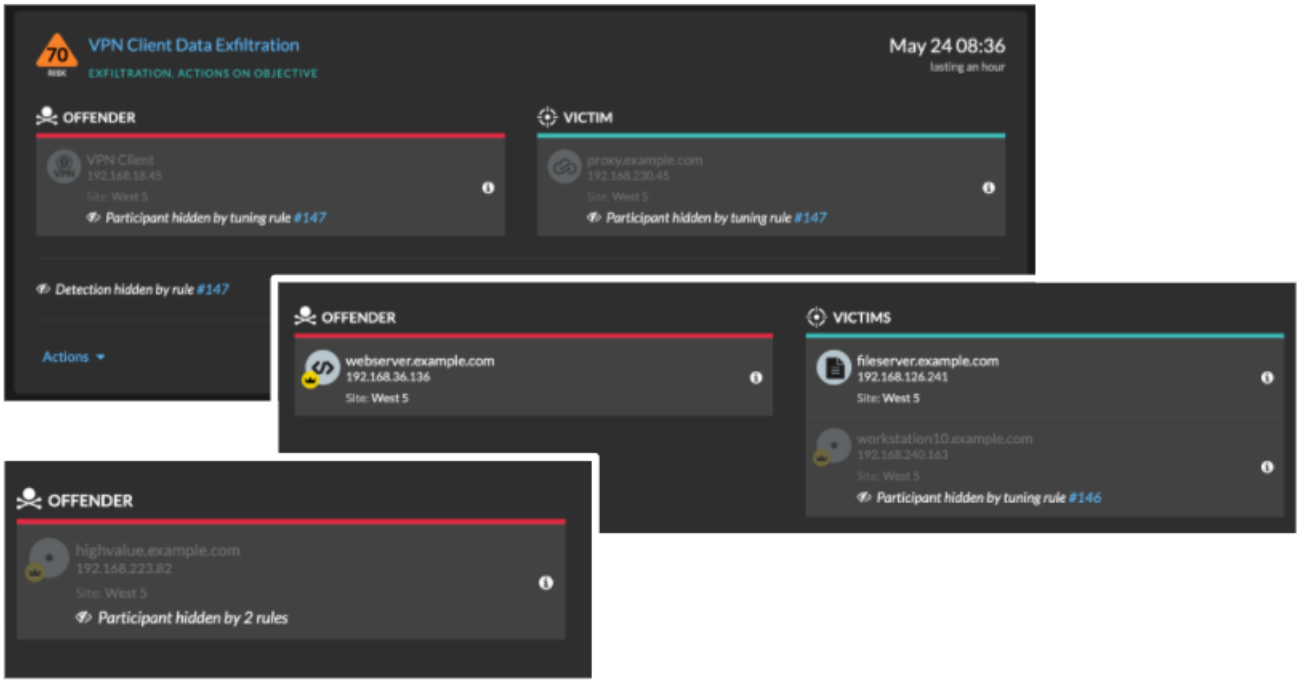
Klicken Sie auf eine Tuning-Regel in der Tuning-Regeln Tabelle zum Öffnen der Optimierungsregel bearbeiten tafel. Aktualisieren Sie Teilnehmer, Regelkriterien oder Eigenschaften, um den Geltungsbereich der Regel anzupassen. Klicken Sie auf die Schaltflächen am unteren Rand des Fensters, um eine Regel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


70
RISK
VPN Client Data Exfiltration
EXFILTRATION, ACTIONS ON OBJECTIVE
May 24 08:36
lasting an hour
OFFENDER
VPN Client
192.168.18.45
Site: West 5
Participant hidden by tuning rule #147
VICTIM
proxy.example.com
192.168.230.45
Site: West 5
Participant hidden by tuning rule #147
Detection hidden by rule #147
Actions
OFFENDER
webserver.example.com
192.168.36.136
Site: West 5
VICTIMS
fileserver.example.com
192.168.126.241
Site: West 5
workstation10.example.com
192.168.240.163
Site: West 5
Participant hidden by tuning rule #146
OFFENDER
highvalue.example.com
192.168.223.82
Site: West 5
Participant hidden by 2 rules