Erkennungen abstimmen

Veröffentlicht: 2024-07-17

Die Erkennungsoptimierung ermöglicht es Ihnen, Geräusche zu reduzieren und kritische Erkennungen zu erkennen, die sofortige Aufmerksamkeit erfordern.

Es gibt zwei Möglichkeiten, Erkennungen zu optimieren: Sie können Optimierungsparameter hinzufügen, die verhindern, dass Erkennungen überhaupt generiert werden, oder Sie können Optimierungsregeln erstellen, die vorhandene Erkennungen basierend auf Erkennungstyp, Teilnehmern oder Erkennungseigenschaften ausblenden.

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

Tuning-Parameter

Mithilfe von Optimierungsparametern können Sie bekannte und vertrauenswürdige Domänen, DNS-Server und HTTP CONNECT-Ziele angeben, die keine Erkennung generieren sollen. Sie können auch Tuning-Parameter aktivieren, die häufige und redundante Erkennungen von Gateway-Geräten und Tor-Knoten unterdrücken.

Die Tuning-Parameter werden über das verwaltet Tuning-Parameter Seite.

Tuning-Regeln

Mithilfe von Optimierungsregeln können Sie Kriterien angeben, die generierte Erkennungen verbergen, die jedoch von geringem Wert sind und keine Aufmerksamkeit erfordern.

Hinweis: Optimierungsregeln verbergen möglicherweise bestimmte Erkennungen nicht, wenn auf Ihren Paketsensoren nicht dieselbe Firmware-Version wie auf Ihrer Konsole ausgeführt wird.

Tuning-Regeln verbergen alle vergangenen, aktuellen und zukünftigen Erkennungen und Teilnehmer, die den angegebenen Kriterien entsprechen und sich auf die folgenden Systembereiche auswirken:

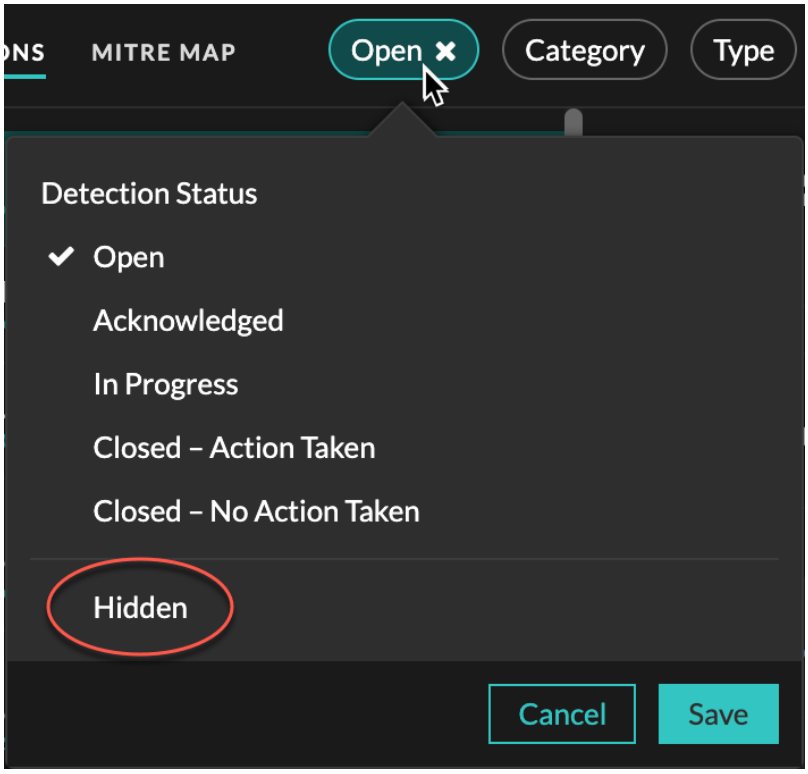
- Versteckte Erkennungen führen nicht dazu, dass zugehörige Trigger und Warnungen ausgeführt werden, solange die Regel aktiviert ist.
- Versteckte Erkennungen werden in Diagrammen nicht als Erkennungsmarkierungen angezeigt.
- Versteckte Entdeckungen erscheinen nicht auf den Aktivitätskarten, aber versteckte Teilnehmer werden auf den Ermittlungskarten angezeigt.
- Versteckte Erkennungen erscheinen nicht in den Erkennungszahlen auf verwandten Seiten, z. B. auf der Seite „Geräteübersicht“ oder der Seite „Aktivität“.
- Versteckte Funde und Teilnehmer erscheinen nicht im Security Operations Report.
- Versteckte Erkennungen sind in E-Mail- und Webhook-Benachrichtigungen nicht enthalten.
- Versteckte Erkennungen werden nicht in ein integriertes SIEM oder SOAR exportiert.

Hinweis: Wenn Sie keine Erkennungsmarkierungen für Erkennungen sehen, bestätigen Sie dies Erkennungsmarker wurden nicht deaktiviert.

Versteckte Entdeckungen anzeigen

Wenn Sie auf der Seite Erkennungen den Status Versteckt anwenden, können Sie Erkennungen anzeigen, die derzeit durch eine Optimierungsregel ausgeblendet sind.

Der Filter Öffnen ist standardmäßig auf der Seite Erkennungen ausgewählt. Klicken Sie auf **Offen** filtern, um auf andere Filteroptionen zuzugreifen. Wenn der Filter Öffnen nicht angewendet wird, klicken Sie auf **Status** um die Filteroptionen anzuzeigen, und klicken Sie dann auf **Versteckt**. Die Zusammenfassung nur für versteckte Entdeckungen wird angezeigt.



Die Zusammenfassung identifiziert die Optimierungsregeln, die derzeit die ausgewählten Erkennungen, versteckten Teilnehmer, Erkennungseigenschaften und Netzwerklokalitäten verbergen.

Klicken Sie auf eine beliebige Optimierungsregel, einen Teilnehmer, eine Eigenschaft oder einen Wert für die Netzwerklokalität, um eine Zusammenfassung der versteckten Erkennungen anzuzeigen, die mit dem ausgewählten Wert verknüpft sind.

Teilnehmer

Listet sowohl Täter als auch Opfer auf, die derzeit versteckt sind. Die Täter- und Opferlisten sind nach der Anzahl der Entdeckungen geordnet, bei denen der Teilnehmer versteckt ist .

Immobilienwerte

Listet die Eigenschaftswerte auf, die dem Erkennungstyp für ausgeblendete Objekte zugeordnet sind. Die Liste der Eigenschaftswerte ist nach der Anzahl der Erkennungen sortiert, bei denen der Eigenschaftswert verborgen ist.

Betroffene Netzwerkstandorte

Führt die Netzwerklokalitäten auf, die versteckte Erkennungen des ausgewählten Typs enthalten. Die Liste der betroffenen Netzwerkorte ist nach der Anzahl der versteckten Entdeckungen in der Netzwerklokalität sortiert.

Indem Sie die Ergebnisse nach einer einzelnen Optimierungsregel, einem einzelnen Teilnehmer, einer Immobilie oder einem Ort filtern, können Sie die Anzahl der versteckten Erkennungen anzeigen, die mit dem angegebenen Wert verknüpft sind. Klicken Sie auf **Erkennungen anzeigen** Schaltfläche, um einzelne Erkennungskarten anzuzeigen.

Optimierte Best Practices

Es ist besser, einen einzelnen Parameter oder eine Regel zu erstellen, die umfassender ist, als mehrere überlappende Parameter und Regeln zu erstellen.

Im Folgenden finden Sie einige Empfehlungen zur Optimierung Ihrer Erkennungsoptimierung:

- Fügen Sie zunächst Optimierungsparameter hinzu, um Erkennungen zu vermeiden, an denen bekannte oder vertrauenswürdige Agenten beteiligt sind. Lesen Sie unbedingt die Tuning-Parameter und Netzwerk-Locations Seiten für bestehende Parameter, um Redundanz zu vermeiden.
- Legen Sie fest, ob Sie alle Erkennungen für einen bestimmten Teilnehmer, z. B. einen Schwachstellenscanner, ausblenden möchten, und wählen Sie **Alle Erkennungsarten**. Wenn Sie sich nach Geräterolle verstecken möchten, erweitern Sie den Bereich auf Gerätegruppe.
- Wenn ein **IP-Adresse oder CIDR-Block** ist in der Dropdownliste Täter oder Opfer ausgewählt. Fügen Sie der Liste im Feld IP-Adressen Einträge hinzu oder entfernen Sie sie, um den Geltungsbereich der Optimierungsregel zu erweitern oder zu reduzieren.
- Standardmäßig laufen Tuning-Regeln nach 8 Stunden ab. Sie können eine andere Ablaufzeit aus der Dropdownliste auswählen oder eine neue Ablaufzeit auswählen, nachdem Sie eine abgelaufene Regel aus dem Tuning-Regeln Seite.
- Das ExtraHop-System löscht automatisch Erkennungen, die seit Beginn der Erkennung 21 Tage im System waren, die nicht andauern und die ausgeblendet sind. Wenn eine neu erstellte oder bearbeitete Optimierungsregel eine Erkennung verbirgt , die diesen Kriterien entspricht, wird die betroffene Erkennung 48 Stunden lang nicht gelöscht.
- Wenn Sie beim Hinzufügen einer Tuning-Regel ein Gerät identifizieren, das nicht korrekt klassifiziert ist, können Sie die Geräterolle ändern.
- Bestimmte Erkennungen erfordern möglicherweise eine genaue Optimierungsregel, die auf einer bestimmten Eigenschaft der Erkennung basiert. Klicken Sie unter der Überschrift Eigenschaft auf das Kontrollkästchen neben einer Eigenschaft, um einen Wert oder regulären Ausdruck anzugeben und Kriterien für eine fokussierte Optimierungsregel hinzuzufügen.
- Wenden Sie das an **Versteckt** Statusfilter zum Erkennungen Seite, um Erkennungen anzuzeigen, die derzeit versteckt indem du Abstimmung optimierst.

Erfahren Sie, wie Unterdrücken Sie Erkennungen mit Tuning-Parametern und Ausblenden von Erkennungen mit Tuning-Regeln.