Erkennungen optimieren

Veröffentlicht: 2023-10-24

Mit der Erkennungsoptimierung können Sie das Rauschen reduzieren und kritische Erkennungen, die sofortige Aufmerksamkeit erfordern, sichtbar machen.

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

Parameter abstimmen

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 im Zusammenhang mit Gateway-Geräten und Tor-Knoten unterdrücken.

Die Tuning-Parameter werden über das verwaltet Parameter abstimmen Seite und vertrauenswürdige Domänen werden von der Seite Network Locations aus verwaltet.

Tuning-Regeln

Mit Optimierungsregeln können Sie Kriterien angeben, die generierte Erkennungen verbergen, die jedoch nur einen geringen Wert haben 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.

Optimierungsregeln verbergen alle vergangenen, aktuellen und zukünftigen Erkennungen und Teilnehmer, die den angegebenen Kriterien entsprechen, und betreffen die folgenden Systembereiche:

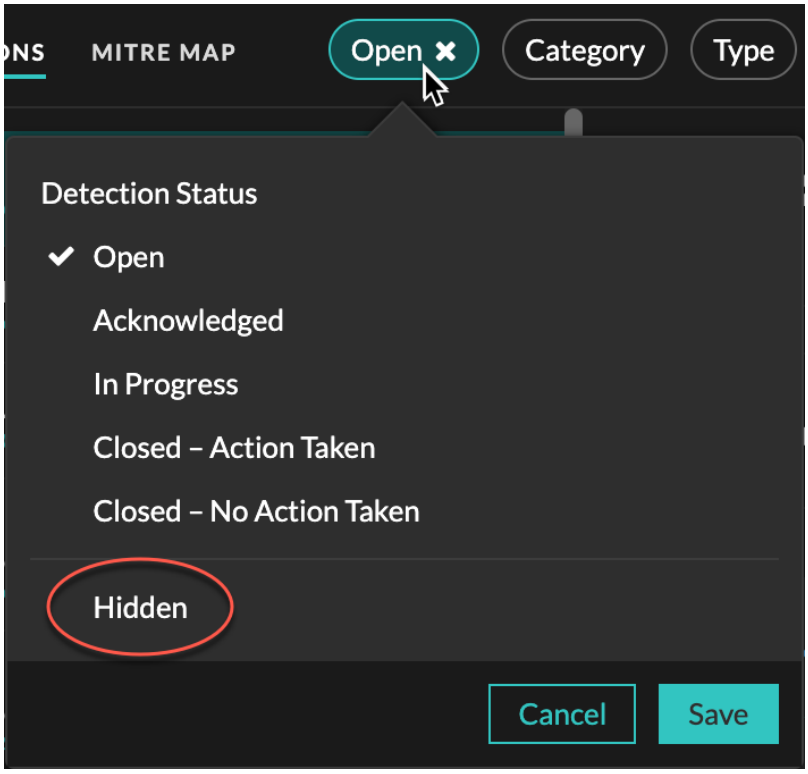
- Versteckte Erkennungen führen nicht dazu, dass entsprechende Auslöser und Warnungen ausgeführt werden, solange die Regel aktiviert ist.
- Versteckte Entdeckungen werden in Diagrammen nicht als Erkennungsmarkierungen angezeigt.
- Versteckte Entdeckungen werden nicht auf Aktivitätskarten angezeigt, aber versteckte Teilnehmer werden auf Ermittlungskarten angezeigt.
- Versteckte Erkennungen werden nicht in der Anzahl der Entdeckungen auf verwandten Seiten angezeigt, z. B. auf der Seite „Geräteübersicht“ oder der Seite „Aktivität“.
- Versteckte Entdeckungen und Teilnehmer erscheinen nicht im Executive Report.
- Versteckte Erkennungen sind nicht in E-Mail- und Webhook-Benachrichtigungen enthalten.

Hinweis: Wenn Sie keine Erkennungsmarkierungen für Erkennungen sehen, bestätigen Sie, dass 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 Vorgehensweisen

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

Im Folgenden finden Sie einige Empfehlungen zur Optimierung Ihrer Erkennungseinstellungen:

- Fügen Sie zunächst Optimierungsparameter hinzu, um Erkennungen zu vermeiden, an denen bekannte oder vertrauenswürdige Agenten beteiligt sind. Lesen Sie unbedingt die Tuning-Parameter und Netzwerkstandorte Seiten für bestehende Parameter, um Redundanz zu vermeiden.
- Stellen Sie fest, ob Sie alle Erkennungen für einen bestimmten Teilnehmer, z. B. einen Schwachstellenscanner, verbergen möchten, und wählen Sie **Alle Erkennungsarten**. Wenn Sie sich nach Geräterolle verstecken möchten, erhöhen Sie den Bereich auf Gerätegruppe.
- Wenn ein **IP-Adresse oder CIDR-Block** ist in der Dropdownliste Täter oder Opfer ausgewählt. Fügen Sie Einträge zur Liste im Feld IP-Adressen hinzu oder entfernen Sie sie, um den Geltungsbereich der Optimierungsregel zu erweitern oder zu reduzieren.
- Standardmäßig laufen Optimierungsregeln nach 8 Stunden ab. Sie können eine andere Ablaufzeit aus der Dropdownliste auswählen oder eine neue Ablaufzeit auswählen, nachdem Sie eine abgelaufene Regel erneut aktiviert haben, aus der Tuning-Regeln Seite.
- 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.
- Wenn Sie beim Hinzufügen einer Optimierungsregel ein Gerät identifizieren, das nicht korrekt klassifiziert ist, können Sie Ändern Sie die Geräterolle.
- 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 einen regulären Ausdruck anzugeben und Kriterien für eine gezielte Optimierungsregel hinzuzufügen.
- Wenden Sie das an **Versteckt** Statusfilter für Erkennungen Seite zum Anzeigen von Erkennungen, die derzeit versteckt durch Tuning-Regeln.

Erfahren Sie, wie Unterdrücken Sie Erkennungen mit Optimierungsparametern und Erkennungen mit Optimierungsregeln ausblenden.