Bedrohungsinformationen

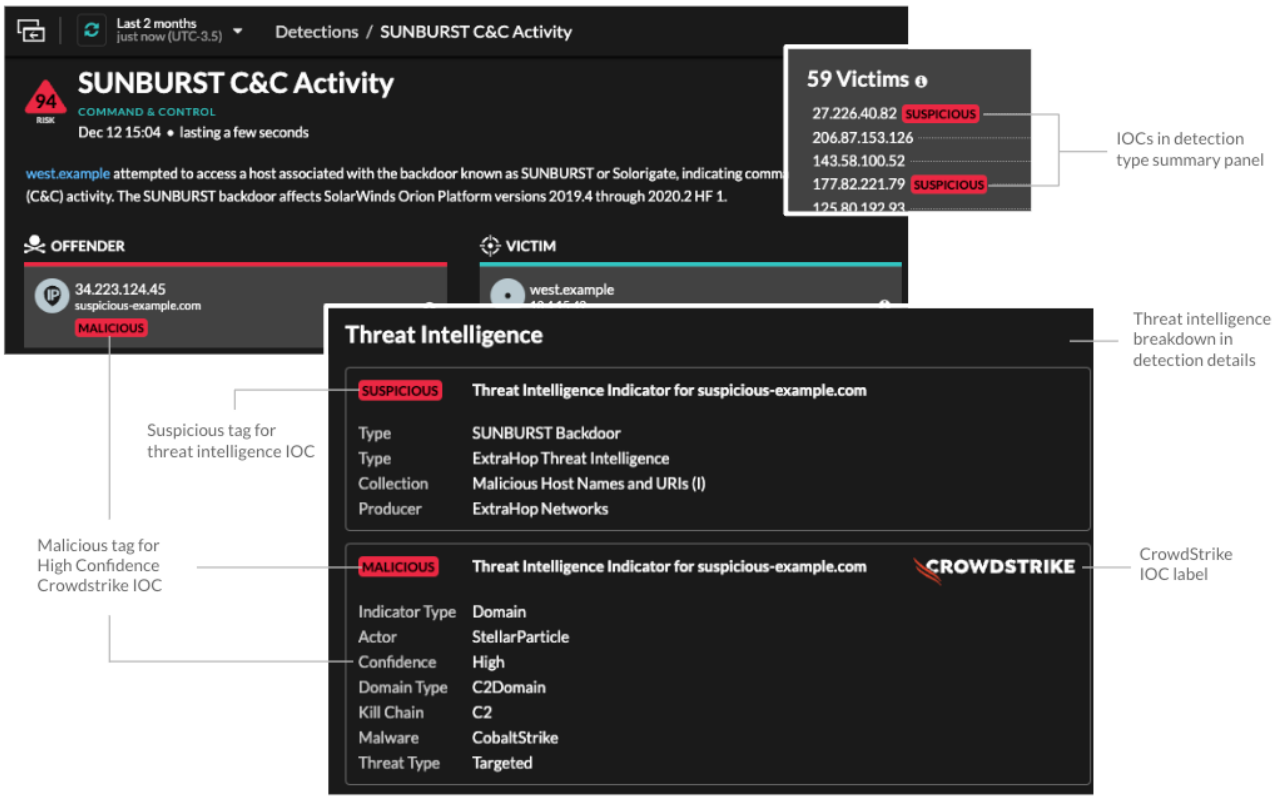
Veröffentlicht: 2024-01-31

Bedrohungsinformationen liefern bekannte Daten über verdächtige IP-Adressen, Domänen, Hostnamen und URIs, die Ihnen helfen können, Risiken für Ihr Unternehmen zu identifizieren.

Video: Sehen Sie sich die entsprechende Schulung an: Bedrohungsinformationen

Bedrohungsinformationsdatensätze, sogenannte Bedrohungssammlungen, enthalten Listen verdächtiger Endpunkte, die als Indicators of Compromise (IOCs) bezeichnet werden. Wenn das ExtraHop-System Aktivitäten beobachtet, die einem Eintrag in einer Bedrohungssammlung entsprechen, wird eine Erkennung für die verdächtige Verbindung generiert.

Teilnehmer, die einer Bedrohungssammlung entsprechen, werden als Verdächtig markiert. (Bei Crowdstrike-IOCs, bei denen das Konfidenzniveau hoch ist, wird der Teilnehmer als bösartig markiert.) Aufzeichnungen, die den verdächtigen Eintrag enthalten, sind mit einem Kamerasymbol gekennzeichnet .



Kuratierte Bedrohungssammlungen von ExtraHop und CrowdStrike Falcon sind standardmäßig in Ihrem ExtraHop-System verfügbar. Sie können auch benutzerdefinierte Sammlungen aus kostenlosen und kommerziellen Quellen in der Sicherheits-Community hochladen.

Sammlungen von Bedrohungen

Das ExtraHop-System unterstützt das Sammeln von Bedrohungen aus verschiedenen Quellen.

Da Cyber-Bedrohungsinformationen von der Community gesteuert werden, gibt es viele externe Quellen für die Erfassung von Bedrohungen. Daten aus diesen Sammlungen können in ihrer Qualität oder Relevanz für Ihre Umgebung variieren. Um die Genauigkeit zu gewährleisten und Störungen zu reduzieren, empfehlen wir, dass Sie Ihre Uploads auf qualitativ hochwertige Bedrohungsdaten beschränken, die sich

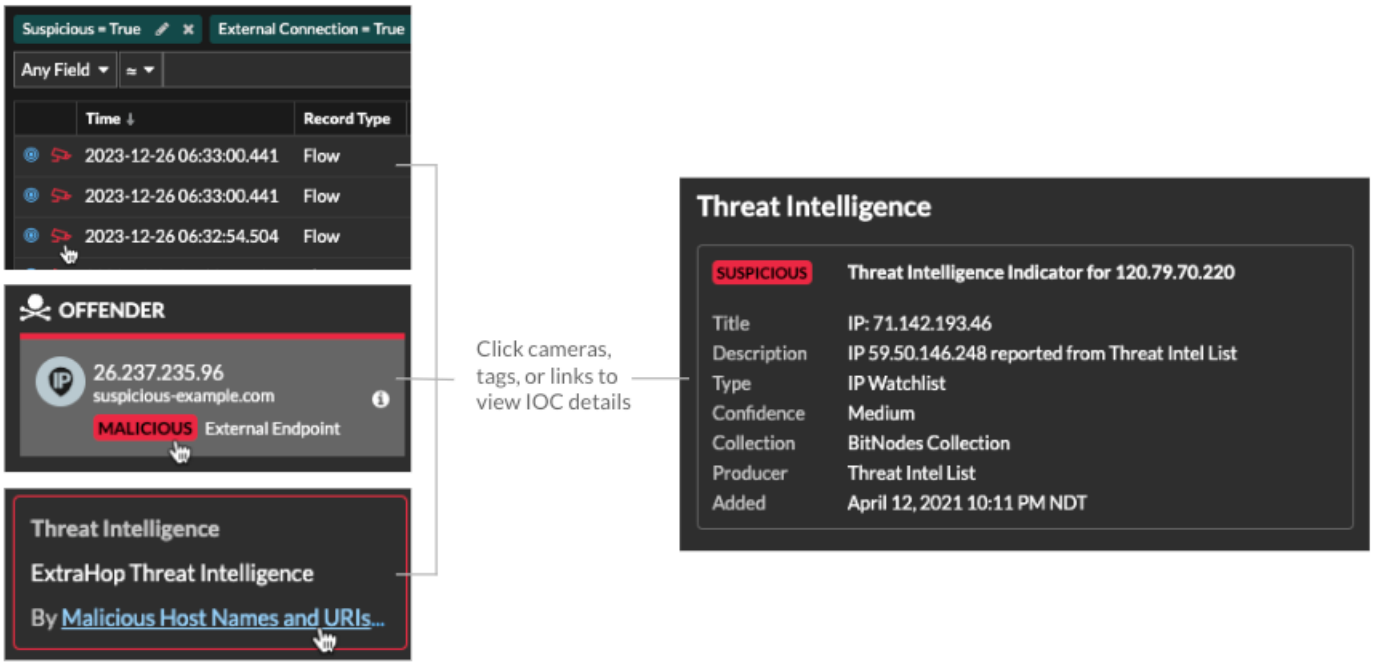
auf eine bestimmte Art von Eindringlingen konzentrieren, z. B. eine Sammlung für Malware und eine andere Sammlung für Botnets.

Von ExtraHop oder Crowdstrike Falcon kuratierte Bedrohungssammlungen werden alle 6 Stunden aktualisiert. Verdächtige IP-Adressen, Domains, Hostnamen und URIs erscheinen in Systemdiagrammen und Datensätzen.

Kostenlose und kommerzielle Sammlungen, die von der Sicherheits-Community angeboten werden die in Structured Threat Information eXpression (STIX) als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert sind, können manuell hochgeladen werden oder über die REST-API zu ExtraHop-Systemen. STIX Version 1.0 - 1.2 werden derzeit unterstützt. Sie müssen jede Bedrohungssammlung einzeln auf Ihre Konsole und alle angeschlossenen Sensoren hochladen.

Untersuchung von Bedrohungen

Nachdem das Reveal (x) -System einen Indikator für eine Gefährdung festgestellt hat, wird die verdächtige IP-Adresse, Domain, Hostname oder URI in den Erkennungszusammenfassungen und auf einzelnen Erkennungskarten als Verdächtig oder Bösartig markiert. In Tabellen und Diagrammen sind Kompromissindikatoren mit einem Kamerasymbol gekennzeichnet, sodass Sie direkt in den Tabellen und Diagrammen, die Sie gerade ansehen, Nachforschungen anstellen können.

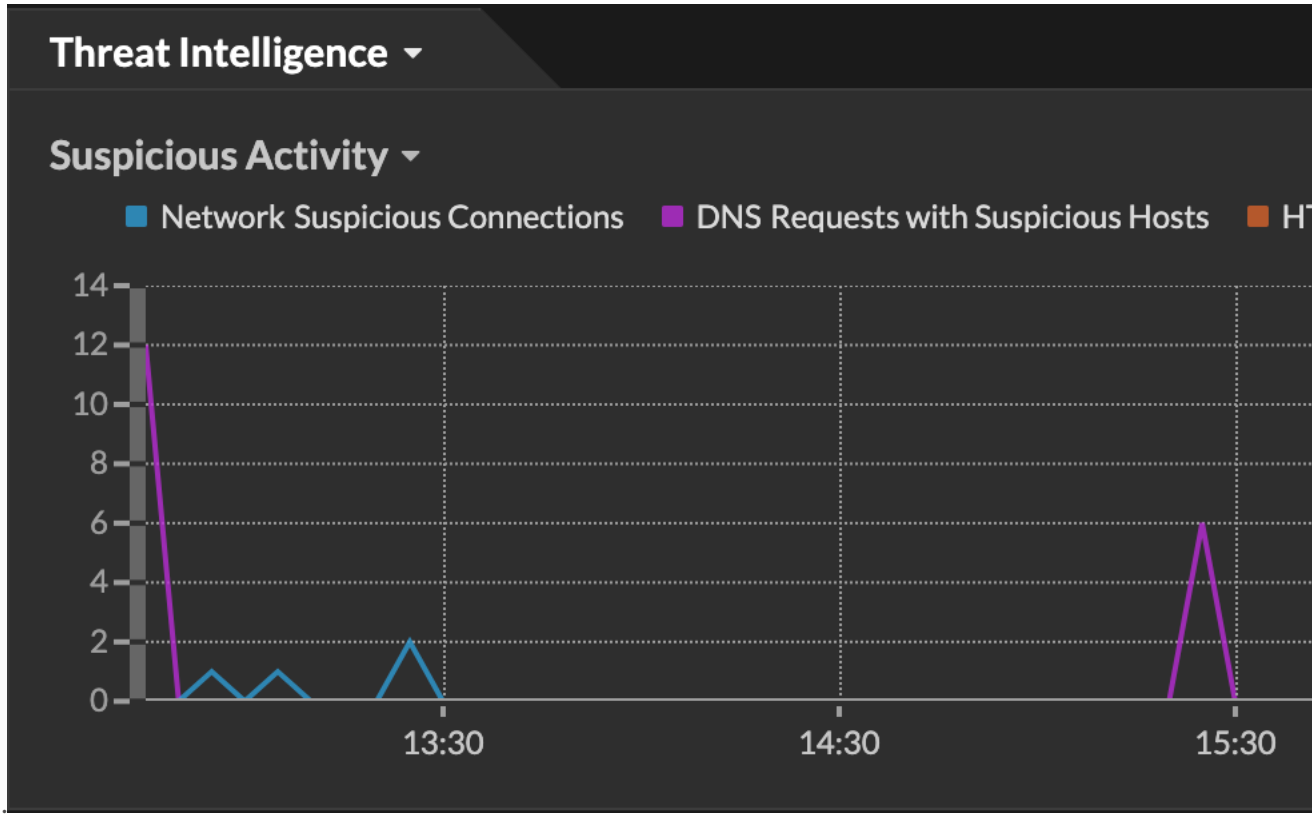


- Wenn die Bedrohungssammlung hinzugefügt oder aktualisiert wird, nachdem das System die verdächtige Aktivität beobachtet hat, werden Bedrohungsinformationen erst dann auf diese IP-Adresse, diesen Hostnamen oder URI angewendet, wenn die verdächtige Aktivität erneut auftritt.
- (Nur Reveal (x) 360) Wenn eine integrierte ExtraHop- oder CrowdStrike-Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System eine automatische Retrospektive Detection (ARD) durch, die nach neuen Domains, Hostnamen, URLs und IP-Adressen sucht, die auf eine Gefährdung in den Datensätzen der letzten 7 Tage hinweisen. Wenn eine Übereinstimmung gefunden wird, generiert das System eine rückwirkende Erkennung.
- Wenn Sie eine Bedrohungssammlung deaktivieren oder löschen, werden alle Indikatoren aus den zugehörigen Metriken und Datensätzen im System entfernt. Erkennungen, die für die Triage auf der Grundlage von Bedrohungsinformationen empfohlen werden, verbleiben im System, nachdem die zugehörige Sammlung deaktiviert wurde.

Hier sind einige Stellen im Reveal (x) -System, an denen die in Ihren Bedrohungssammlungen gefundenen Bedrohungsindikatoren angezeigt werden:

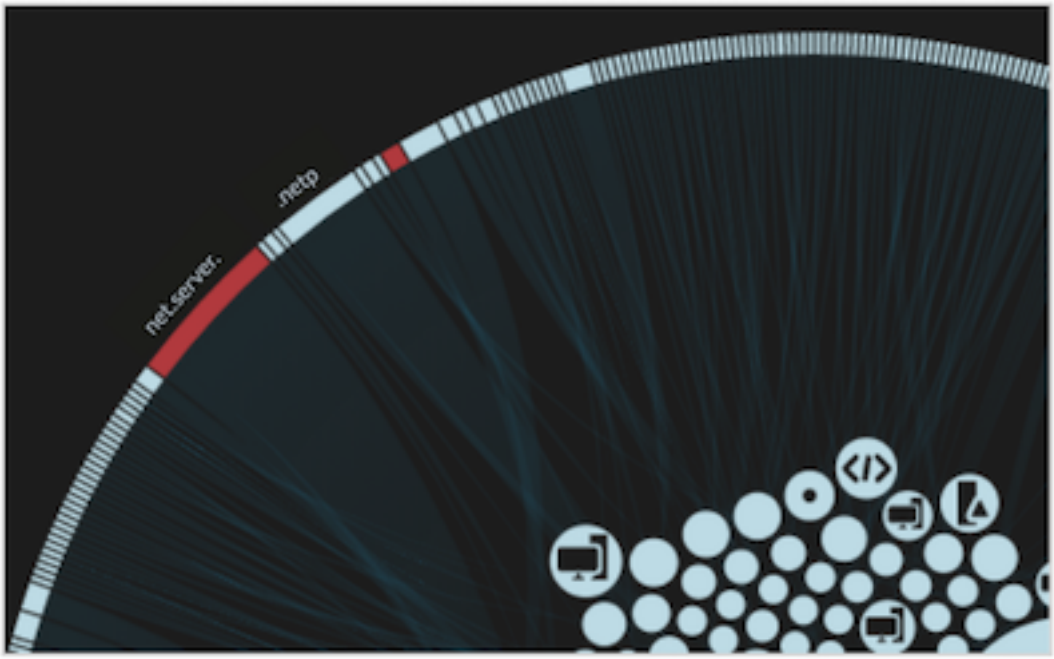
Dashboard zur Erhöhung der Sicherheit

Das Region „Bedrohungsinformationen“ enthält Kennzahlen für verdächtige Aktivitäten, die mit den Daten in Ihren Bedrohungssammlungen übereinstimmen. Wenn Sie auf eine beliebige Metrik klicken, z. B. auf HTTP-Anfragen mit verdächtigen Hosts, können Sie Details zu der Metrik aufrufen oder Datensätze für verwandte Transaktionen abfragen.



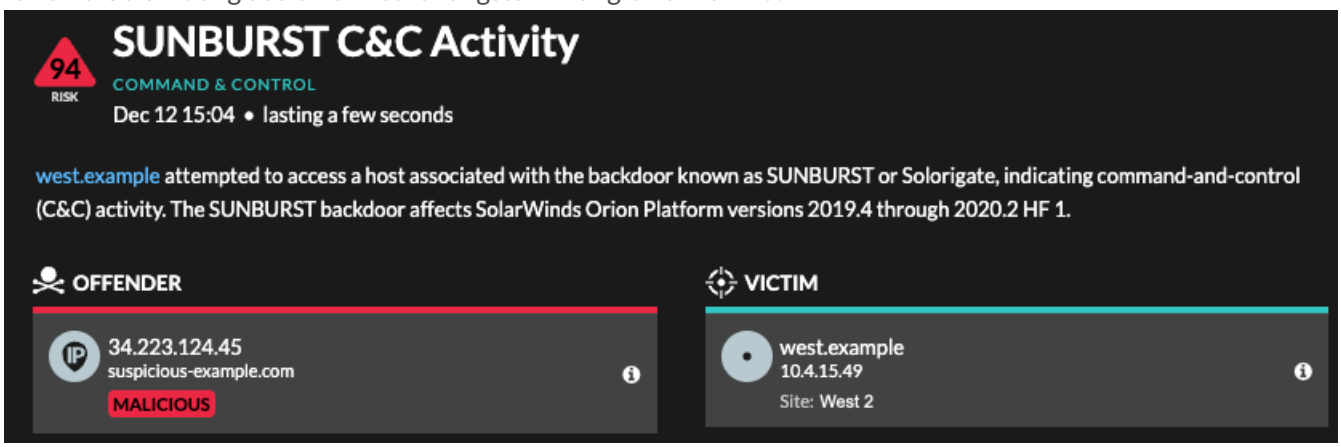
Perimeter im Überblick

In der Halo-Visualisierung sind alle Endpunkte, die mit Einträgen zur Bedrohungserfassung übereinstimmen, rot hervorgehoben.



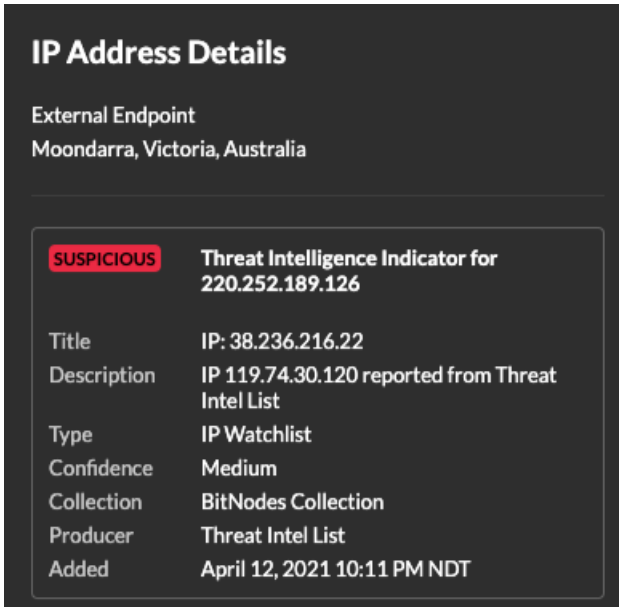
Erkennungen

Eine Erkennung erfolgt, wenn im Netzwerkverkehr ein Indikator für eine Gefährdung aus einer Bedrohungssammlung erkannt wird.



Angaben zur IP-Adresse

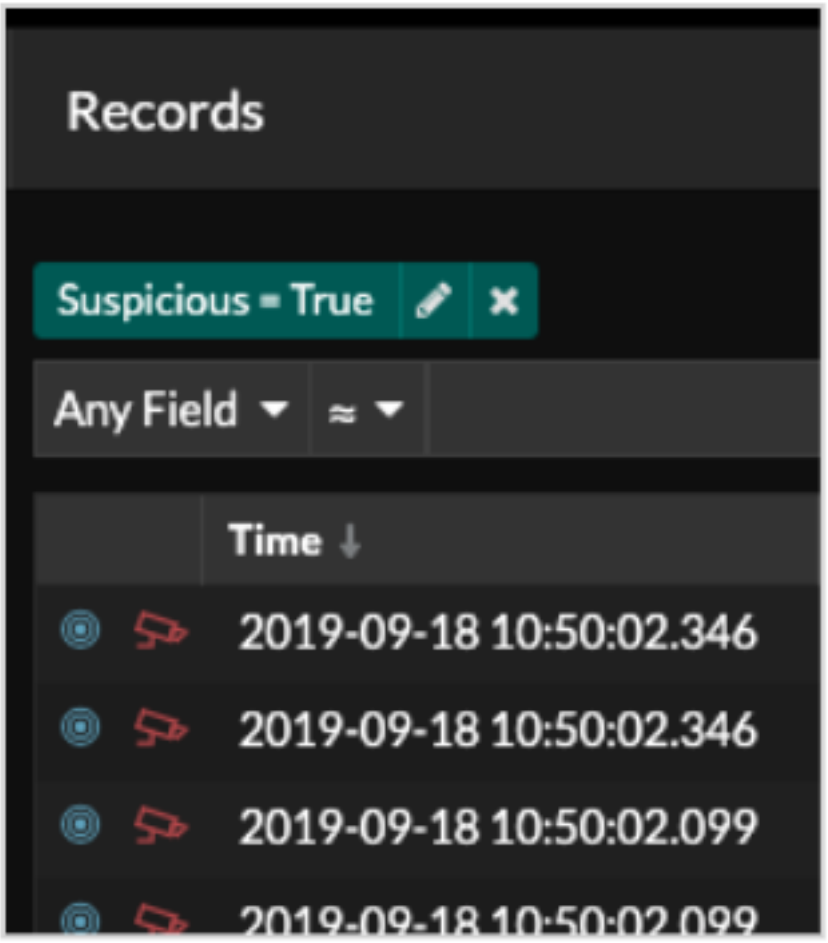
Auf den IP-Adressdetailseiten werden vollständige Bedrohungsinformationen zu IP-Adressindikatoren für kompromittierte IP-Adressen angezeigt.



Aufzeichnungen

Auf der Seite „Datensätze“ können Sie direkt nach Transaktionen abfragen, die den Einträgen zur Bedrohungssammlung entsprechen.

- Klicken Sie unter der Facette Verdächtig auf **Wahr** um nach allen Datensätzen mit Transaktionen zu filtern, die mit verdächtigen IP-Adressen, Hostnamen und URIs übereinstimmen.
- Erstellen Sie einen Filter, indem Sie Verdächtige, Verdächtige IP, Verdächtige Domain oder Verdächtige URI aus dem Dreifeld-Dropdownmenü, einen Operator und einen Wert auswählen.
- Klicken Sie auf das rote Kamerasymbol um Bedrohungsinformationen einzusehen.



Rückwirkende Erkennungen

(Nur Reveal (x) 360) Wenn eine ExtraHop- oder CrowdStrike-Bedrohungssammlung aktualisiert wird, führt das ExtraHop-System eine automatische Retrospektive Detection (ARD) durch, die nach neuen Domains, Hostnamen, URLs und IP-Adressen sucht, die auf eine Gefährdung in den Datensätzen der letzten 7 Tage hinweisen. Wenn eine frühere Verbindung zu einer verdächtigen Domain erkannt wird, generiert das System eine nachträgliche Erkennung.

Der Zeitstempel einer rückwirkenden Erkennung gibt den Zeitpunkt an, zu dem die Aktivität ursprünglich stattgefunden hat und möglicherweise nicht in der aktuellen Erkennungsliste erscheint. Rückwirkende Erkennungen finden Sie, indem Sie auf Retrospective Threat Intelligence klicken Bedrohungsübersicht. Du kannst auch eine Regel für Erkennungsbenachrichtigungen erstellen um Ihnen eine E-Mail zu senden, wenn diese Arten von Erkennungen auftreten.