Untersuchen Sie Leistungserkennungen

Veröffentlicht: 2023-09-30

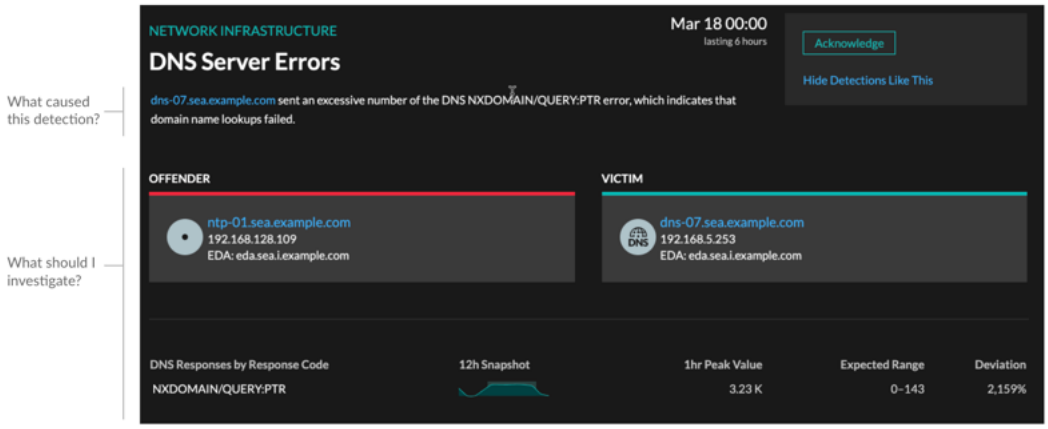
Wenn eine interessante Erkennung auftritt, sollten Sie untersuchen, ob das erkannte Verhalten auf ein Problem mit niedriger Priorität oder auf ein potenzielles Problem hindeutet. Sie können Ihre Untersuchung direkt von der Erkennungskarte aus starten, die Links zu Daten im gesamten ExtraHop-System enthält.

Es gibt eine Reihe von Tools, die Ihnen beim Filtern helfen können Ihre Ansicht, um die Erkennungen zu sehen, denen Sie bei der Untersuchung Priorität einräumen möchten. Halten Sie zunächst nach den folgenden Trends Ausschau:

- Gab es zu ungewöhnlichen oder unerwarteten Zeiten Erkennungen, z. B. bei Benutzeraktivitäten am Wochenende oder außerhalb der Geschäftszeiten?
- Erscheinen irgendwelche Erkennungen in großen Clustern auf der Timeline?
- Werden Erkennungen für hochwertige Endgeräte angezeigt?
- Sind Geräte, die an der Erkennung beteiligt sind, auch an anderen Erkennungen beteiligt?

Beginne deine Untersuchung

Lesen Sie den Titel und die Zusammenfassung der Erkennung, um zu erfahren, was die Erkennung verursacht hat.



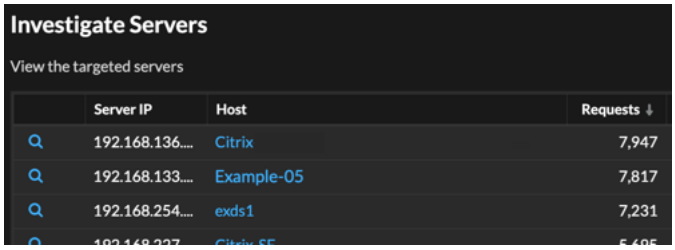
Verfeinern Sie Ihre Untersuchung

Karten mit Erkennungsdetails enthalten zugehörige Daten zur Erkennung. Die Verfügbarkeit der Daten hängt von den Geräten und Metriken ab, die mit der Erkennung verknüpft sind. Nachdem Sie auf einen Link geklickt haben, können Sie zur Erkennungskarte zurückkehren, indem Sie im Navigationspfad auf den Namen der Erkennung klicken. Jede Untersuchungsoption wird in den folgenden Abschnitten beschrieben.

Ermittlungsdaten überprüfen

Die meisten Daten, die Sie benötigen, um eine Erkennung zu verstehen, zu validieren und zu untersuchen, werden auf der Erkennungsdetailseite angezeigt: Tabellen mit relevanten Metrikdaten, Datensatztransaktionen und Links zu Rohpaketen.

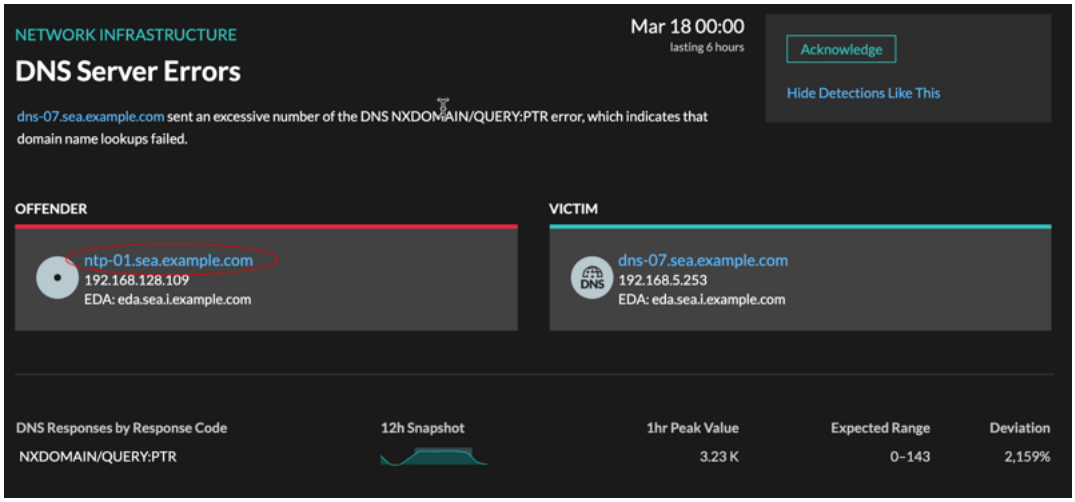
Klicken Sie auf einen Hostnamen, um zur Seite „Geräteübersicht“ zu gelangen, oder klicken Sie mit der rechten Maustaste, um ein Diagramm mit diesem Gerät als Quelle und den entsprechenden Messwerten zu erstellen.



Name des Geräts

Klicken Sie auf einen Gerätenamen, um zur Seite „Geräteübersicht“ zu gelangen, die die Rolle, Benutzer und Tags enthält, die mit diesem Gerät verknüpft sind. Klicken Sie im linken Bereich auf einen Protokollnamen, um alle mit dem Gerät verknüpften Protokollmetriken anzuzeigen. Auf der Protokollseite erhalten Sie einen vollständigen Überblick darüber, was dieses Gerät zum Zeitpunkt der Erkennung getan hat.

Wenn Sie beispielsweise feststellen, dass Datenbanktransaktionen fehlschlagen, können Sie sich über andere Aktivitäten im Zusammenhang mit dem Server informieren, der die Datenbank-Instance hostet.



Verfügbarkeit

Links zu Gerätenamen sind nur für Geräte verfügbar, die vom ExtraHop-System automatisch erkannt wurden. Remote-Geräte, die sich außerhalb Ihres Netzwerk befinden, werden durch ihre IP-Adressen dargestellt.

Karte der Aktivitäten

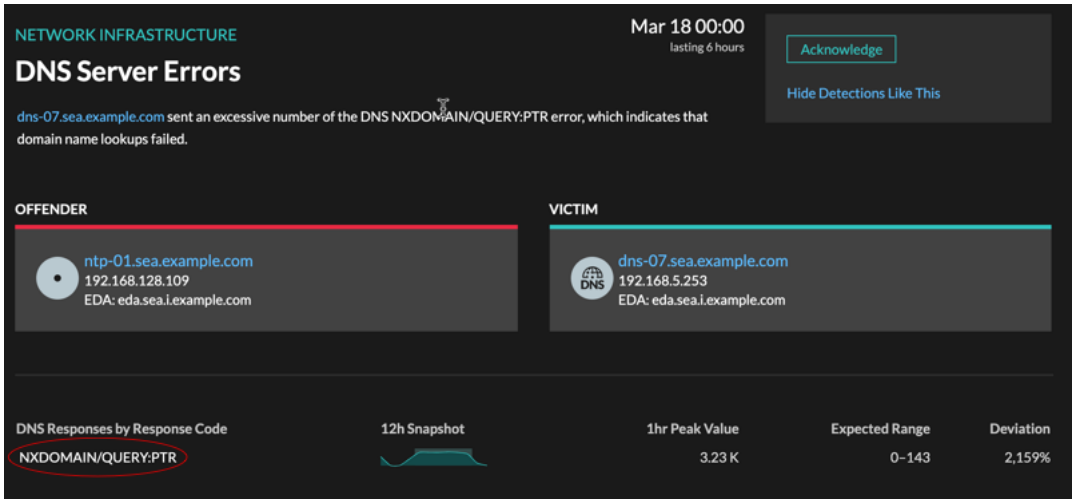
Klicken Sie auf das Activity Map-Symbol neben einem Gerätenamen, um die Geräteverbindungen nach Protokoll während der Erkennung anzuzeigen. Wenn Sie beispielsweise eine Erkennung von LDAP-Authentifizierungsfehlern erhalten, können Sie eine Aktivitätsdiagramm erstellen, um zu erfahren, welche Geräte während der Erkennung mit einem LDAP-Server verbunden waren.

Verfügbarkeit

Eine Aktivitätsdiagramm ist verfügbar, wenn ein einzelner Client oder Server mit ungewöhnlichen L7-Protokollaktivitäten in Verbindung gebracht wird, z. B. einer hohen Anzahl von HTTP-Fehlern oder Timeouts bei DNS-Anfragen.

Detaillierter Metrik Drilldown

Klicken Sie auf einen Link zur Detail-Metrik, um einen Metrikwert aufzuschlüsseln. Es wird eine Seite mit Detail-Metrik angezeigt , auf der Metrikwerte nach einem Schlüssel aufgelistet sind, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Fehler. Wenn Sie beispielsweise eine Authentifizierungserkennung für einen LDAP-Server erhalten, können Sie im Detail herausfinden, welche Client-IP-Adressen die ungültigen Anmeldedaten übermittelt haben, die zur Gesamtzahl der LDAP-Fehler beigetragen haben.

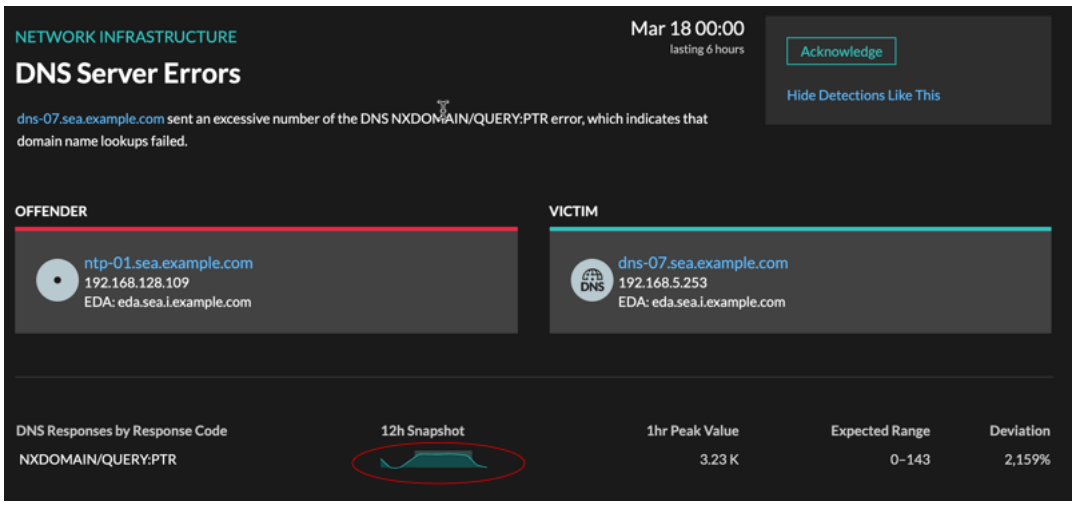


Verfügbarkeit

Die Drilldown-Option ist für Erkennungen verfügbar, die mit Topnset detaillierte Metriken.

Sparkline

Klicken Sie auf die Sparkline, um ein Diagramm zu erstellen, das die Quelle, das Zeitintervall und die Drilldown-Details der Erkennung enthält. Sie können es dann einem Dashboard zur zusätzlichen Überwachung hinzufügen. Wenn Sie beispielsweise Probleme mit dem Erkennung feststellen, können Sie ein Diagramm mit den 500 vom Server gesendeten Statuscodes erstellen und dieses Diagramm dann zu einem Dashboard über die Leistung der Website hinzufügen.

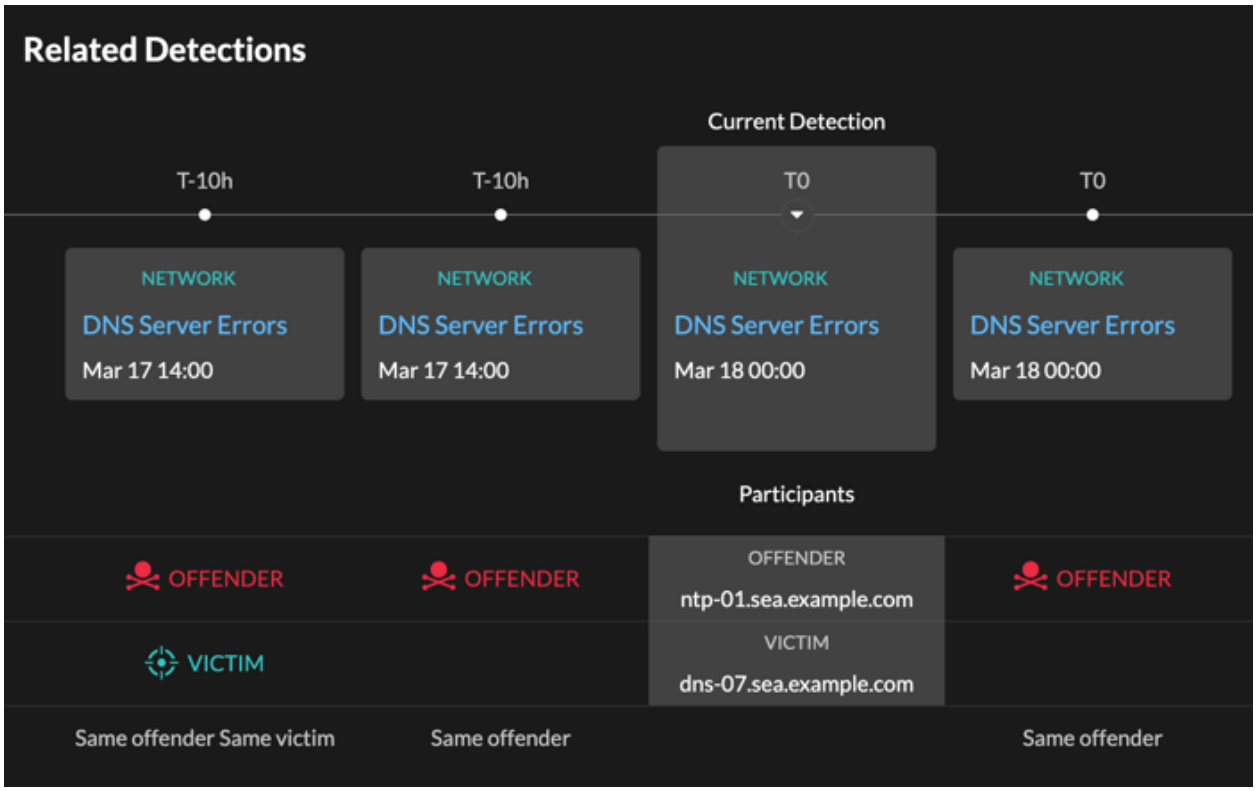


Verfügbarkeit

Die Sparkline-Option ist für Erkennungen verfügbar, die mit Metriken verknüpft waren.

Verwandte Erkennungen

Klicken Sie auf eine entsprechende Erkennung, um Informationen zu Netzwerk-, Anwendung- und Infrastrukturproblemen bei mehreren Erkennungen mit gemeinsamen Teilnehmern zu erhalten. Beispielsweise ist ein als Täter identifiziertes Gerät die wahrscheinliche Quelle eines Problems, z. B. ein Datenbankserver, der eine übermäßige Anzahl von Antwortfehlern sendet. Ein Gerät, das als Opfer identifiziert wurde, ist in der Regel negativ von dem Problem betroffen, z. B. bei Clients, bei denen langsame oder fehlgeschlagene Datenbanktransaktionen auftreten. Sie können zugehörige Erkennungsdetails anzeigen, um festzustellen, ob die Erkennungsereignisse ähnlich sind, um zu sehen, welche anderen Geräte beteiligt sind, und um Metrikdaten einzusehen.



Verfügbarkeit

Die zugehörige Erkennungszeitleiste ist verfügbar, wenn es Erkennungen gibt, an denen dieselben Opfer- oder Täterteilnehmer wie an der aktuellen Erkennung beteiligt sind. Ähnliche Erkennungen sind möglicherweise vor oder nach der aktuellen Erkennung aufgetreten.