Untersuchen Sie Sicherheitserkennungen

Veröffentlicht: 2023-09-30

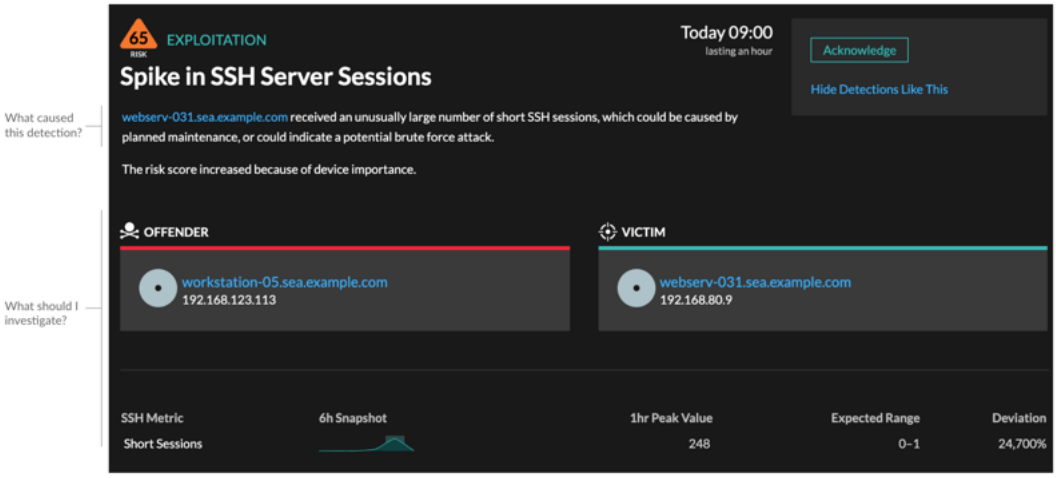
Wenn eine interessante Erkennung auftritt, sollten Sie untersuchen, ob das erkannte Verhalten auf ein Problem mit niedriger Priorität oder auf ein potenzielles Sicherheitsrisiko hindeutet. Sie können Ihre Untersuchung direkt von der Erkennungskarte aus starten, die Links zu Daten im gesamten ExtraHop-System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

Es gibt eine Reihe von Tools, die Ihnen beim Filtern helfen können Ihre Ansicht, um die Erkennungen zu sehen, die Sie für die Untersuchung priorisieren 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?
- Gibt es Entdeckungen mit hohen Risikowerten?
- Sind Geräte, die an der Erkennung beteiligt sind, auch an anderen Erkennungen beteiligt?
- Werden anhand einer Bedrohungssammlung im Zusammenhang mit der Erkennung Indikatoren für eine Gefährdung identifiziert?

Beginne deine Untersuchung

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



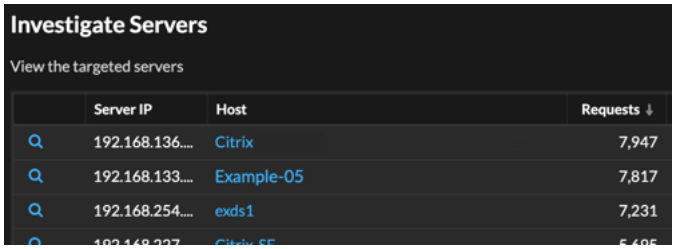
Verfeinern Sie Ihre Untersuchung

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.

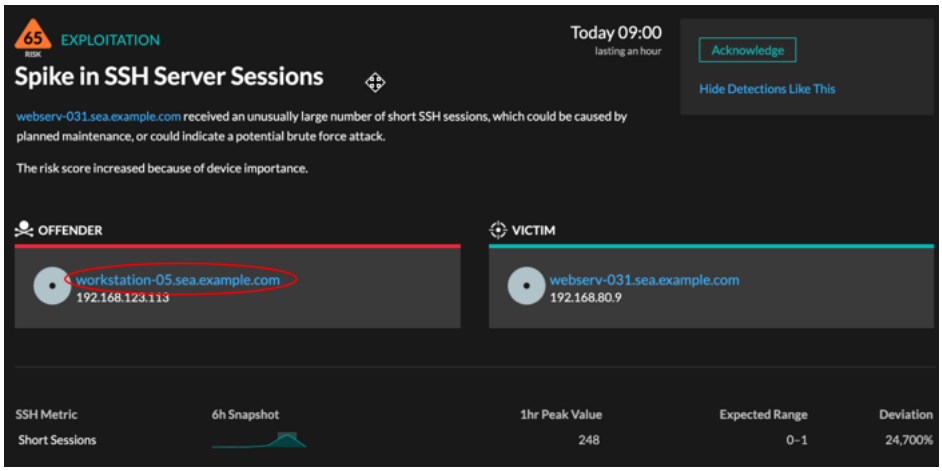
Klicken Sie auf einen Hostnamen, um zur Seite „Geräteübersicht“ zu gelangen, oder klicken Sie mit der rechten Maustaste, um ein Diagramm mit diesem Gerät als Quelle und den entsprechenden Messwerten zu erstellen.



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 einen Erkennungsscan erhalten, können Sie herausfinden, ob dem mit dem Scan verknüpften Gerät die Rolle Vulnerability Scanner zugewiesen wurde.



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 laterale Bewegung Bewegungserkennung erhalten, können Sie herausfinden, ob das verdächtige Gerät über ein

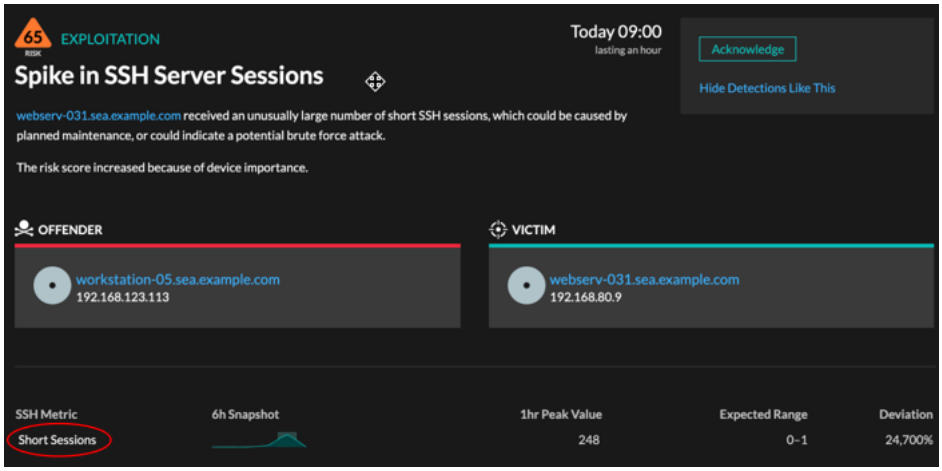
Fernsteuerungsprotokoll Verbindungen mit anderen Clients, IT-Servern oder Domänencontrollern in Ihrem Netzwerk hergestellt hat.

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 Erkennung durch einen Aufklärungsscan erhalten, können Sie im Detail herausfinden, welche Client-IP-Adressen während der Erkennung mit der ungewöhnlich hohen Anzahl von 404-Statuscodes verknüpft wurden.

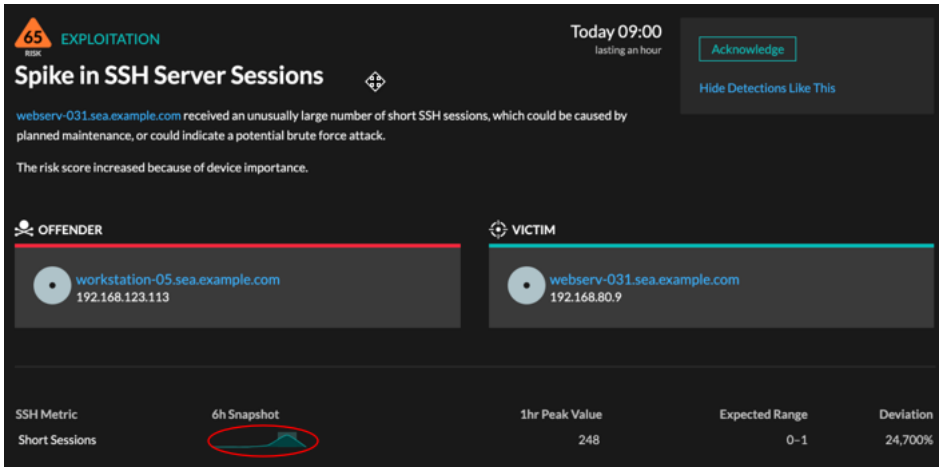


Verfügbarkeit

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, das Sie dann zu einem Dashboard zur Überwachung hinzufügen können. Wenn Sie beispielsweise eine ungewöhnliche Anzahl von Remotesitzungen feststellen, erstellen Sie ein Diagramm mit SSH-Sitzungen für diesen Server und fügen Sie dieses Diagramm dann einem Dashboard zur Sitzungsverwaltung hinzu.

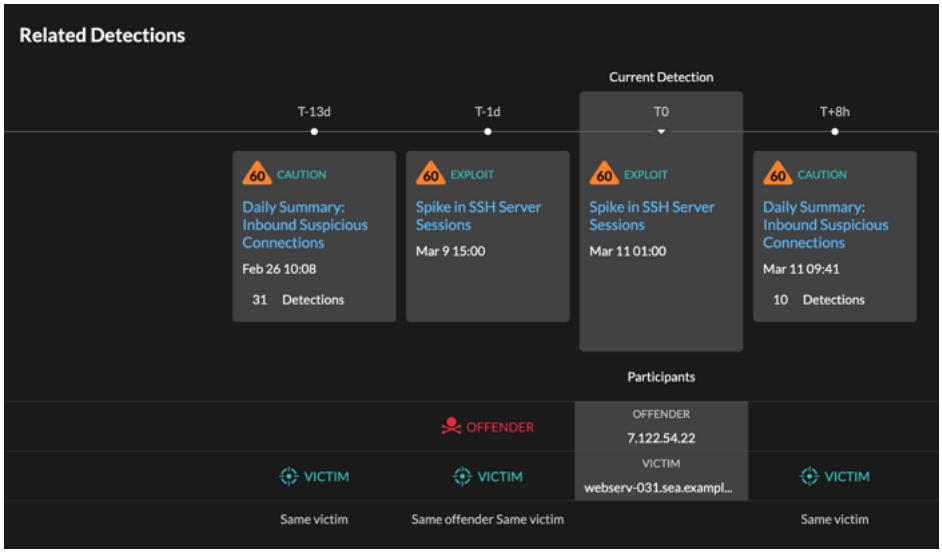


Verfügbarkeit

Die Sparkline-Option ist für Erkennungen verfügbar, die mit Metriken verknüpft waren und eine Dauer von mehr als einer Stunde hatten. Für 1-Sekunden-Metriken ist eine Sparkline verfügbar, wenn die Dauer mehr als 30 Sekunden betrug.

Verwandte Erkennungen

Klicken Sie auf verwandte Erkennungen , um Einblicke in verdächtiges Verhalten und neue Angriffe bei mehreren Erkennungen mit gemeinsamen Teilnehmern zu erhalten. Beispielsweise könnte ein Opfer bei der aktuellen Erkennung, das als Täter an einer späteren Erkennung beteiligt ist, darauf hinweisen, dass das Gerät kompromittiert wurde. Sie können zugehörige Erkennungsdetails anzeigen, um festzustellen, ob die Erkennungsereignisse ähnlich sind, und um zu sehen , welche anderen Geräte beteiligt sind.



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.

Bedrohungsinformationen

Klicken Sie auf ein rotes Kamerasymbol um auf detaillierte Bedrohungsinformationen über einen Bedrohungsindikator zuzugreifen.

Threat Intelligence liefert bekannte Daten über verdächtige IP-Adressen, Hostnamen und URIs, anhand derer Risiken für Ihr Unternehmen identifiziert werden können. Diese Datensätze, die als Bedrohungssammlungen bezeichnet werden, sind standardmäßig in Ihrem Reveal (x) -System und in der Sicherheits-Community aus kostenlosen und kommerziellen Quellen verfügbar.

Verfügbarkeit

Threat Intelligence muss auf Ihrem Reveal (x) -System aktiviert sein, bevor Sie diese Indikatoren sehen können.