

Untersuchen Sie Sicherheitserkennungen

Veröffentlicht: 2024-07-02

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.

The screenshot shows a detection card with the following details:

- Risk Level:** 65 EXPLOITATION
- Title:** Spike in SSH Server Sessions
- Time:** Today 09:00 (lasting an hour)
- Buttons:** Acknowledge, Hide Detections Like This
- Description:** webserv-031.sea.example.com received an unusually large number of short SSH sessions, which could be caused by planned maintenance, or could indicate a potential brute force attack. The risk score increased because of device importance.
- Offender:** workstation-05.sea.example.com (192.168.123.113)
- Victim:** webserv-031.sea.example.com (192.168.80.9)
- SSH Metric:** Short Sessions
- 6h Snapshot:** A line graph showing a spike in short sessions.
- 1hr Peak Value:** 248
- Expected Range:** 0-1
- Deviation:** 24,700%

Verfeinern Sie Ihre Untersuchung

Erkennungsdetailkarten enthalten verwandte 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 Erkennungsnamen klicken. Jede Untersuchungsoption wird in den folgenden Abschnitten beschrieben.

Überprüfen Sie die Ermittlungsdaten

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, Aufzeichnungstransaktionen 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 relevanten Messwerten zu erstellen.

Investigate Servers

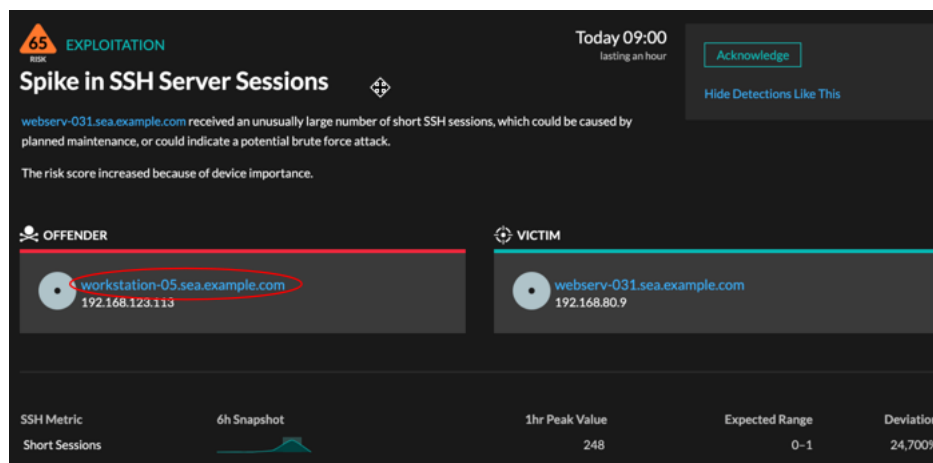
View the targeted servers

	Server IP	Host	Requests ↓
🔍	192.168.136...	Citrix	7,947
🔍	192.168.133...	Example-05	7,817
🔍	192.168.254...	exds1	7,231
🔍	192.168.227...	Citrix-5F	5,485

Name des Geräts

Klicken Sie auf einen Gerätenamen, um zur Seite Geräteübersicht zu gelangen, die die Rolle, Benutzer und Tags enthält, die diesem Gerät zugeordnet sind. Klicken Sie im linken Bereich auf einen Protokollnamen, um alle mit dem Gerät verknüpften Protokollmetriken anzuzeigen. Auf der Protokollseite erhalten Sie ein vollständiges Bild davon, was dieses Gerät zum Zeitpunkt der Erkennung getan hat.


Wenn Sie beispielsweise einen Reconnaissance-Scan erkennen, können Sie Erkennung, ob dem Gerät, das mit dem Scan verknüpft ist, 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

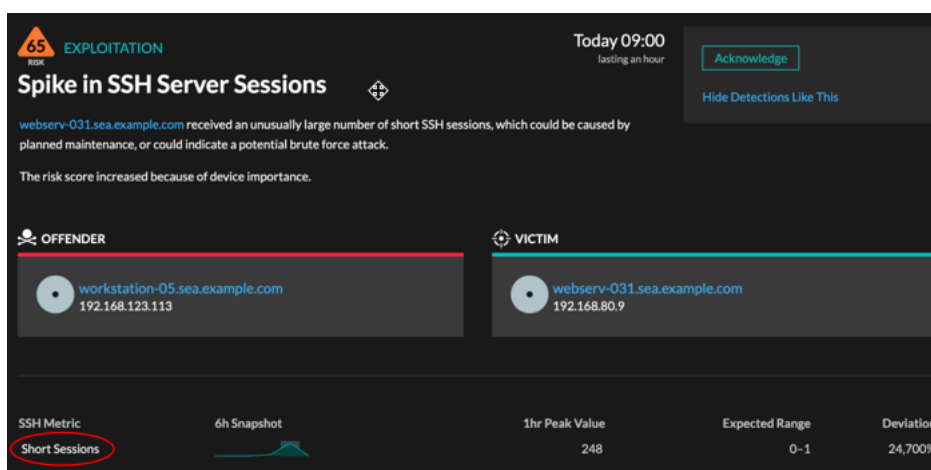
Fernsteuerungsprotokoll Verbindungen zu anderen Clients, IT-Servern oder Domänencontrollern in Ihrem Netzwerk hergestellt hat.

Verfügbarkeit

Eine Aktivitätsdiagramm ist verfügbar, wenn ein einzelner Client oder Server mit ungewöhnlichen L7-Protokollaktivitäten verknüpft ist, z. B. einer hohen Anzahl von HTTP-Fehlern oder DNS-Anforderungs-Timeouts.

Detaillierter Metrik Drilldown

Klicken Sie auf einen Link zur Detail-Metrik, um einen Metrikwert genauer zu betrachten. Eine Metrik-Detailseite wird angezeigt, auf der Messobjektwerte nach einem Schlüssel aufgelistet sind, z. B. Client-IP-Adresse, Server-IP-Adresse, Methode oder Fehler. Wenn bei Ihnen beispielsweise ein Reconnaissance Scan erkannt wird, können Sie einen Drilldown durchführen, um herauszufinden, welche Client-IP-Adressen während der Erkennung mit der ungewöhnlich hohen Anzahl von 404-Statuscodes verknüpft waren.

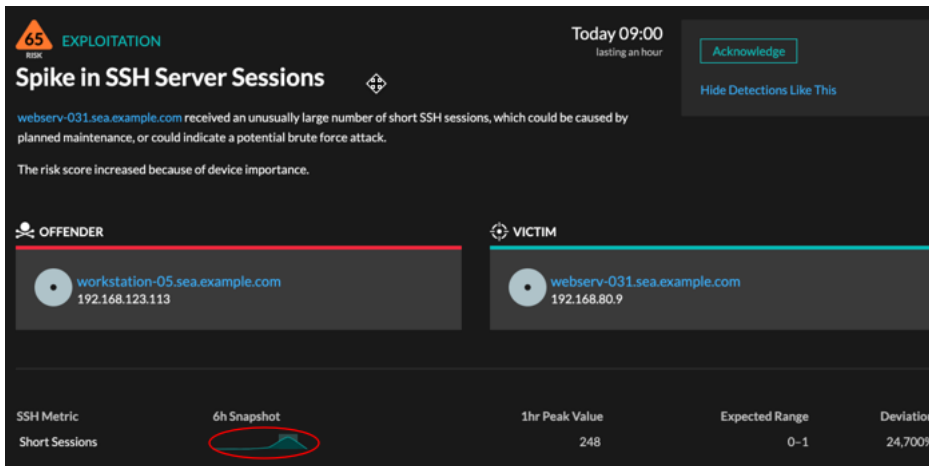


Verfügbarkeit

Die Drilldown-Option ist verfügbar für Erkennungen im Zusammenhang mit Topset 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. Dieses Diagramm können Sie dann zur Überwachung zu einem Dashboard hinzufügen. 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.

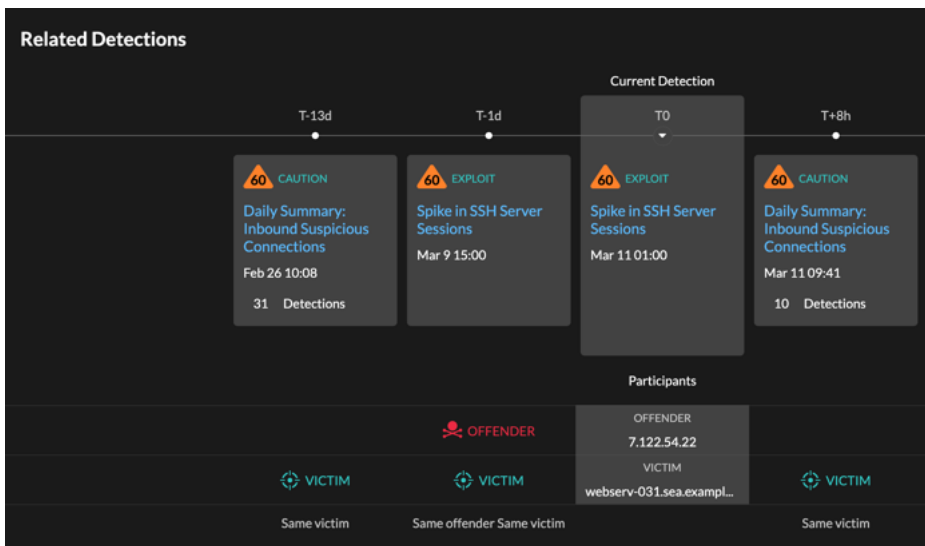


Verfügbarkeit

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

Verwandte Erkennungen


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



Verfügbarkeit

Die entsprechende Zeitleiste für Erkennungen ist verfügbar, wenn es Erkennungen gibt, bei denen dieselben Opfer- oder Täterteilnehmer wie bei der aktuellen Erkennung aufgetreten sind. Ähnliche Erkennungen sind möglicherweise vor oder nach der aktuellen Erkennung aufgetreten.

Bedrohungsinformationen

Klicken Sie auf ein rotes Kamerasymbol  um detaillierte Bedrohungsinformationen zu einem Bedrohungsindikator abzurufen.

Bedrohungsinformationen liefern bekannte Daten über verdächtige IP-Adressen, Hostnamen und URIs, die Ihnen helfen können, Risiken für Ihr Unternehmen zu identifizieren. Diese Datensätze, sogenannte Bedrohungssammlungen, sind standardmäßig in Ihrem RevealX-System und aus kostenlosen und kommerziellen Quellen in der Sicherheits-Community verfügbar.

Verfügbarkeit

Bedrohungsinformationen müssen auf Ihrem RevealX-System aktiviert sein, bevor Sie diese Indikatoren sehen können.