Ermittlungen

Veröffentlicht: 2025-03-28

(nur NDR-Modul) Mithilfe von Untersuchungen können Sie mehrere Funde in einer einzigen Zeitleiste und Karte hinzufügen und anzeigen. Anhand einer Zusammenfassung verbundener Erkennungen können Sie feststellen, ob verdächtiges Verhalten eine gültige Bedrohung darstellt und ob die Bedrohung von einem einzelnen Angriff oder Teil einer größeren Angriffskampagne stammt.

Sie können Untersuchungen von einer Entdeckungsdetailseite aus erstellen und zu ihnen hinzufügen, **Aktionen** Menü auf einem individuelle Erkennungskarte, oder die **Massenaktionen** Menü auf einem Zusammenfassung der Erkennung. Ihr ExtraHop-System erstellt außerdem empfohlene Untersuchungen durch Smart Investigations, bei denen es sich um Untersuchungen handelt, die automatisch als Reaktion auf potenziell bösartige Aktivität erstellt werden.

Jede Ermittlungsseite enthält die folgenden Tools:

Zeitplan der Untersuchung

Die Untersuchungszeitleiste wird auf der linken Seite der Seite angezeigt und listet die hinzugefügten Funde auf, beginnend mit der neuesten Erkennung. Neue Funde, die der Untersuchung hinzugefügt werden, werden in der Zeitleiste entsprechend der Uhrzeit und dem Datum der Erkennung angezeigt. Erkennungsteilnehmer werden unter dem Erkennungstitel angezeigt, und Informationen zur Erkennungsverfolgung, wie Beauftragter und Status, werden neben den Teilnehmern angezeigt.

Angriffskategorien

Die Kategorien der hinzugefügten Funde werden oben auf der Ermittlungsseite angezeigt.

Die Kette der Angriffskategorien zeigt die Anzahl der Funde in jeder Kategorie an, nicht die Reihenfolge, in der die Erkennungen aufgetreten sind. Einen genauen Überblick darüber, wie die Erkennungen im Laufe der Zeit aufgetreten sind, finden Sie im Zeitplan der Untersuchung.

Untersuchungen anzeigen

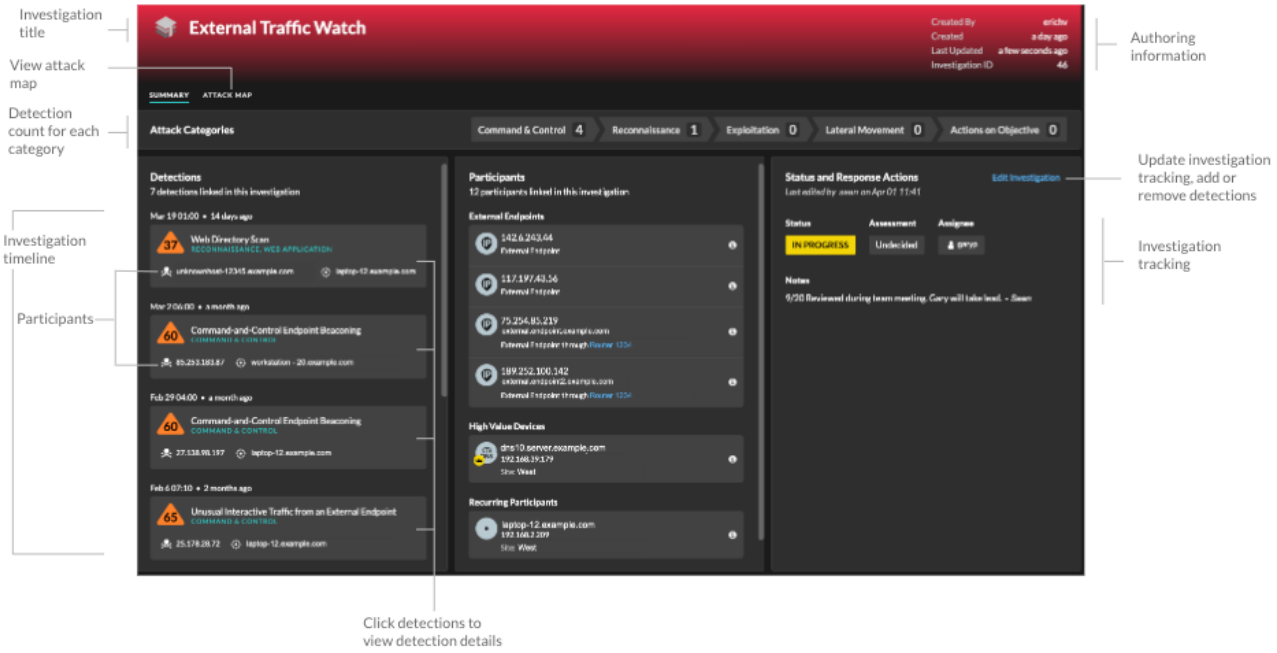
Oben auf der Ermittlungsseite gibt es zwei Optionen, um die Untersuchung anzuzeigen: Zusammenfassung und Angriffskarte. Beide Optionen bieten einen einzigartigen Überblick über Ihre Untersuchung.

Zusammenfassung

Standardmäßig beginnen Ermittlungen in **Zusammenfassung** Ansicht, die den Zeitplan für die Erkennung, eine aggregierte Teilnehmerliste und ein Panel zur Verfolgung des Status und der Reaktionsmaßnahmen für die Untersuchung enthält.

Sie können in der Untersuchungszeitleiste auf eine Erkennung klicken, um sie anzuzeigen Erkennungsdetails, klicken Sie dann auf das X-Symbol, um die Erkennungsdetails zu schließen und zur Zusammenfassung der Untersuchung zurückzukehren. Sie können auch auf Gehe zu klicken Symbol in der oberen rechten Ecke, um die Seite mit den Erkennungsdetails in einem neuen Tab anzuzeigen.

Im Panel „ Teilnehmer“ werden die Teilnehmer an der Untersuchung nach externen Endpunkten, hoher Wert Geräten und wiederkehrenden Teilnehmern gruppiert. Dabei handelt es sich um Teilnehmer, die bei mehreren Funden in der Untersuchung vorkommen. Klicken Sie auf einen Teilnehmer, um Details anzuzeigen und auf Links zuzugreifen.

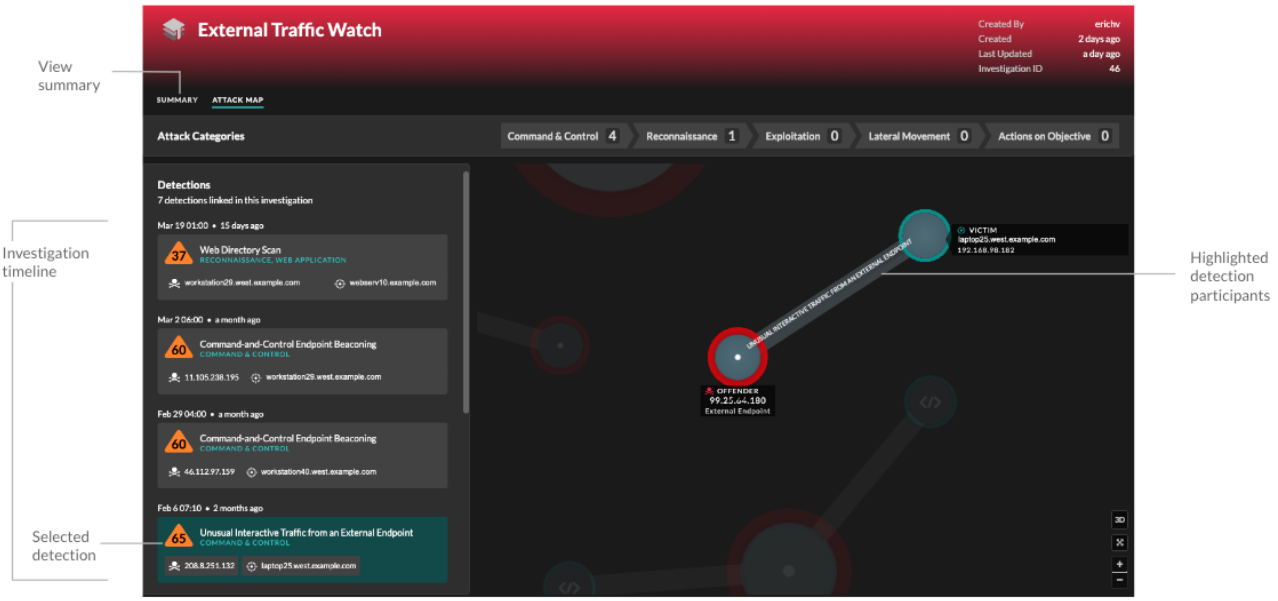


In der Status - und Reaktionsmaßnahmen Panel, klicken **Untersuchung bearbeiten** um den Namen der Untersuchung zu ändern, den Status oder die endgültige Bewertung der Untersuchung festzulegen, einen Beauftragten anzugeben oder Anmerkungen hinzuzufügen .

Sie können fortfahren Verfolgen Sie einzelne Erkennungen nachdem Sie sie zu einer Untersuchung hinzugefügt haben.

Angriffskarte

In **Angriffskarte** Ansicht, der Täter und das Opfer von jeder Erkennung in der Untersuchung werden auf einer interaktiven Karte neben dem Zeitplan der Untersuchung angezeigt.



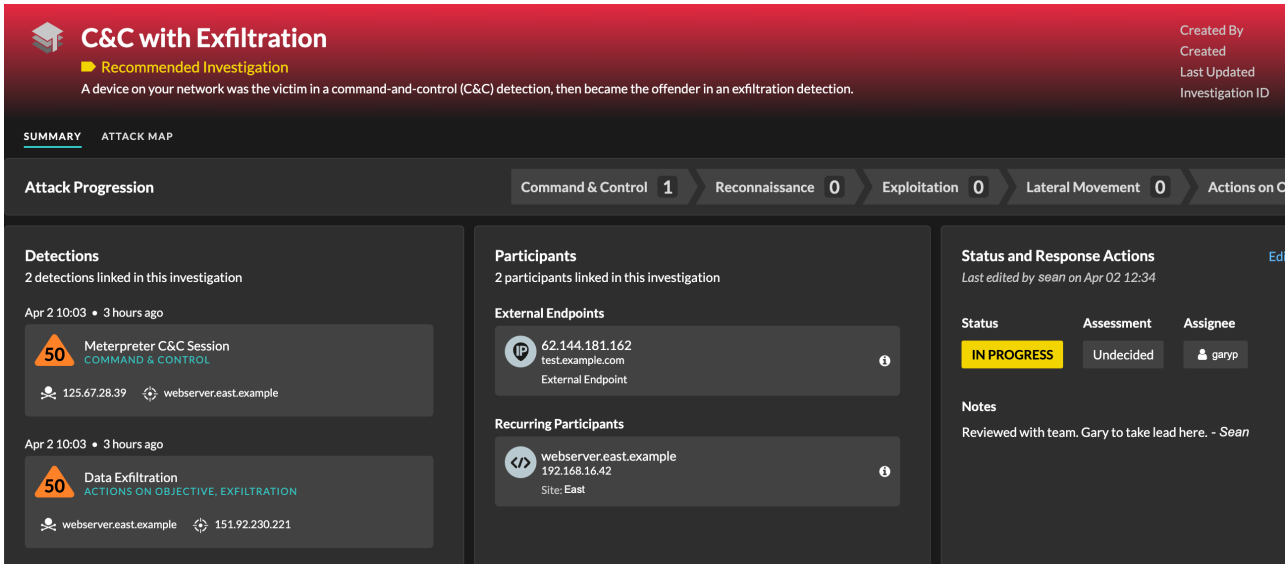
Die Teilnehmer sind durch Linien verbunden, die mit dem Erkennungstyp beschriftet sind, und die Geräterollen werden durch ein Symbol dargestellt.

- Klicken Sie in der Zeitleiste der Untersuchung auf eine Erkennung, um die Teilnehmer hervorzuheben. Kreise werden rot hervorgehoben, wenn das Gerät bei mindestens einer Erkennung im Rahmen der Untersuchung als Täter aufgetreten ist, und blaugrün hervorgehoben, wenn es sich bei dem Gerät um ein Opfer handelt. Die Markierungen werden aktualisiert , wenn Sie auf eine andere Erkennung klicken, damit Sie leichter erkennen können, wann ein Teilnehmer vom Opfer zum Täter wird.
- Klicken Sie auf einen Kreis, um Details wie den Hostnamen, die IP-Adresse oder die MAC-Adresse des Gerät anzuzeigen oder um zu den zugehörigen Erkennungen oder dem Seite „Geräteübersicht“.
- Zeigen Sie mit der Maus auf einen Kreis oder eine Linie, um das Etikett anzuzeigen.

Empfohlene Untersuchungen

Der ExtraHop Machine Learning Service überwacht die Netzwerkaktivität auf Kombinationen von Angriffstechniken, die auf bösartiges Verhalten hinweisen könnten. Wenn eine Kombination identifiziert wird, erstellt das ExtraHop-System eine empfohlene Untersuchung, sodass Ihre Sicherheitsteams die Situation beurteilen und schnell reagieren können, wenn bösartiges Verhalten bestätigt wird.

Wenn beispielsweise ein Gerät Opfer einer Erkennung in der Kategorie Command-and-Control wird, bei einer Exfiltrationserkennung aber zum Täter wird, empfiehlt das ExtraHop-System eine C&C mit Exfiltrationsuntersuchung.



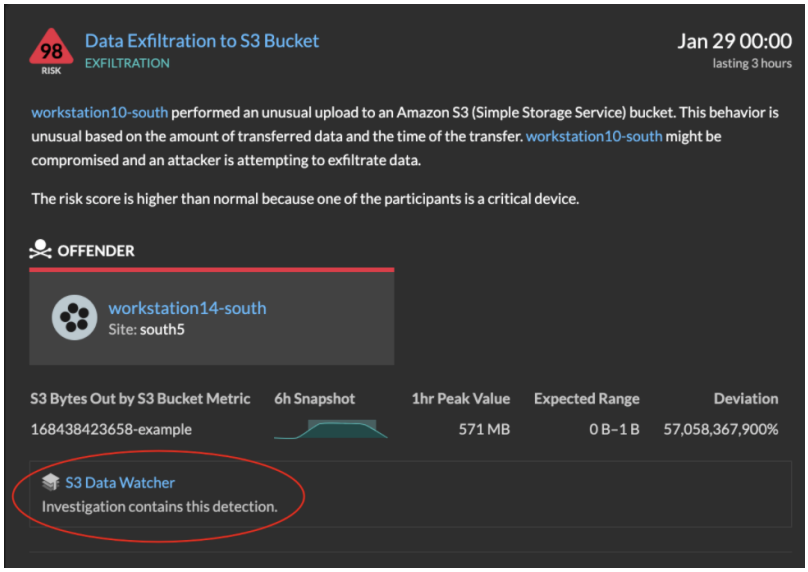
Sie können mit empfohlenen Untersuchungen auf die gleiche Weise interagieren wie von Benutzern erstellte Untersuchungen, z. B. indem Sie Erkennungen hinzufügen oder entfernen, einen Beauftragten angeben und einen Status und eine Bewertung festlegen.

Empfohlene Untersuchungen finden Sie in der Tabelle der Untersuchungen. Sie können die sortieren Erstellt von Spalte, um Untersuchungen zu finden, die von ExtraHop erstellt wurden.

Durch Ermittlungen navigieren

Nachdem eine Erkennung zu einer Untersuchung hinzugefügt wurde, wird unten auf der Erkennungskarte und auf der Seite mit den Erkennungsdetails ein Link zu der Untersuchung angezeigt.

Klicken Sie auf den Namen, um die Untersuchung zu öffnen, und klicken Sie dann auf der Ermittlungsseite auf den Namen der Entdeckung, um zur Erkennungsdetailseite zurückzukehren.



Erfahren Sie, wie eine Untersuchung erstellen.