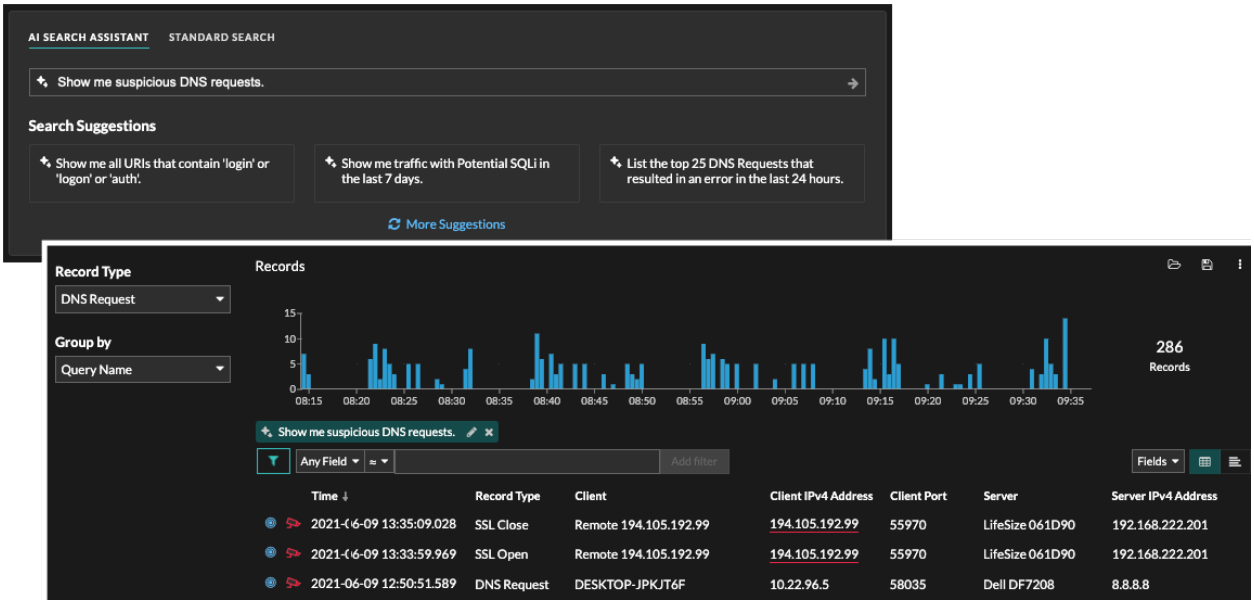
Was ist neu

Veröffentlicht: 2024-07-18

Während Versionshinweise geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.7.

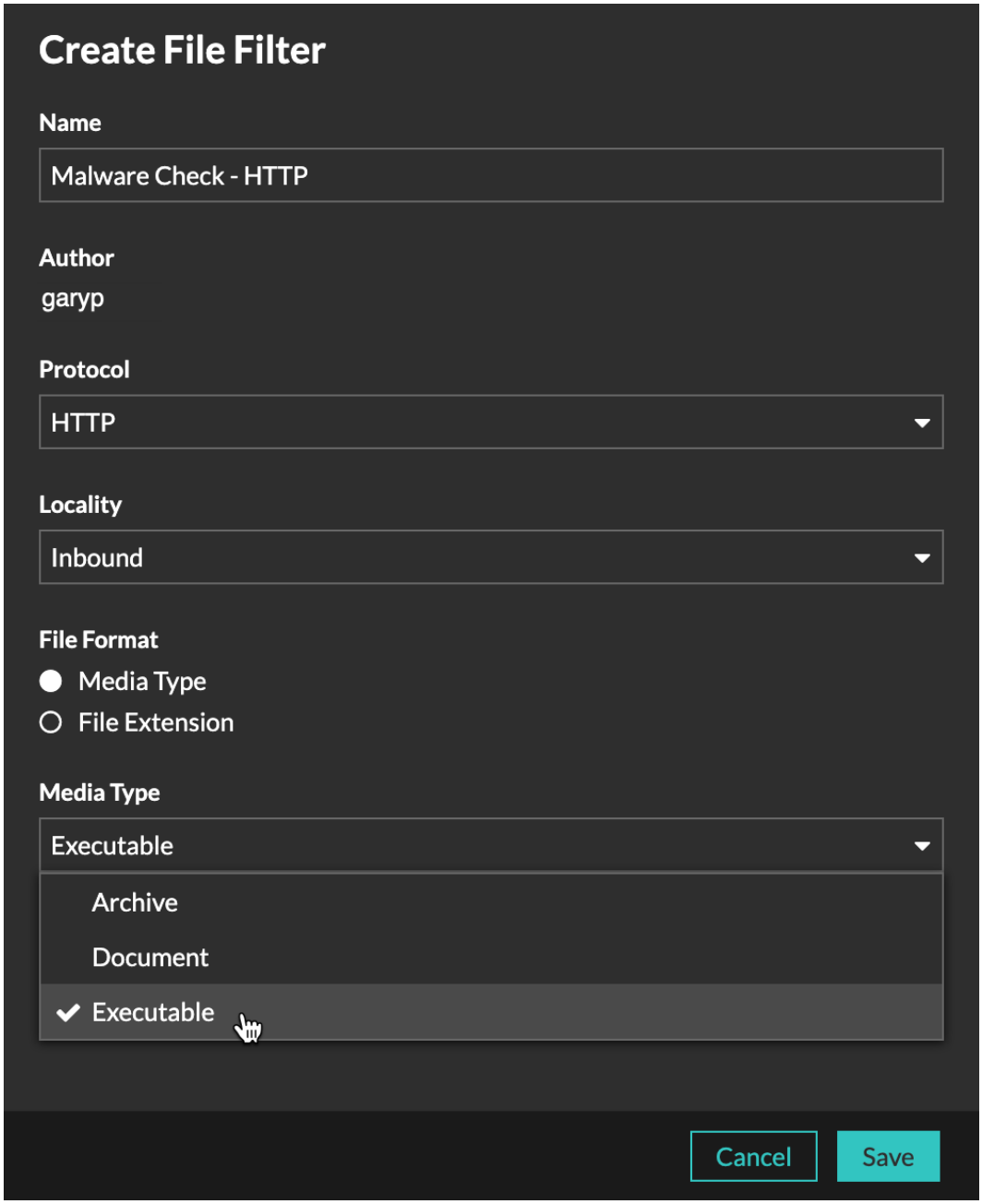
KI-Suchassistent

KI-Suchassistent ermöglicht es Ihnen jetzt, Suchvorgänge von der Datensatzseite aus zu starten, indem Sie eine Frage oder Anfrage zu Ihren gespeicherten Datensätzen eingeben. Diese Frage oder Aufforderung wird Filterkriterien zugeordnet und gibt Suchergebnisse zurück. RevealX 360- und RevealX Enterprise-Administratoren müssen sich für diese Funktion anmelden, die standardmäßig deaktiviert ist.



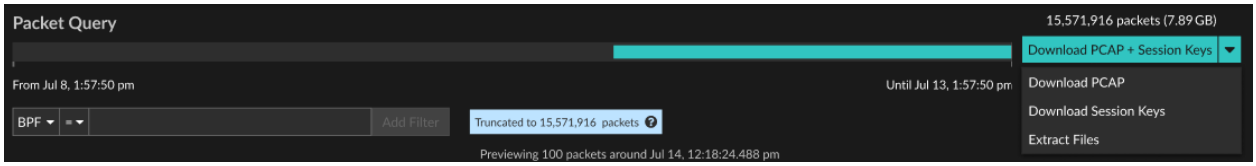
Datei-Analyse

Du kannst jetzt benutzerdefinierte Dateifilter erstellen die bestimmen, welche Dateien auf dem System mit dem SHA-256-Hashing-Algorithmus gehasht werden. Datei-Hashes, die einer Bedrohungssammlung entsprechen, generieren eine Erkennung, und Datei-Hashdaten können in Datensätzen abgefragt werden.

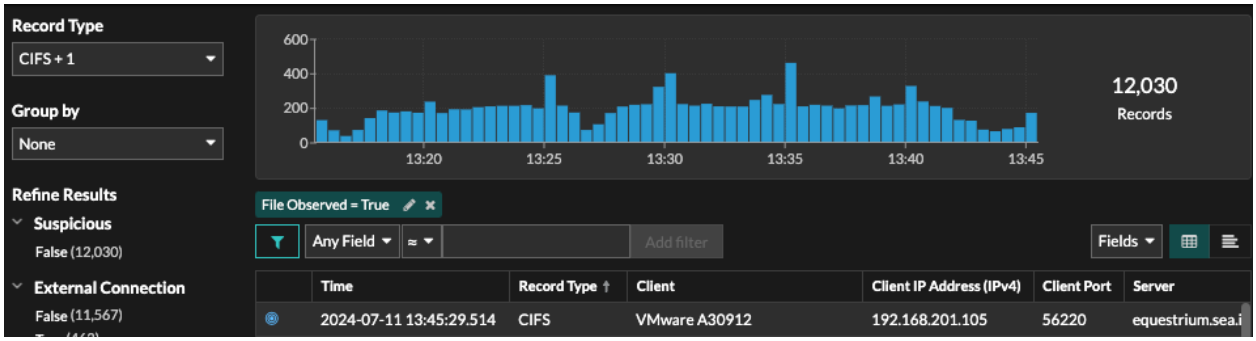


Dateiextraktion

Du kannst Extrahieren Sie Dateien aus Paketen die Daten aus dem HTTP- oder CIFS-Verkehr enthalten. Extrahierte Dateien werden in einer ZIP-Datei vom Browser auf Ihren lokalen Computer heruntergeladen. Die Dateiextraktion (auch bekannt als File Carving) ist nur für Benutzer mit Zugriff auf die Module NDR und Packet Forensics verfügbar.

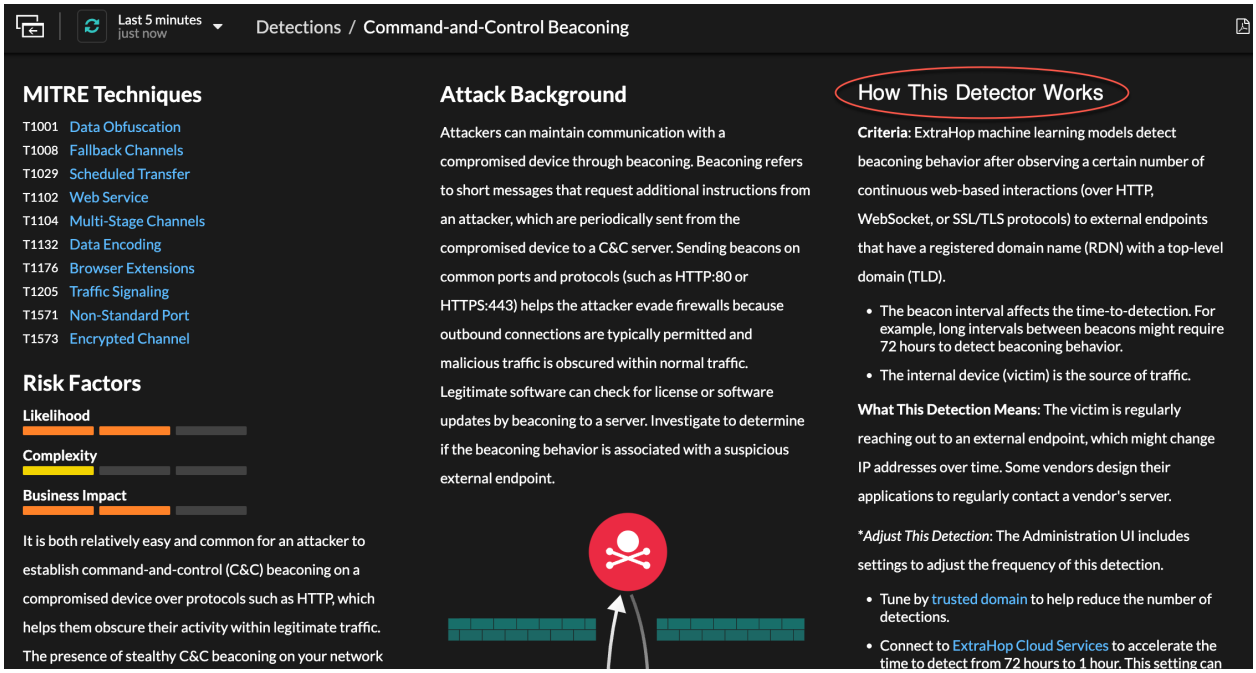


Auf der Seite „Datensätze“ können Sie nach HTTP- oder CIFS-Datensatztypen suchen und nach „Datei beobachtet“ filtern. Klicken Sie auf das Paketsymbol neben dem Datensatz, der den Dateien zugeordnet ist, die Sie extrahieren möchten.



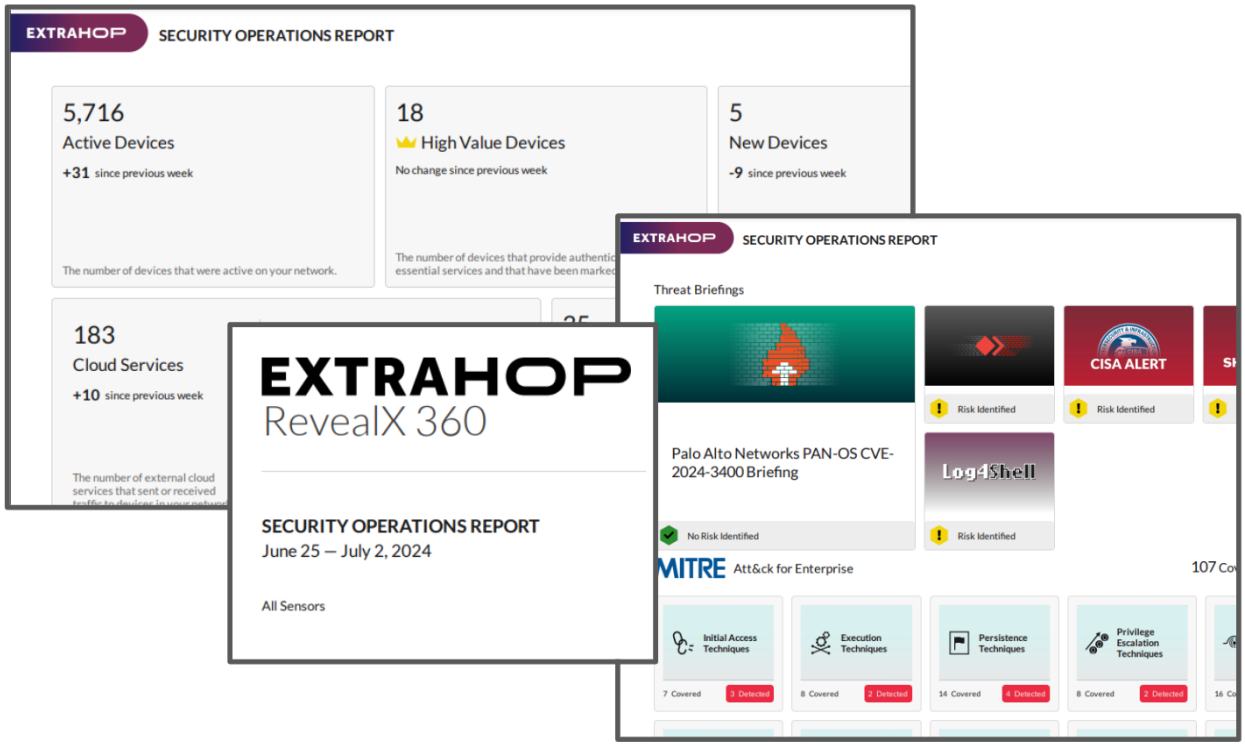
So funktioniert dieser Detektor

Für einige Erkennungstypen ist ein Abschnitt zur Funktionsweise dieses Melders verfügbar unter Erkennungsdetails Hier finden Sie Antworten auf häufig gestellte Fragen dazu, warum eine Erkennung in Ihrem ExtraHop-System erscheint.



Bericht über Sicherheitsoperationen

Der Security Operations Report (früher Executive Report genannt) enthält eine erweiterte Zusammenfassung wichtiger Systemindikatoren, die sich auf Ihre Angriffsfläche und Bedrohungsabdeckung beziehen.



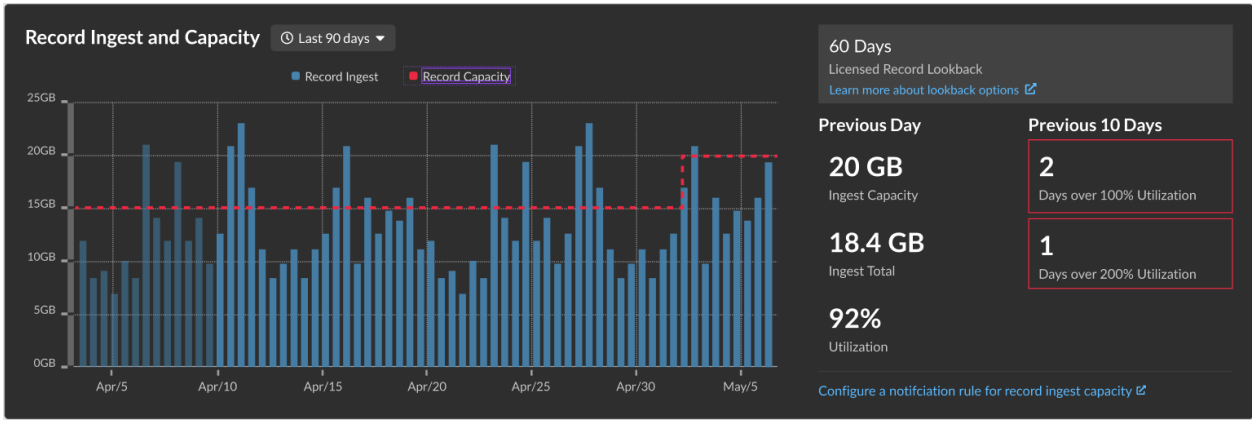
Für Administratoren

Neues maximales Sensorlimit

Das ExtraHop-System unterstützt jetzt Konsolen, die bis zu 250 Sensoren verwalten.

Lookback-Optionen für Aufzeichnungen

Aus dem Aufnahme- und Kapazitätsdiagramm aufzeichnen, ExtraHop-Administratoren für RevealX 360 können je nach Umfang des lizenzierten Datensatz-Lookbacks, das rechts neben dem Balkendiagramm angezeigt wird, ein Intervall von 30, 60, 90, 120 oder 180 Tagen auswählen.



Für API-Entwickler

API auslösen

Mit dem neuen können Sie jetzt Metriken speichern und auf Eigenschaften für NTP- und TFTP-Verkehr zugreifen `NTPMit` der `NTP-Klasse (Network Time Protocol)` können Sie `Metriken speichern und auf Eigenschaften zugreifen NTP_MESSAGE Ereignisse.` und `TFTPMit` der `TFTP-Klasse (Trivial FTP)` können Sie `Metriken speichern und auf Eigenschaften zugreifen TFTP_REQUEST und TFTP_RESPONSE Ereignisse.` Klassen.

REST-API

Du kannst jetzt Extrahieren Sie Dateien (auch bekannt als File Carving) aus Paketen über den `/packets/search` Endpunkt durch Angabe der `output` Parameter als `extract`.