

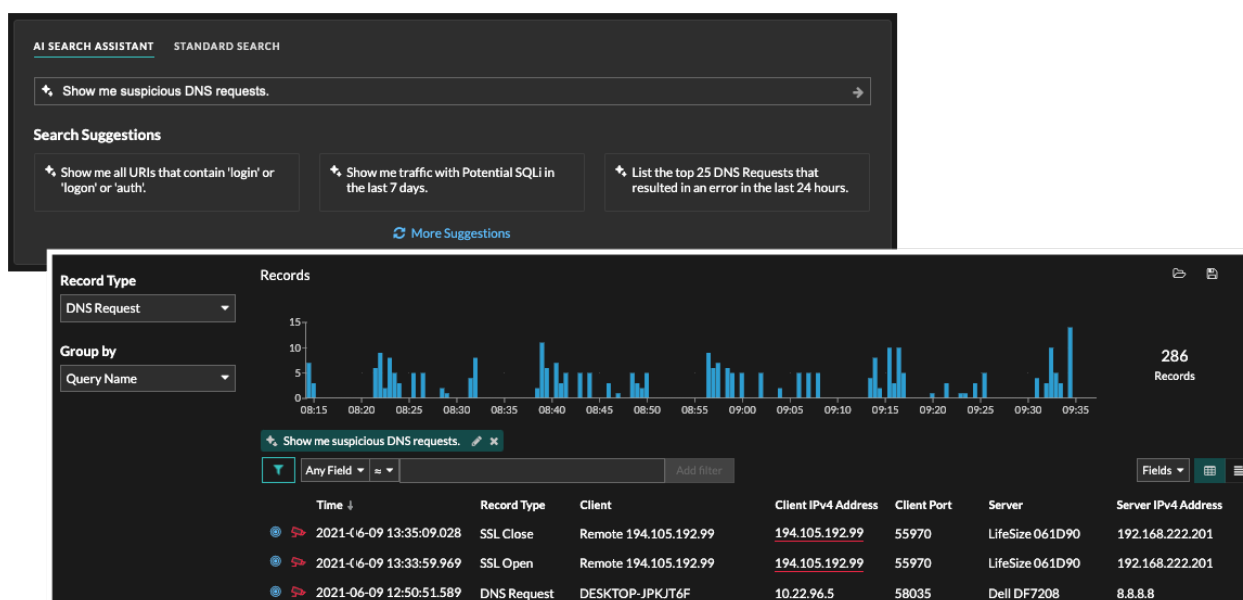
Was ist neu

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.

Create File Filter

Name

Malware Check - HTTP

Author

garyp

Protocol

HTTP

Locality

Inbound

File Format

☒ Media Type
☐ File Extension

Media Type

Executable

Archive

Document

✓ Executable

Cancel Save

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.

Packet Query

15,571,916 packets (7.89 GB)

Download PCAP + Session Keys

From Jul 8, 1:57:50 pm

Until Jul 13, 1:57:50 pm

Download PCAP

BPF Add Filter

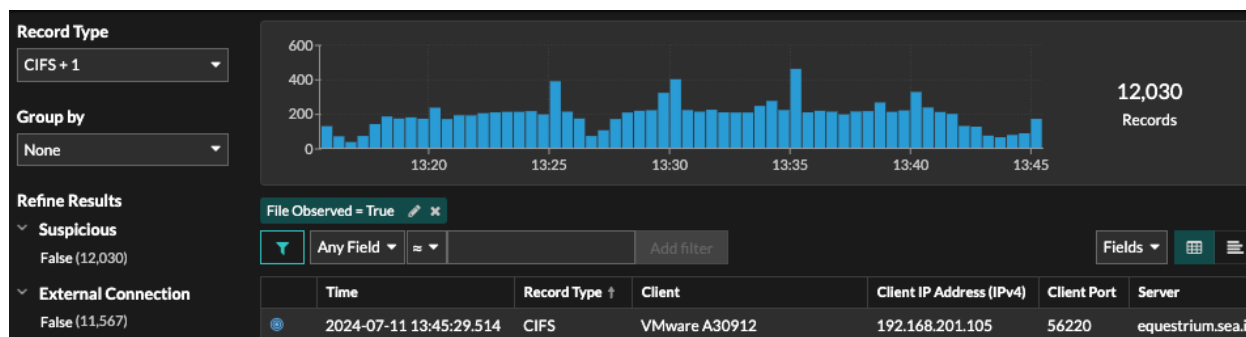
Download Session Keys

Truncated to 15,571,916 packets

Extract Files

Previewing 100 packets around Jul 14, 12:18:24.488 pm

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.

The screenshot shows the ExtraHop interface with the following sections:

- MITRE Techniques:**
 - T1001 Data Obfuscation
 - T1008 Fallback Channels
 - T1029 Scheduled Transfer
 - T1102 Web Service
 - T1104 Multi-Stage Channels
 - T1132 Data Encoding
 - T1176 Browser Extensions
 - T1205 Traffic Signaling
 - T1571 Non-Standard Port
 - T1573 Encrypted Channel
- Risk Factors:**
 - Likelihood:** High
 - Complexity:** Medium
 - Business Impact:** High
- Attack Background:**

Attackers can maintain communication with a compromised device through beaconing. Beaconing refers to short messages that request additional instructions from an attacker, which are periodically sent from the compromised device to a C&C server. Sending beacons on common ports and protocols (such as HTTP:80 or HTTPS:443) helps the attacker evade firewalls because outbound connections are typically permitted and malicious traffic is obscured within normal traffic. Legitimate software can check for license or software updates by beaconing to a server. Investigate to determine if the beaconing behavior is associated with a suspicious external endpoint.
- How This Detector Works:**

Criteria: ExtraHop machine learning models detect beaconing behavior after observing a certain number of continuous web-based interactions (over HTTP, WebSocket, or SSL/TLS protocols) to external endpoints that have a registered domain name (RDN) with a top-level domain (TLD).

 - The beacon interval affects the time-to-detection. For example, long intervals between beacons might require 72 hours to detect beaconing behavior.
 - The internal device (victim) is the source of traffic.

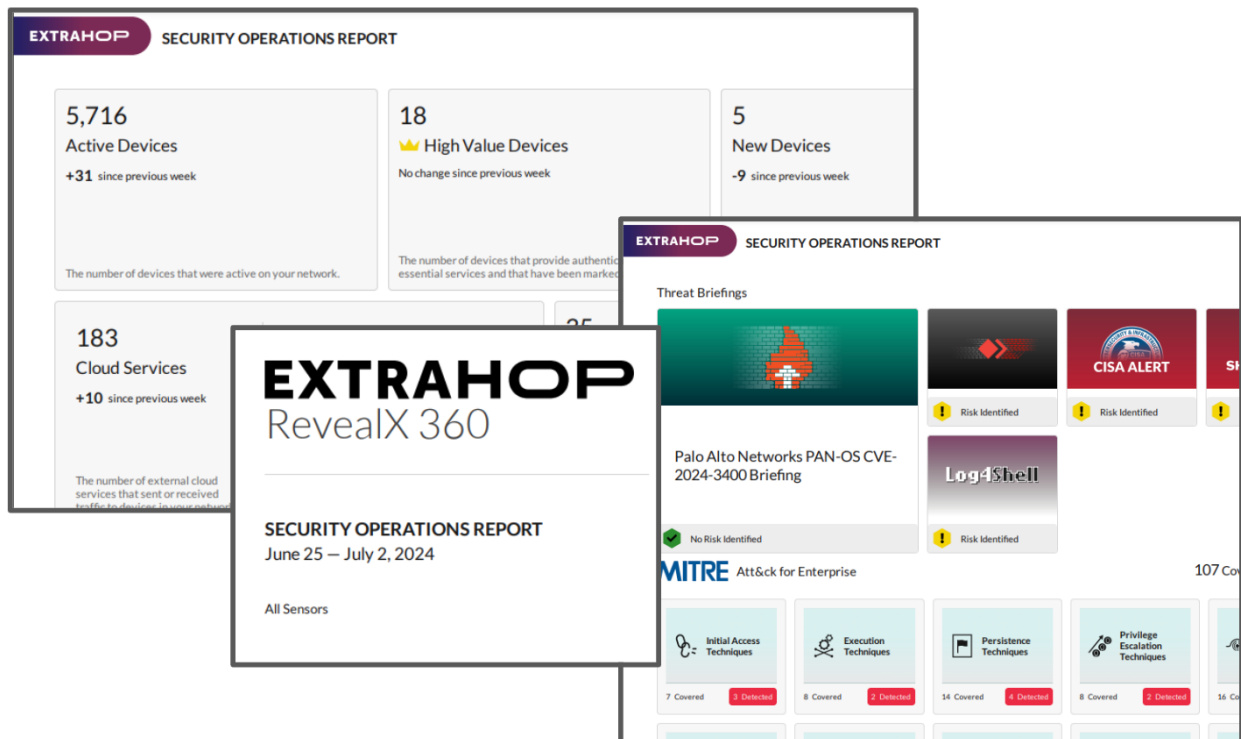
What This Detection Means: The victim is regularly reaching out to an external endpoint, which might change IP addresses over time. Some vendors design their applications to regularly contact a vendor's server.

***Adjust This Detection:** The Administration UI includes settings to adjust the frequency of this detection.

 - Tune by **trusted domain** to help reduce the number of detections.
 - Connect to **ExtraHop Cloud Services** to accelerate the time to detect from 72 hours to 1 hour. This setting can

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.



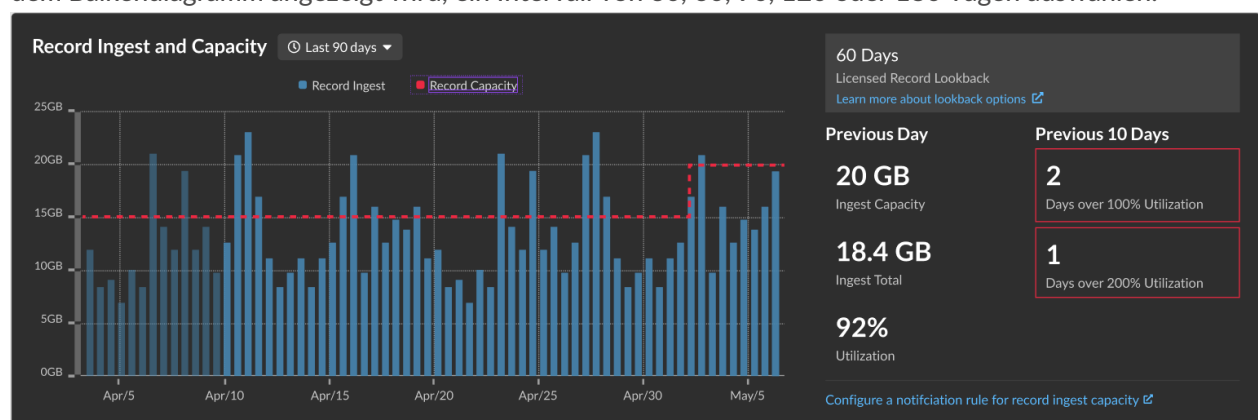
Für Administratoren

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.