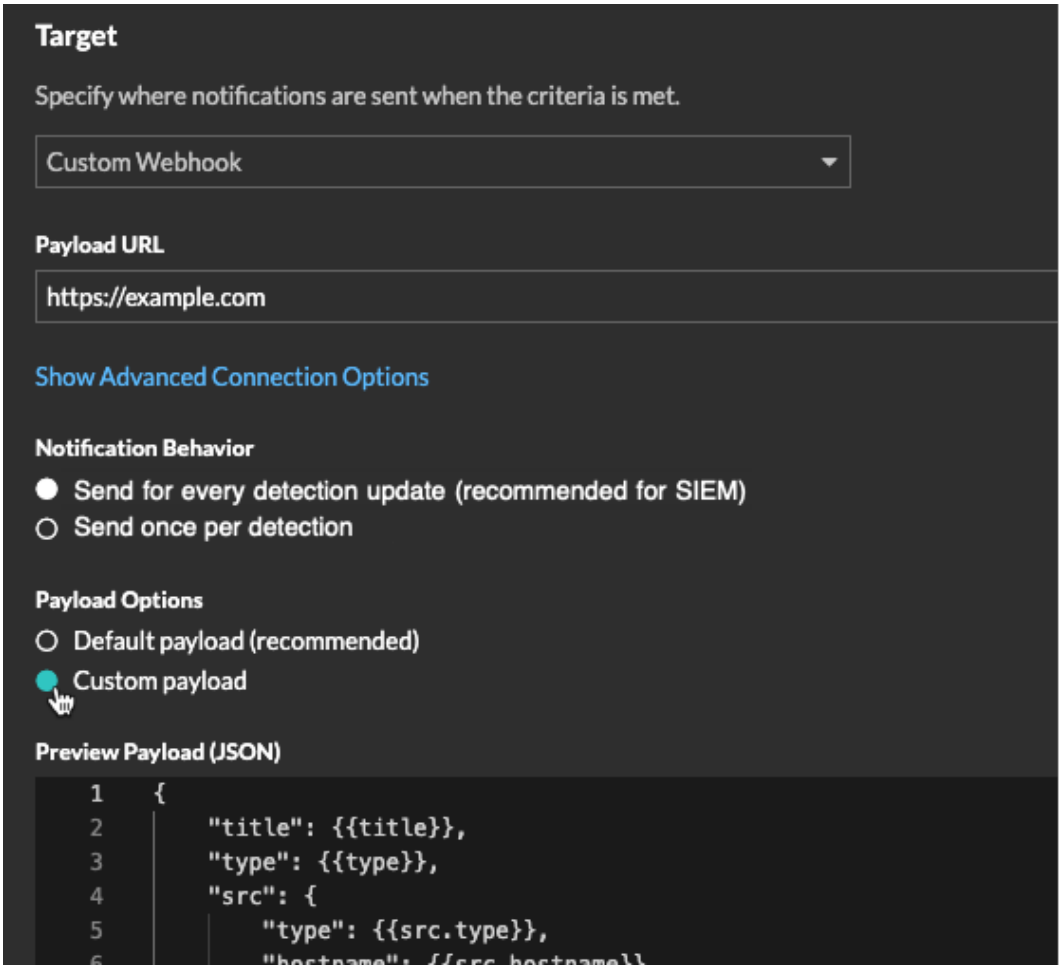
Was ist neu

Veröffentlicht: 2024-10-26

Während Versionshinweise geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.8.

Verbesserte Erkennungsbenachrichtigungen

Erkennungen und Erkennungsbenachrichtigungen wurden für den Export granularer Erkennungsdaten optimiert. Benutzer können jetzt Benachrichtigungsregeln konfigurieren um eine standardmäßige oder benutzerdefinierte Webhook-Nutzlast für jedes Erkennungsupdate zu senden oder nur eine Benachrichtigung für jede Erkennung zu senden.

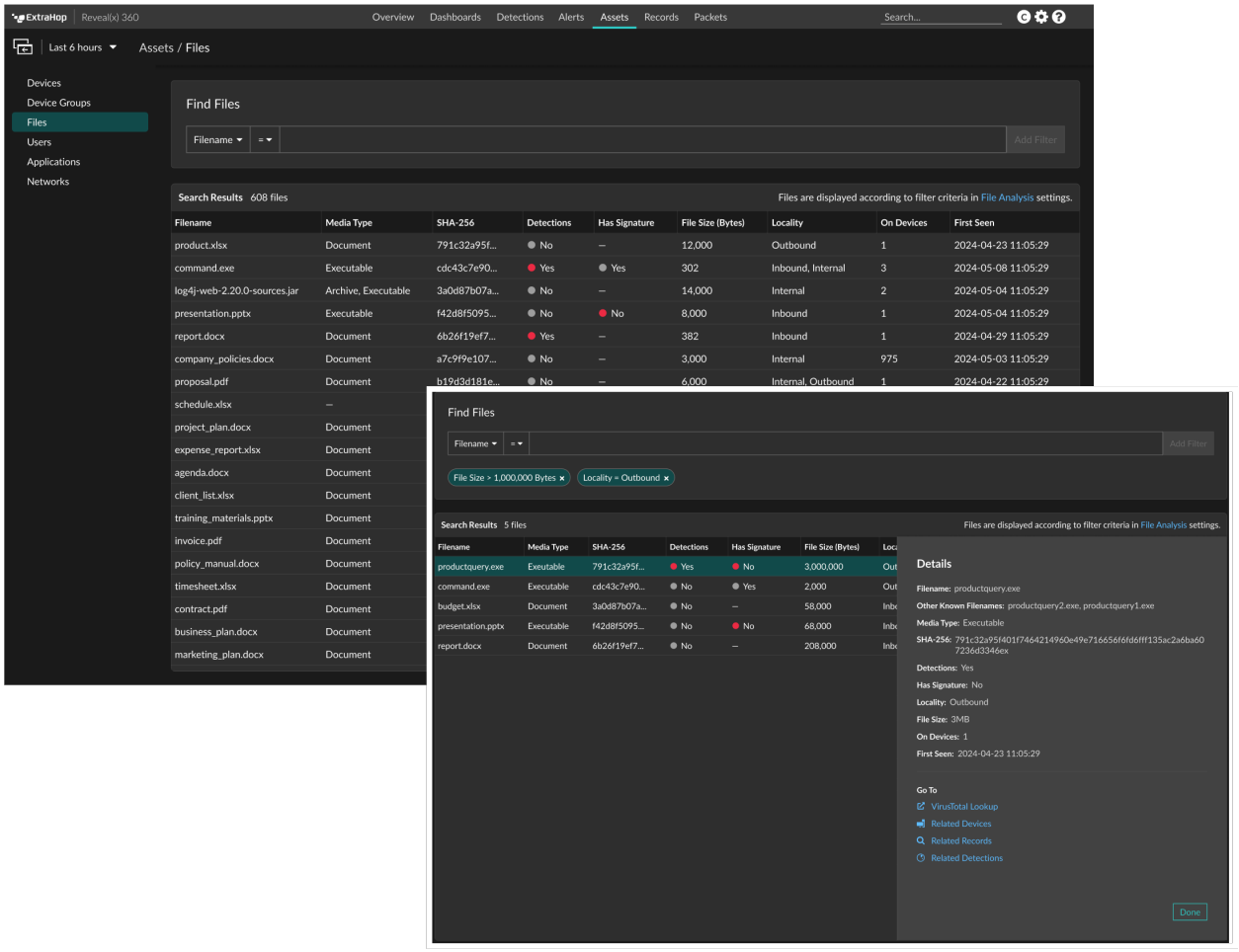


Bericht über Sicherheitsoperationen

Sie können jetzt den Inhalt auswählen, der in eine aufgenommen werden soll Bericht über Sicherheitsoperationen die Sie von einer Übersichtsseite aus generieren.

Seite „Neue Dateien“

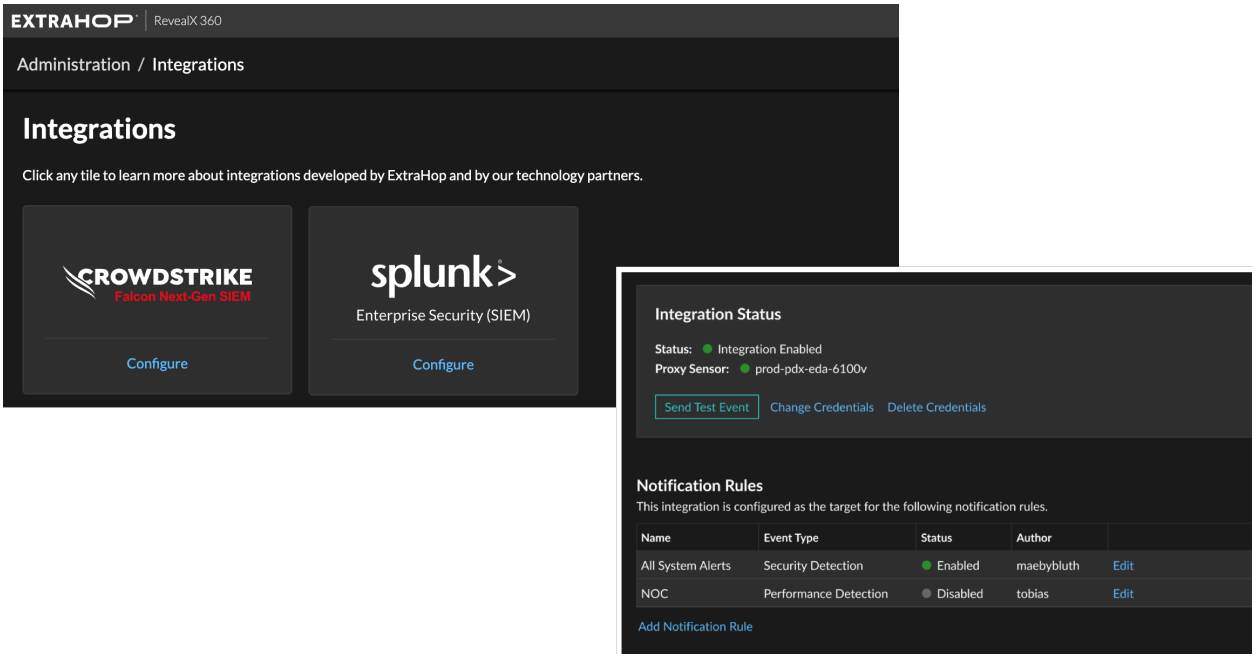
Das Seite „Dateien“ zeigt eine Tabelle mit Dateien an, die gemäß Filtern gehasht wurden, die in den Dateianalyse-Einstellungen konfiguriert und aktiviert wurden. Mithilfe von Dateidetails können Sie den SHA-256-Datei-Hash in Geräten, Datensätzen, Erkennungen und VirusTotal Lookup, einem Drittanbieter-Tool, weiter untersuchen.



Neue RevealX 360-Integrationen

SIEM-Integrationen der nächsten Generation

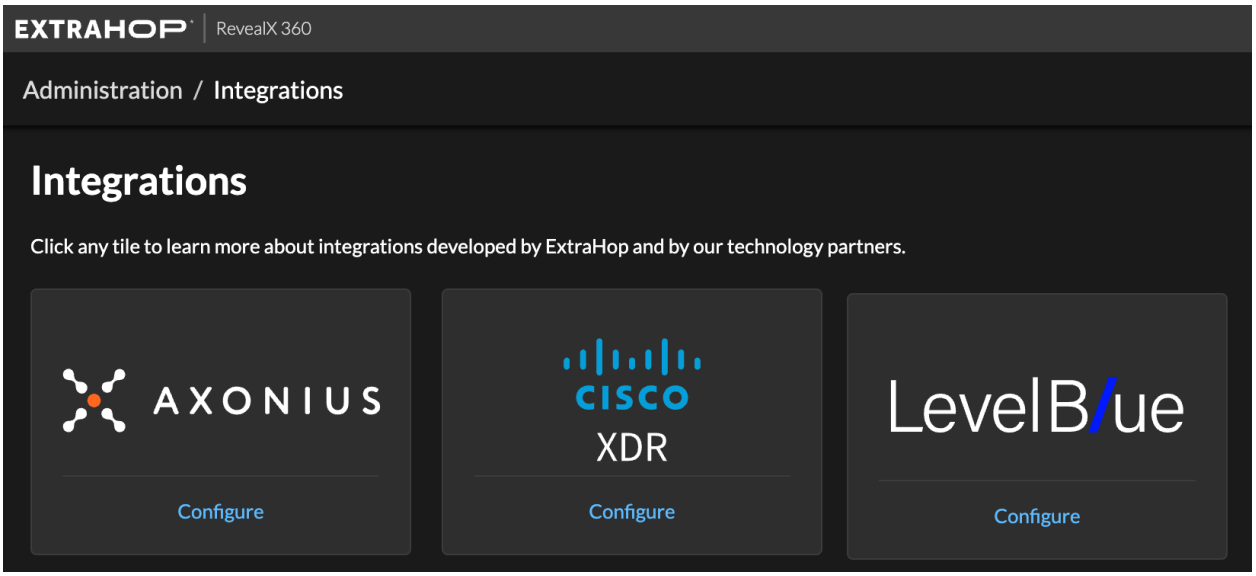
Integrationen hinzugefügt für CrowdStrike Falcon SIEM der nächsten Generation und Splunk SIEM für Unternehmenssicherheit diese Hebelwirkung Regeln für Benachrichtigungen um ExtraHop-Erkennungsdaten in das Ziel-SIEM zu exportieren.



Integrationen von LevelBlue, Axonius und Cisco XDR

Die folgenden neuen Integrationen wurden hinzugefügt, um Ihnen zu helfen, Gerät- und Erkennungsdaten zu untersuchen und darauf zu reagieren:

- Level Blau bietet Managed Erkennung and Response (MDR).
- Axonius ist ein Tool zur Verwaltung Asset Cybersicherheitsressourcen.
- Cisco XDR ist eine Cloud-basierte erweiterte Erkennung- und Reaktionslösung.

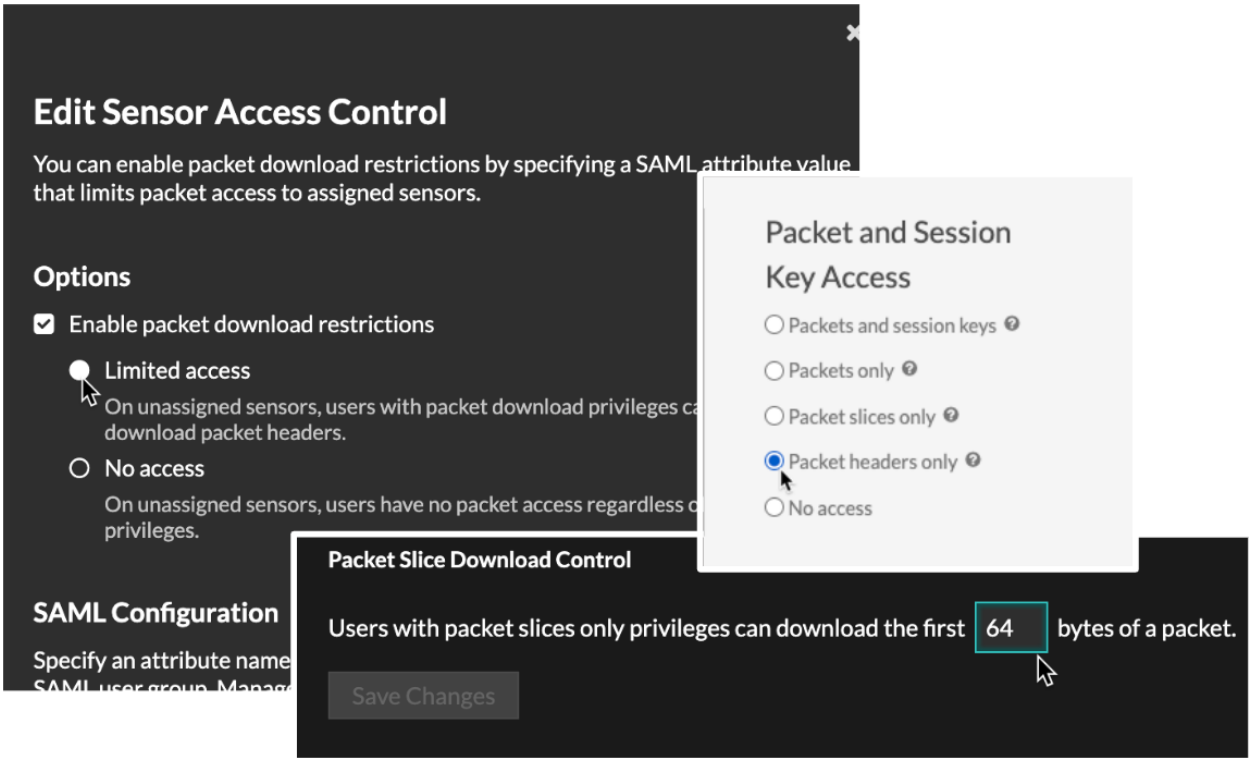


Für Administratoren

Paketzugriffskontrolle

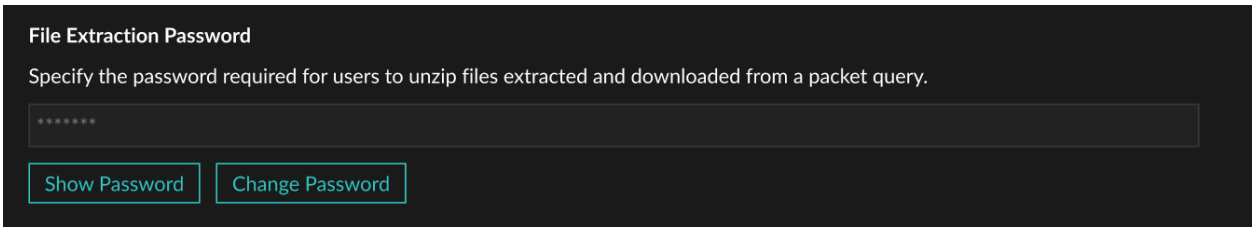
Administratoren können jetzt gewähren Privilegien die es Benutzern ermöglichen, nur Paket-Header herunterzuladen. RevealX 360-Administratoren können auch eine einrichten globale Politik

für Paketsegmentgröße und Sensorzugriffskontrolle aktivieren um bestimmten Benutzergruppen Zugriff zu gewähren.



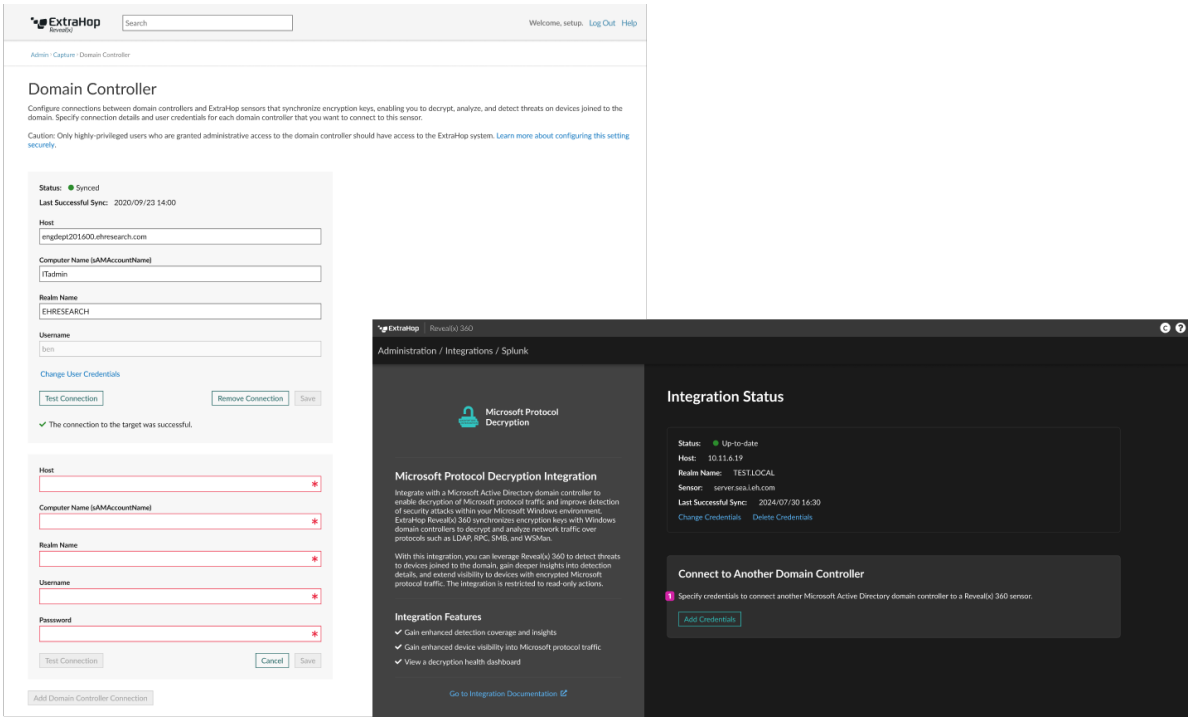
Passwort für die Dateiextraktion

Zum Öffnen von.zip-Dateien, die aus Paketen extrahiert oder geschnitzt wurden, ist ein Passwort erforderlich. Administratoren können das Passwort für die Dateiextraktion in den Administrationseinstellungen auf festlegen RevealX Enterprise oder RevealX 360 und teilen Sie das Passwort mit zugelassenen Benutzern.



Entschlüsselung für mehrere Domänencontroller

Das ExtraHop-System jetzt unterstützt die Verbindung mehrerer Domänencontroller zu einem Sensor, um den Domänencontroller-Verkehr zu entschlüsseln. Sie können die Entschlüsselung auf einem einzelnen Sensor auf RevealX Enterprise oder über eine Integration auf RevealX 360 konfigurieren.



Für API-Entwickler

API auslösen

Sie können jetzt Metriken speichern und auf Eigenschaften für SOCKS- und NMF-Verkehr zugreifen mit neuen SOCKS und NMF Klassen.

REST-API

Das wurde hinzugefügt `/appliances/sensortags` Endpunkt zum RevealX 360 REST-API, mit dem Sie Sensor-Tags anzeigen und verwalten können.