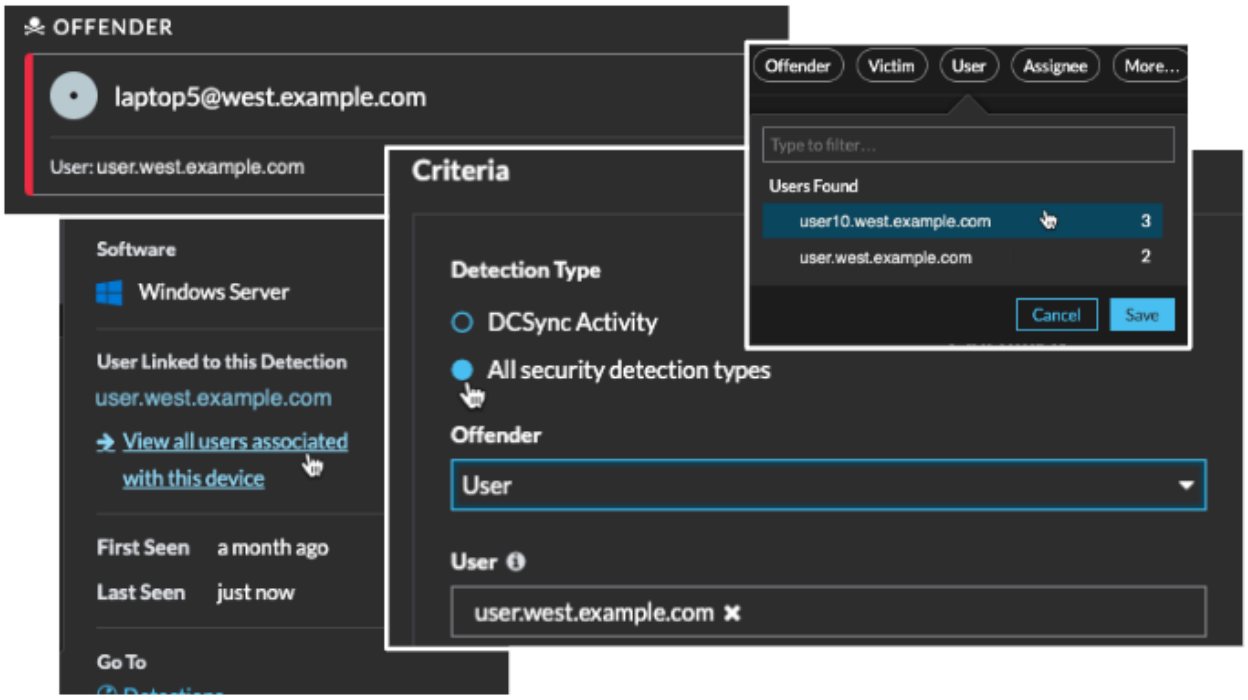
Quoi de neuf

Publié: 2025-02-04

Alors que notes de version pour un aperçu complet de nos mises à jour de versions, voici un aperçu des fonctionnalités les plus intéressantes d'ExtraHop 9.9.

Utilisateurs dans les détections

Les noms d'utilisateur sont désormais inclus dans les informations relatives aux participants à la détection lorsqu'elles sont disponibles. Tu peux détections de filtres par utilisateur, consultez les utilisateurs spécifiques liés aux détections dans résumés des détections et informations sur les participants, et ajoutez un nom d'utilisateur de participant en tant que règle de réglage ou notification de détection critères.



Journal de détection

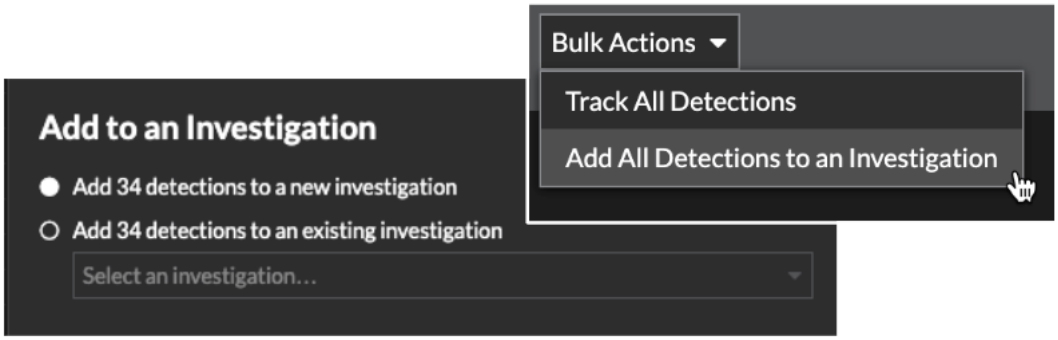
Détails de détection contiennent désormais un journal horodaté de l'activité associée à la détection. Le journal de détection répertorie toutes les mises à jour associées à la détection et règles d'exceptions associée à une activité spécifique.

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	–

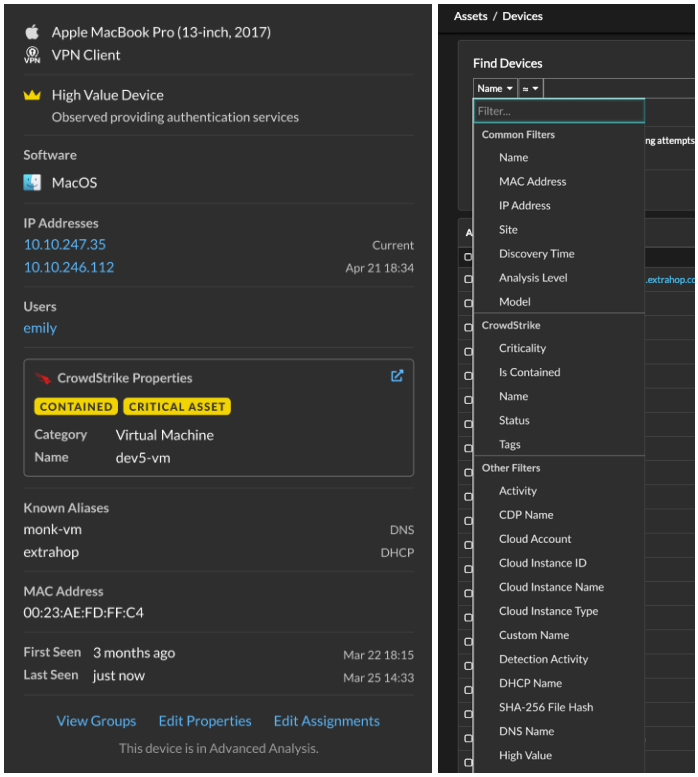
Actions groupées

Vous pouvez désormais ajouter toutes les détections dans un résumé de la détection à une enquête. Dans le nouveau menu déroulant Actions groupées, vous pouvez suivre toutes les détections dans le résumé ou ajoutez toutes les détections à un investigation.



Propriétés des appareils mises à jour dans le cloud

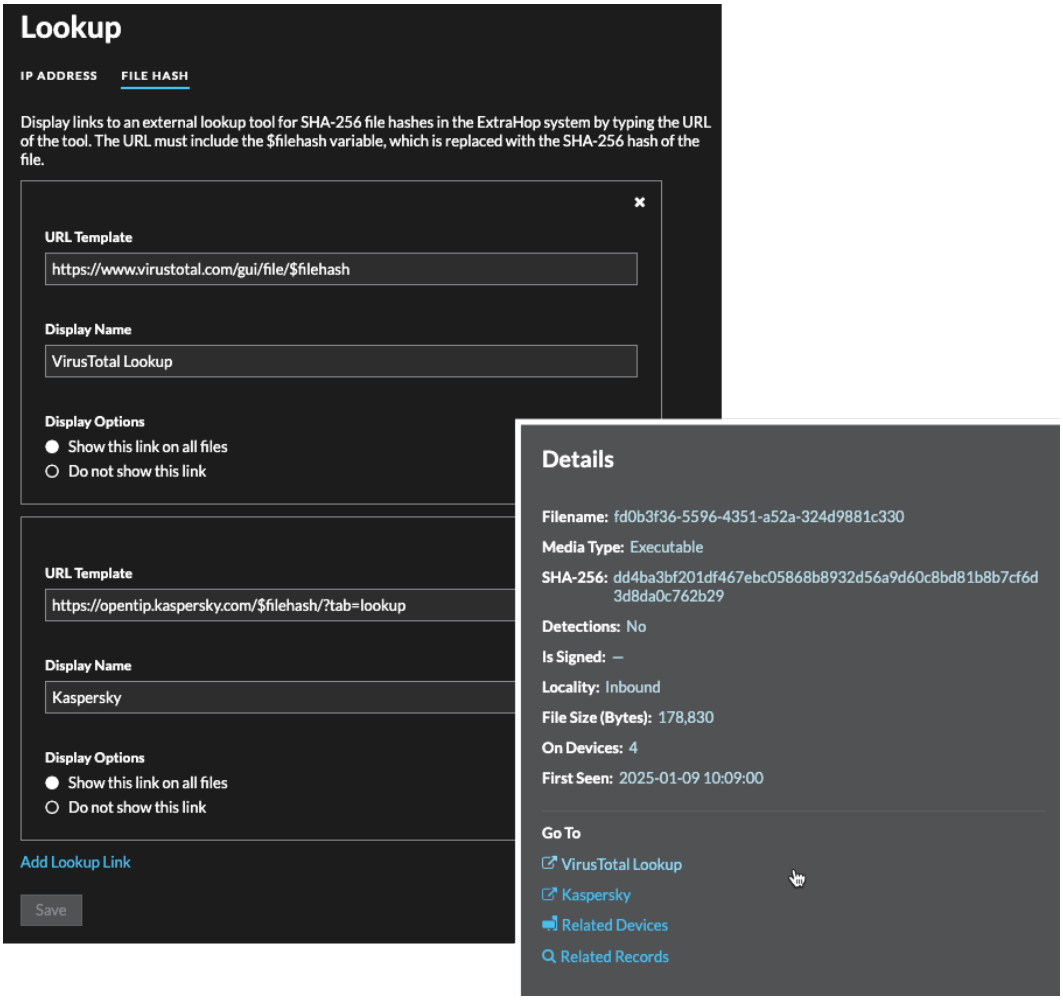
(RevealX 360 uniquement) Ajout de la prise en charge de l'affichage mis à jour dans le cloud propriétés de l'équipement obtenu auprès de intégrations configuré sur votre système ExtraHop, tel que CrowdStrike. Vous pouvez filtrer par propriétés d'équipement cloud pour trouver un équipement et à créer un groupe dcesséquipements dynamique.



Pour les administrateurs

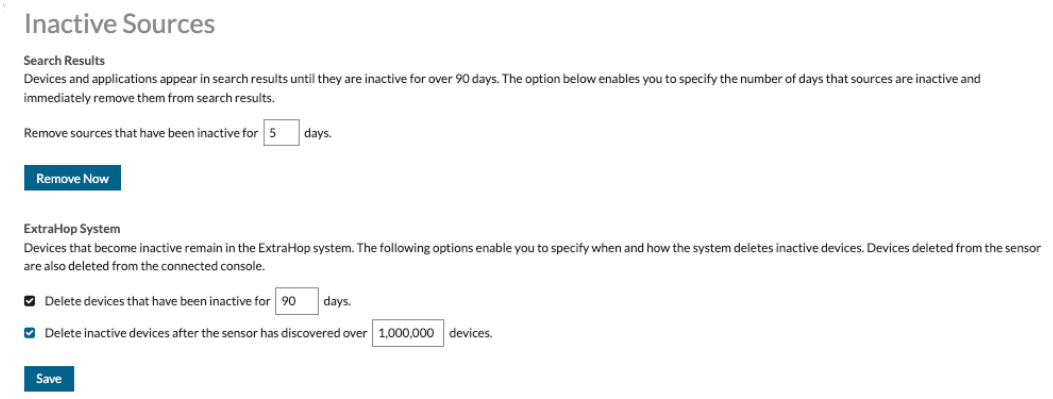
Liens de recherche de hachage de fichiers

Ajout de la possibilité de configurer des liens vers des outils de recherche externes pour rechercher facilement les hachages de fichiers SHA-256 pour RevealX 360 et RevealX Enterprise. VirusTotal Lookup est configuré par défaut. Les liens configurés sont affichés sur les pages Appareils, Fichiers, Enregistrements et Détections.



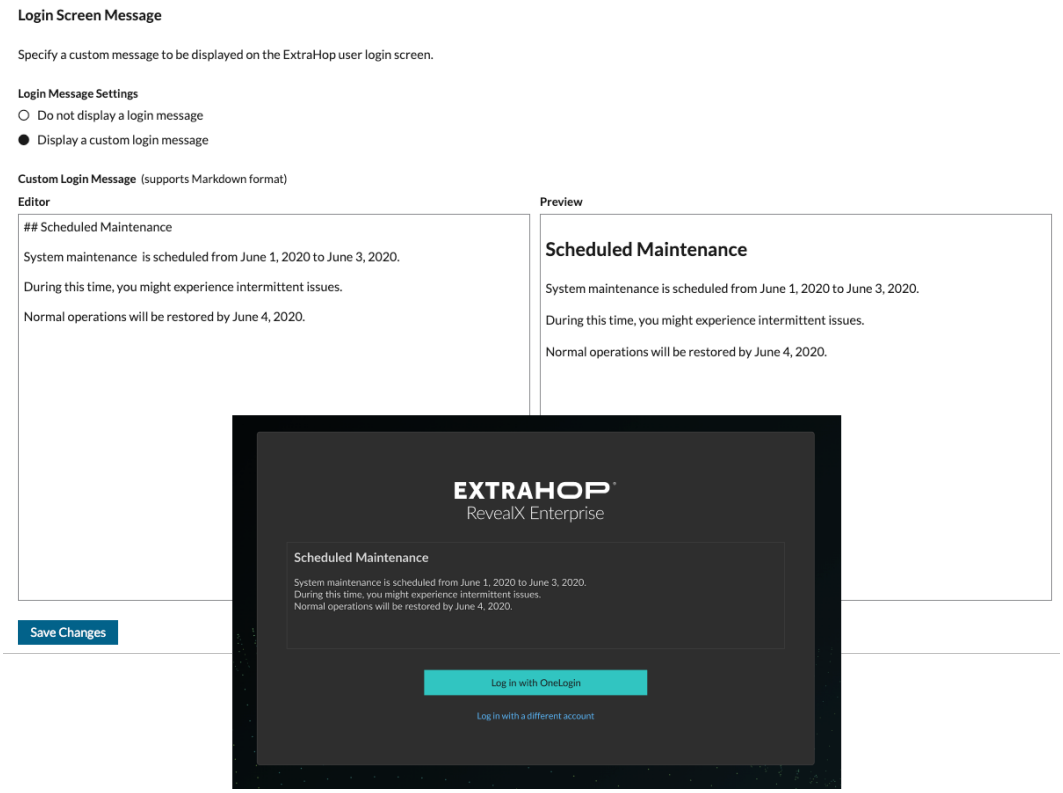
Suppression d'appareils inactifs

Vous pouvez spécifier quand et comment le système fonctionne automatiquement supprime les appareils inactifs du système ExtraHop. Vous pouvez supprimer des appareils qui sont restés inactifs pendant un certain nombre de jours et vous pouvez supprimer des appareils inactifs une fois que la sonde en a découvert plus d'un certain nombre.



Message sur l'écran de connexion

(RevealX Enterprise uniquement) Vous pouvez ajouter un message personnalisé à l'écran de connexion de votre système ExtraHop pour afficher des graphiques et des logos et pour transmettre des informations aux utilisateurs telles que les exigences en matière de mot de passe, les déclarations de politique, les liens d'assistance ou les annonces de maintenance. Le message de l'écran de connexion prend en charge le texte et les graphiques dans Syntaxe Markdown.



Pour les développeurs d'API

API REST

A ajouté le `/users/{username}/lock` point de terminaison du Ressource pour les utilisateurs, qui vous permet de déverrouiller des comptes utilisateurs. Ce point de terminaison n'est accessible que si vous avez configuré le système pour verrouiller automatiquement les comptes utilisateurs après un certain nombre de tentatives de connexion infructueuses via le fichier de configuration en cours d'exécution.