

Comment supprimer les noms de recherche corrélés en double dans la liste déroulante Examen des incidents de sécurité d'entreprise (ES)

Applicabilité

Splunk Enterprise Security

Description

La création de nouvelles recherches de corrélation à partir de recherches de corrélation existantes peut entraîner des noms en double dans la liste déroulante de révision des incidents.

Lorsque les recherches de corrélation s'exécutent, elles peuvent créer des événements notables, ces événements étant liés à ces recherches.

Comme ces événements peuvent nécessiter d'étudier ces événements notables dans le futur, les recherches de corrélation qui déclenchent ces événements sont conservées, ce qui peut conduire à l'affichage de noms en double.

Si vous êtes sûr que vous n'aurez pas besoin d'enquêter sur ces anciens notables liés à ces recherches, les noms dupliqués peuvent être supprimés.

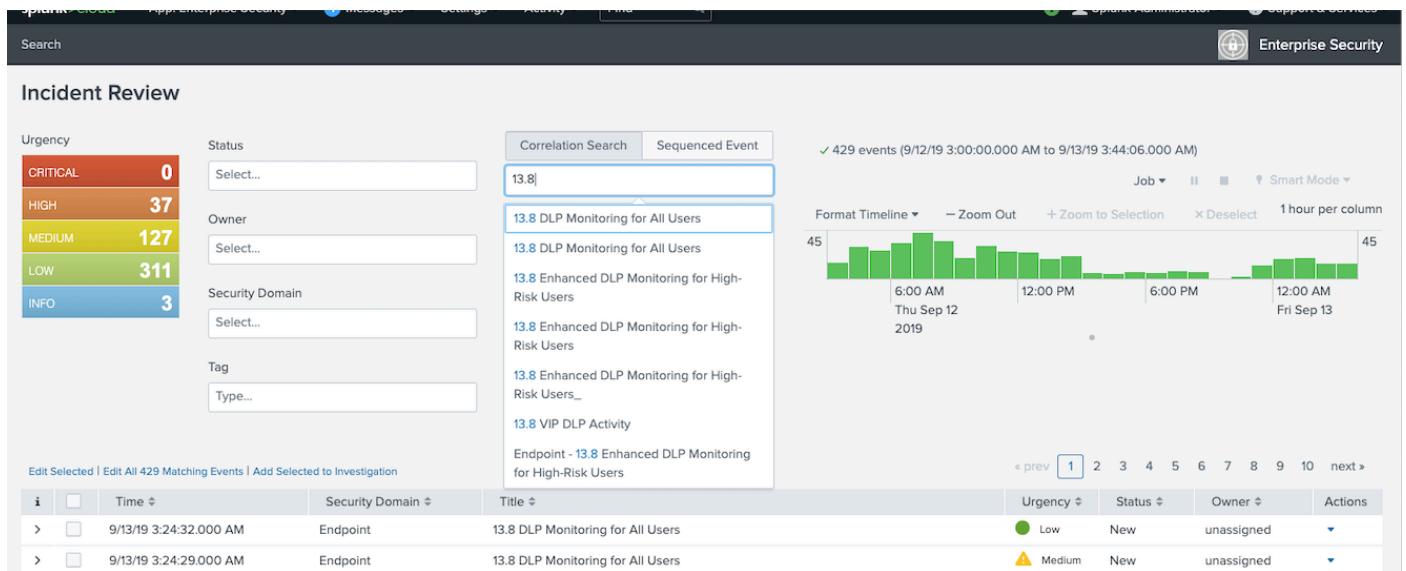
Si vous pensez avoir besoin de les examiner, il est préférable de laisser les doublons.

Une recherche appelée « Threat - Correlation Searches - Lookup Gen » s'exécute et crée les noms des règles de recherche de corrélation, elle ajoute les noms à un kvstore appelé `corRelationsearches_lookup`.

Il est possible de supprimer les doublons, mais comme mentionné ci-dessus, cela peut avoir un impact sur les investigations d'événements précédents.

Enquête

La révision des incidents ES peut afficher des noms en double.



Résolution

Suppression des entrées en double.

1) Faites une copie de sauvegarde du kvstore, en exécutant le fichier et exportez-le vers un fichier CSV, cela peut être utilisé pour récupérer ce kvstore si nécessaire.

```
| inputlookup correlationsearches_lookup
```

2) Pour supprimer un doublon, lancez une recherche en supprimant le nom dupliqué et en le remplaçant dans le kvstore.

Dans cet exemple, j'ai utilisé le nom de règle « 01.XYZ Duplicate search ». Remplacez ce nom par un nom en double que vous souhaitez supprimer.

```
| inputlookup correlationsearches_lookup | search rule_name != "01.XYZ Duplicate search"
| outputlookup correlationsearches_lookup
```

Lorsque la recherche "01.XYZ Recherche dupliquée" s'exécute à nouveau, le nom de la règle manquante doit être renseigné dans le kvstore, et apparaître à nouveau dans la liste.

Comme vous avez une copie du kvstore dans CSV, il peut être fait comme un fichier de recherche, puis utilisé pour écraser le kvstore corRelationsearches_lookup et le recréer à partir de la sauvegarde.

Liens connexes

Réponses Splunk

[Pourquoi la page Analyse des incidents ES répertorie-t-elle toujours les recherches de corrélation supprimées dans la zone de sélection multiple « Nom de la recherche de corrélation » ?](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.