

Come eliminare i nomi delle ricerche di correlazione duplicati nell'elenco a discesa Esame degli incidenti di Enterprise Security (ES)

Applicabilità

Splunk Enterprise Security

Descrizione

La creazione di nuove ricerche di correlazione da ricerche di correlazione esistenti può causare la presenza di nomi duplicati nell'elenco a discesa per la revisione degli incidenti.

Quando le ricerche di correlazione vengono eseguite, possono creare eventi di rilievo, tali eventi sono collegati a tali ricerche.

Poiché questi eventi potrebbero richiedere l'analisi di questi eventi importanti in futuro, le ricerche di correlazione che attivano questi eventi vengono mantenute, ciò può portare alla visualizzazione di nomi duplicati.

Se si è certi che non sarà necessario analizzare le note meno recenti relative a queste ricerche, i nomi dei duplicati possono essere eliminati.

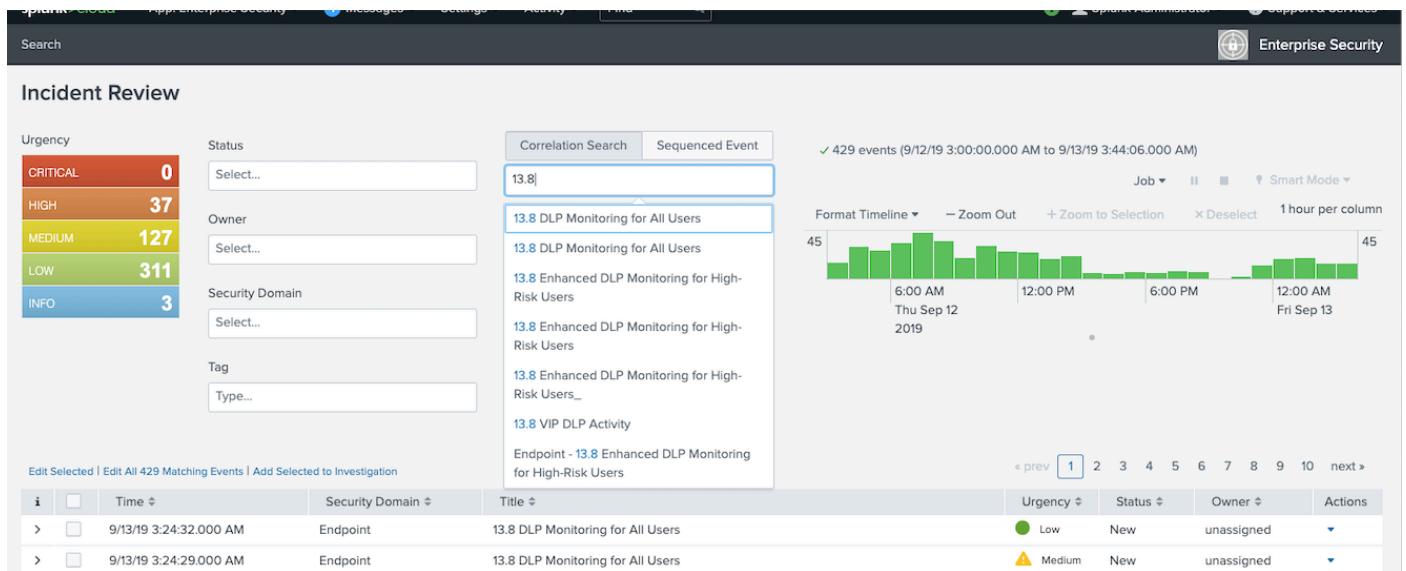
Se pensi di dover indagare su di loro, è meglio lasciare i duplicati.

Viene eseguita una ricerca denominata "Minaccia - Ricerche di correlazione - Generazione ricerca" che crea i nomi delle regole di ricerca di correlazione e li aggiunge a un kvstore denominato `correlations_lookup`.

È possibile eliminare i duplicati, ma, come accennato in precedenza, ciò può influire sulle indagini relative a eventi precedenti.

Indagine

Dalla revisione degli incidenti ES possono essere visualizzati nomi duplicati.



Risoluzione

Eliminazione delle voci duplicate.

1) Creare una copia di backup del kvstore, eseguire il file ed esportarlo in un file CSV, questo può essere utilizzato per recuperare questo kvstore, se necessario.

```
| inputlookup correlationsearches_lookup
```

2) Per eliminare un duplicato, eseguire una ricerca rimuovendo il nome duplicato e loro sovrascrivendo nuovamente questo sul kvstore.

In questo esempio è stato utilizzato il nome della regola "01.XYZ Duplicate search". Sostituire il nome con qualsiasi nome duplicato che si desidera rimuovere.

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

Quando la ricerca "01.XYZ Duplicate search" viene eseguita nuovamente, il nome della regola mancante deve essere compilato nel kvstore, visualizzando di nuovo nell'elenco.

Poiché si dispone di una copia di kvstore in CSV, è possibile crearla come file di ricerca, quindi utilizzarla per sovrascrivere kvstore correlations_lookup e ricrearla dal backup.

Collegamenti correlati

Risposte Splunk

[Perché la pagina Esamina incidente ES elenca ancora Ricerche di correlazione eliminate nella casella Multiselect "Nome ricerca correlazione"?](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).