

Hoe dubbele correlatienamen te verwijderen in de vervolgkeuzelijst Enterprise Security (ES) Incident Review

toepasbaarheid

Splunk Enterprise-beveiliging

Beschrijving

Het maken van nieuwe correlatie zoekopdrachten van bestaande correlatie zoekopdrachten kan dubbele namen in de incident review drop down lijst veroorzaken.

Wanneer de correlatiezoekopdrachten worden uitgevoerd, kunnen ze opmerkelijke gebeurtenissen maken, deze gebeurtenissen zijn gekoppeld aan die zoekopdrachten. Aangezien deze gebeurtenissen in de toekomst deze opmerkelijke gebeurtenissen mogelijk moeten onderzoeken, worden de correlatiezoekopdrachten die deze gebeurtenissen activeren bewaard, dit kan ertoe leiden dat dubbele namen worden weergegeven.

Als u er zeker van bent dat u deze oudere notabelen met betrekking tot deze zoekopdrachten niet hoeft te onderzoeken, kunnen de dubbele namen worden verwijderd.

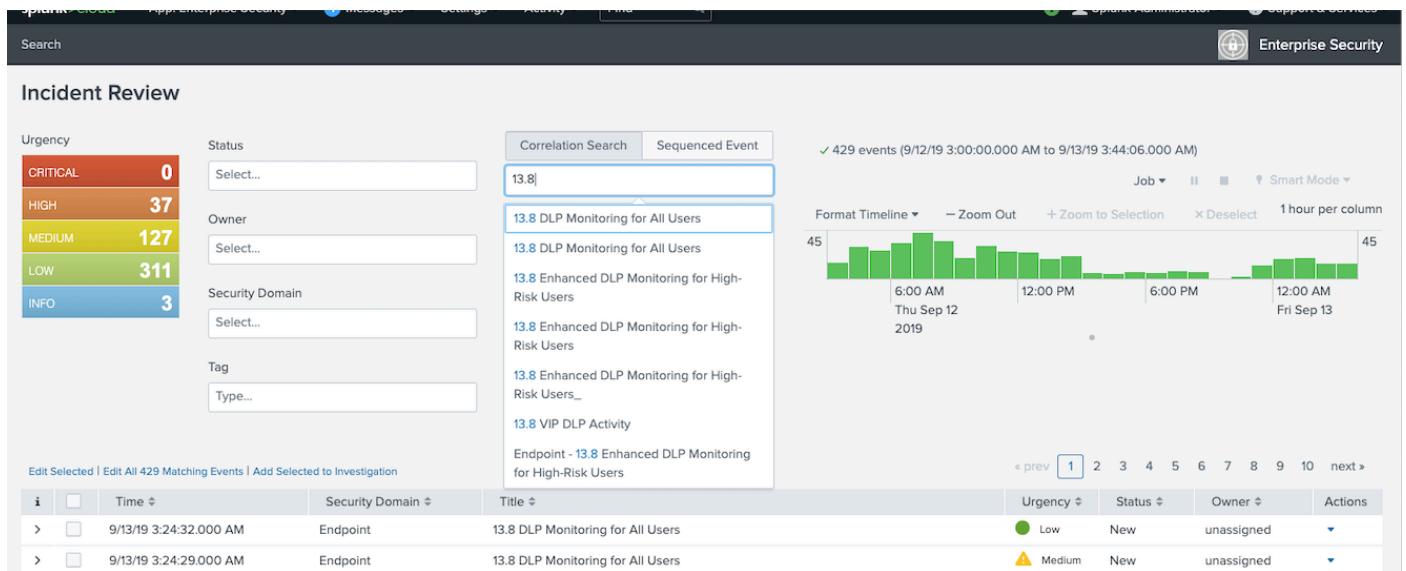
Als je denkt dat je ze misschien moet onderzoeken, is het beter om de duplicaten achter te laten.

Een zoekopdracht met de naam "Threat - Correlation Searches - Lookup Gen" wordt uitgevoerd en maakt de namen van de correlatieregels, deze voegt de namen toe aan een kvstore met de naam correlationsearches_lookup.

Het is mogelijk om duplicaten te verwijderen, maar zoals hierboven vermeld, kan dit van invloed zijn op onderzoeken naar eerdere gebeurtenissen.

onderzoek

In de ES incident review ziet u mogelijk dubbele namen.



resolutie

Dubbele vermeldingen verwijderen.

1) Maak een back-up kopie van de kvstore, het uitvoeren van het bestand en deze exporteren naar een CSV-bestand, dit kan worden gebruikt om deze kvstore te herstellen indien nodig.

```
| inputlookup correlationsearches_lookup
```

2) Als u een duplicaat wilt verwijderen, voert u een zoekopdracht uit waarbij de duplicaatnaam wordt verwijderd en deze wordt overschreven naar de kvstore. In dit voorbeeld heb ik de regelnaam "01.XYZ Duplicate search" gebruikt. Wijzig deze naam in een dubbele naam die u wilt verwijderen.

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

Wanneer de zoekopdracht "01.XYZ Duplicate search" opnieuw wordt uitgevoerd, moet de ontbrekende regelnaam in de kvstore worden ingevuld en opnieuw in de lijst worden weergegeven.

Aangezien u een kopie van de kvstore in CSV hebt, kan deze worden gemaakt als een opzoekbestand en vervolgens worden gebruikt om de kvstore correlationsearches_lookup te overschrijven en opnieuw te maken vanuit de back-up.

Gerelateerde links

Splunk Antwoorden

[Waarom wordt op de ES Incident Review-pagina nog steeds een lijst met verwijderde correlatiezoekopdrachten weergegeven in het vak Multiselect "Correlation Search Name"?](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.