

Como excluir nomes de pesquisas de correlação duplicadas na lista suspensa de análise de incidentes do Enterprise Security (ES)

Aplicabilidade

Segurança corporativa Splunk

Descrição

A criação de novas pesquisas de correlação a partir de pesquisas de correlação existentes pode causar nomes duplicados na lista suspensa de análise de incidentes.

Quando as pesquisas de correlação são executadas, elas podem criar eventos notáveis, que são vinculados a essas pesquisas.

Como esses eventos podem precisar investigar esses eventos notáveis no futuro, as pesquisas de correlação que desencadeiam esses eventos são mantidas, isso pode levar à exibição de nomes duplicados.

Se você tiver certeza de que não precisará investigar esses nomes mais antigos relacionados a essas pesquisas, os nomes duplicados poderão ser excluídos.

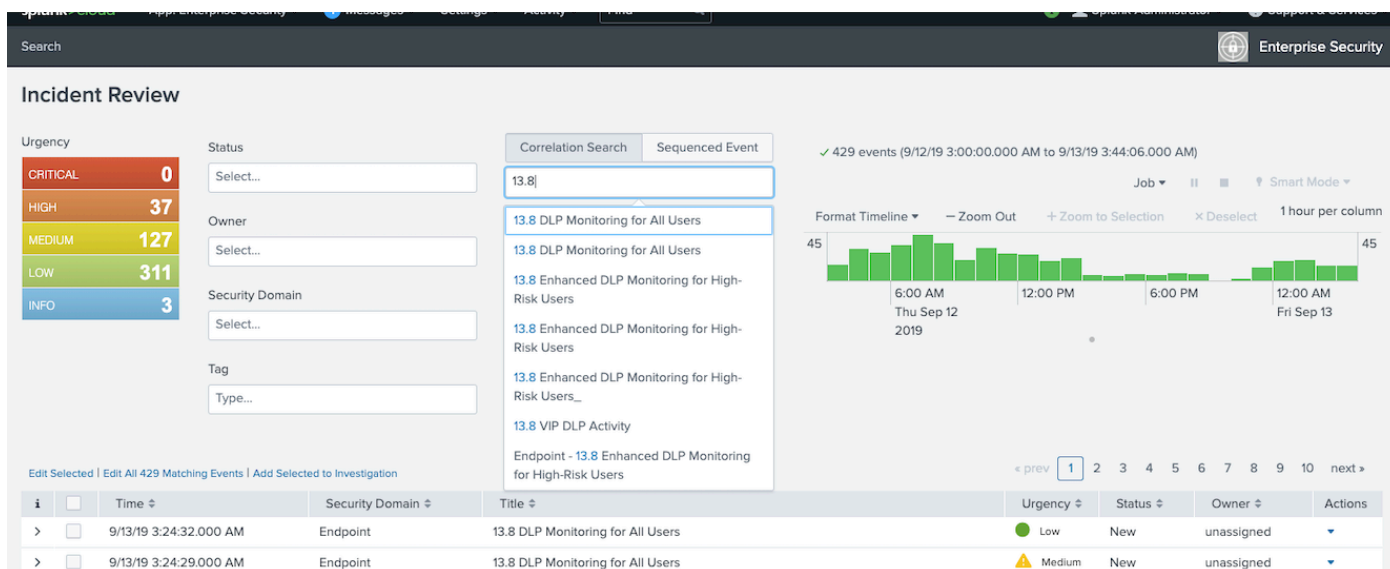
Se você acha que pode precisar investigá-los, é melhor deixar as duplicatas.

Uma pesquisa chamada "Ameaça - Pesquisas de correlação - Geração de pesquisa" é executada e cria os nomes das regras de pesquisa de correlação; ela acrescenta os nomes a uma kvstore chamada `correlacionearquisa_pesquisa`.

É possível eliminar duplicatas, mas, como mencionado acima, isso pode afetar as investigações de eventos anteriores.

Investigação

Na análise de incidentes ES, você pode ver nomes duplicados.



Resolução

Excluindo as entradas duplicadas.

1) Faça uma cópia de backup do kvstore, execute o arquivo e exporte-o para um arquivo CSV, que pode ser usado para recuperar este kvstore, se necessário.

```
| inputlookup correlationsearches_lookup
```

2) Para excluir uma duplicata, execute uma pesquisa removendo o nome duplicado e substituindo-o de volta ao kvstore.

Neste exemplo, usei o nome de regra "01.XYZ Pesquisa duplicada". Altere-o para qualquer nome duplicado que você queira remover.

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

Quando a pesquisa "01. XYZ Pesquisa duplicada" é executada novamente, o nome de regra ausente deve ser preenchido na kvstore, aparecendo na lista novamente.

Como você tem uma cópia do kvstore no CSV, ele pode ser feito como um arquivo de pesquisa, então usado para sobrescrever o kvstore correlationsearch_lookup e recriá-lo a partir do backup.

Links relacionados

Respostas de Splunk

[Por que a página ES Incident Review ainda lista as pesquisas de correlação excluídas na caixa de seleção múltipla "Correlation Search Name"?](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.