

如何删除重复关联搜索企业安全(ES)事件审核下拉列表中的名称

适用范围

Splunk企业安全

描述

从现有关联搜索创建新关联搜索可能导致事件审核下拉列表中的名称重复。

当关联搜索运行时，它们可以创建值得注意的事件，这些事件会链接到这些搜索。由于这些事件将来可能需要调查这些值得关注的事件，因此会保留触发这些事件的关联搜索，这可能导致显示重复的名称。

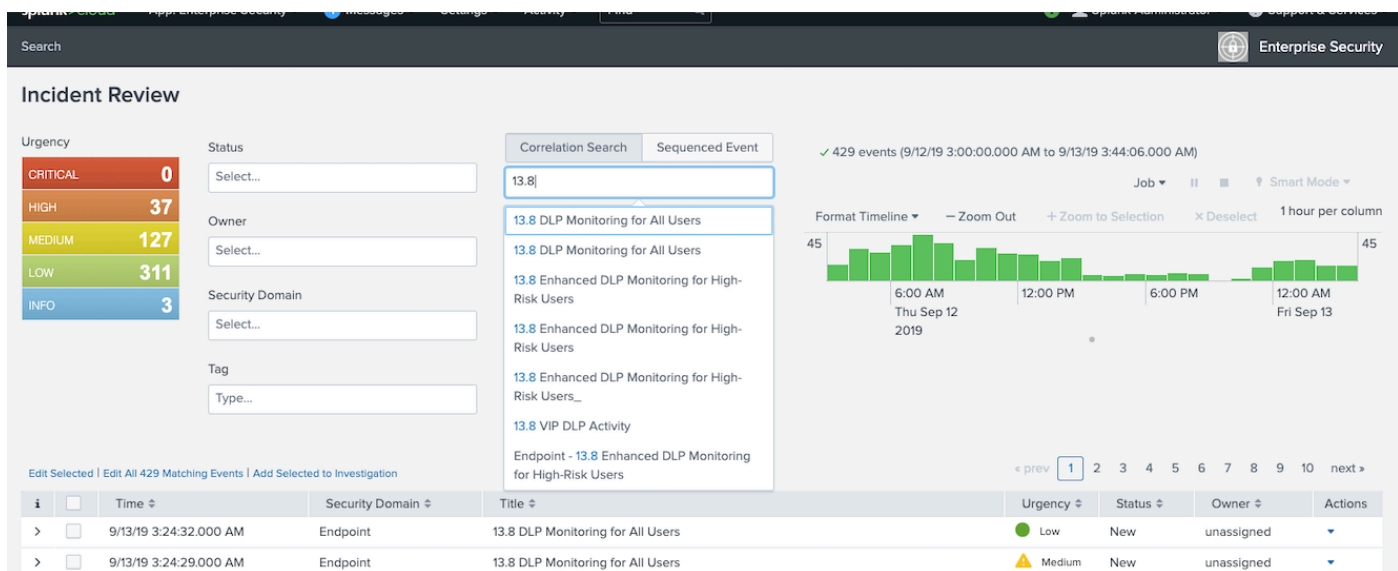
如果您确定不需要调查与这些搜索相关的这些旧记录，则可以删除重复的名称。如果你觉得可能需要调查它们，最好不要重复这些内容。

名为“Threat - Correlation Searches - Lookup Gen”的搜索运行并创建关联搜索规则名称，然后将名称附加到名为correlationsearches_lookup的kvstore。

可以删除重复项，但如上所述，这可能会影响对以前事件的调查。

调查

在ES事件检查中，您可能会看到重复的名称。



分辨率

删除重复条目。

1)创建kvstore的备份副本，运行该文件并将其导出为CSV文件，如有必要，这可用于恢复此kvstore。

```
| inputlookup correlationsearches_lookup
```

2)要删除重复项，请运行搜索删除重复项名称，然后将其覆盖回kvstore。
在本例中，我使用了规则名称“01.XYZ重复搜索”。 请将此名称更改为您要删除的任何重复名称。

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

当再次运行搜索“01.XYZ重复搜索”时，缺少的规则名称应填充在kvstore中，再次显示在列表中。

由于CSV格式的kvstore副本，它可以作为查找文件，然后用于覆盖kvstore correlationsearches_lookup并从备份重新创建它。

相关链接

Splunk答案

[为什么ES Incident Review页面仍在Multiselect框“Correlation Search Name”中列出删除的关联搜索？](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。