

ES(Enterprise Security) 인시던트 검토 드롭다운 목록에서 중복 상관관계 검색 이름을 삭제하는 방법

적용 가능성

Splunk 엔터프라이즈 보안

설명

기존 상관관계 검색에서 새 상관관계 검색을 생성하면 인시던트 검토 드롭다운 목록에서 이름이 중복될 수 있습니다.

상관관계 검색이 실행되면 주목할 만한 이벤트를 생성할 수 있으며, 이러한 이벤트는 해당 검색에 연결됩니다.

이러한 이벤트는 향후 이러한 주목할 만한 이벤트를 조사해야 할 수 있으므로, 이러한 이벤트를 트리거하는 상관관계 검색이 유지되므로 중복된 이름이 표시될 수 있습니다.

이러한 검색과 관련된 이러한 이전 이름을 조사할 필요가 없는 경우 중복 이름을 삭제할 수 있습니다.

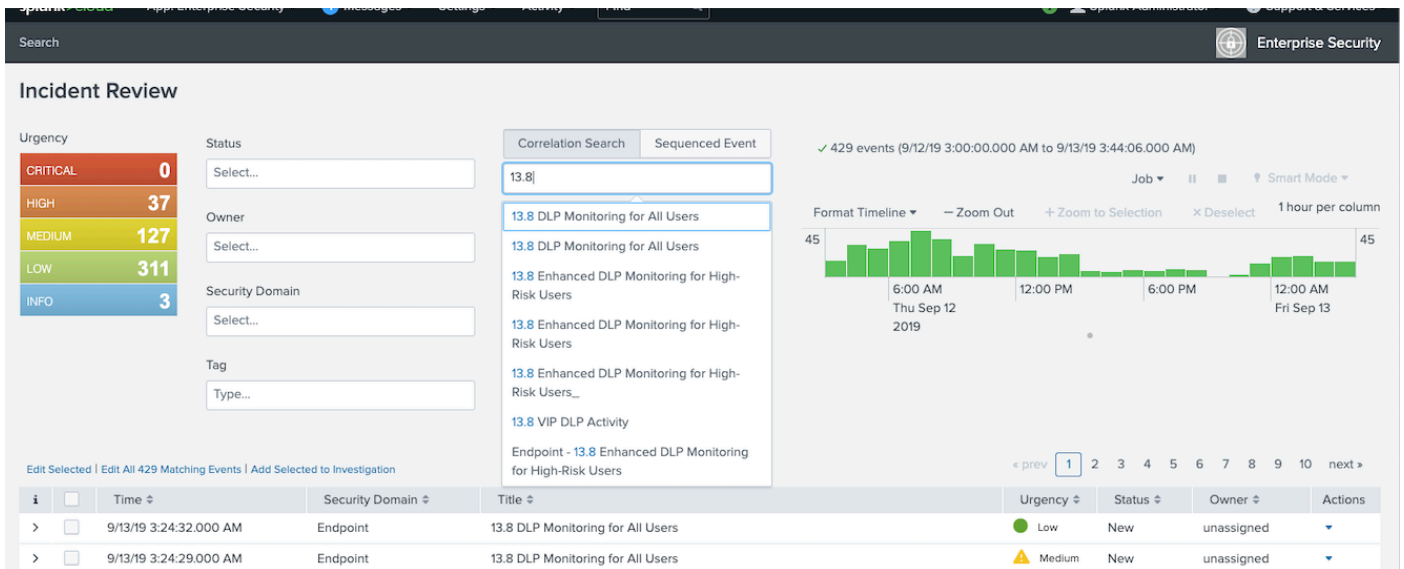
당신이 그들을 조사해야 할 필요가 있다고 생각한다면 복사를 남기는 것이 좋습니다.

"Threat - Correlation Searches - Lookup Gen"이라는 검색이 실행되고 상관관계 검색 규칙 이름이 생성되면 이 이름은 correlationsearches_lookup이라는 kvstore에 추가됩니다.

중복 항목을 삭제할 수 있지만 위에서 언급한 것처럼 이전 이벤트의 조사에 영향을 미칠 수 있습니다.

조사

ES 인시던트 검토에서 중복된 이름이 표시될 수 있습니다.



해결

중복 항목을 삭제하는 중입니다.

1) kvstore의 백업 복사본을 만들고 파일을 실행하여 CSV 파일로 내보냅니다. 필요한 경우 이 복사본을 사용하여 이 kvstore를 복구할 수 있습니다.

```
| inputlookup correlationsearches_lookup
```

2) 중복을 삭제하려면 중복 이름을 제거하는 검색을 실행하여 다시 kvstore에 덮어씁니다. 이 예에서는 규칙 이름 "01.XYZ Duplicate search(01.XYZ 중복 검색)"를 사용했습니다. 제거할 중복 이름으로 변경하십시오.

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

"01.XYZ Duplicate search(01.XYZ 중복 검색)" 검색이 다시 실행되면 누락된 규칙 이름이 kvstore에 채워지고 목록에 다시 표시됩니다.

CSV에 kvstore 사본이 있으므로 조회 파일로 만든 다음 kvstore correlationsearches_lookup을 덮어쓰고 백업에서 다시 만드는 데 사용할 수 있습니다.

관련 링크

Splunk Answers

[ES Incident Review\(ES 인시던트 검토\) 페이지에 Multiselect\(다중 선택\) 상자 "Correlation Search Name\(상관관계 검색 이름\)"에 삭제된 상관관계 검색이 여전히 나열되는 이유는 무엇입니까?](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.