

重複する相関の検索名をエンタープライズセキュリティ(ES)インシデントレビュードロップダウンリストから削除する方法

適用性

Splunkエンタープライズセキュリティ

説明

既存の相関検索から新しい相関検索を作成すると、インシデントレビューのドロップダウンリストで名前が重複する可能性があります。

相関検索を実行すると、注目すべきイベントを作成できます。これらのイベントは、これらの検索にリンクされます。

これらのイベントは今後これらの注目すべきイベントを調査する必要がある可能性があるため、これらのイベントをトリガーする相関検索が保持され、重複する名前が表示される可能性があります。

これらの検索に関連する古いnotableを調査する必要がないことがわかっている場合は、重複する名前を削除できます。

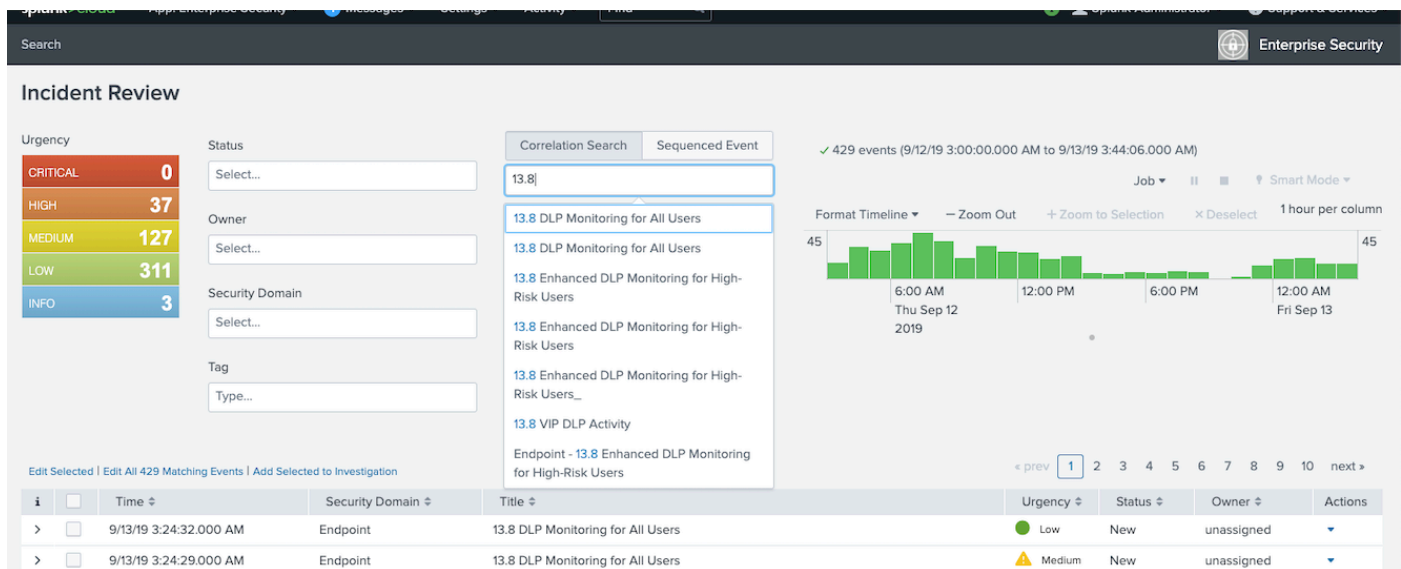
調査が必要と思われる場合は、重複を残しておくことをお勧めします。

「Threat - Correlation Searches - Lookup Gen」という検索が実行され、相関検索ルール名が作成され、correlationsearches_lookupという名前のkvstoreに名前が追加されます。

重複を削除することは可能ですが、前述のように、以前のイベントの調査に影響を与える可能性があります。

調査

ESインシデントレビューでは、重複する名前が表示されることがあります。



解決方法

重複するエントリを削除しています。

1) ファイルを実行してkvstoreのバックアップコピーを作成し、これをCSVファイルにエクスポートします。これは、必要に応じてこのkvstoreを回復するために使用できます。

```
| inputlookup correlationsearches_lookup
```

2) 重複を削除するには、重複する名前を削除して検索を実行し、その名前を上書きしてkvstoreに戻します。

この例では、「01.XYZ Duplicate search」というルール名を使用しています。重複する名前を削除するには、この名前を変更してください。

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

検索「01.XYZ Duplicate search」が再度実行されると、欠落しているルール名がkvstoreに入力され、リストに再度表示されます。

CSV形式でkvstoreのコピーを保持しているため、このファイルをルックアップファイルとして作成し、このファイルを使用してkvstore correlationsearches_lookupを上書きし、バックアップから再作成することができます。

関連リンク

Splunkの回答

[ES Incident Reviewページで、複数選択ボックスの「Correlation Search Name」に、削除された
相関検索が引き続き表示されるのはなぜですか。](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。