

تامولعم ةحول يف اقحلم سيل فصولا لقح ءاهجولل ثادحألا ةعجارم

قيبطتلا ةيلباق

Splunk Enterprise - 7.3.x نامأ

فصولا

نم ديدعلا نأ ثيح ،طابترالا نع ةصصخلمل ثحبلا تايلمع ةفاك ىلع رثؤت ةلكشملا نأ ودبي صصخم ثحب ىلع لاثم يلي امي ف .ثدحلا ةعجارم تامولعم ةحول يف اهتئبعت متي مل لوقحلا طابترالا نع .

طابترالا نع ثحبلا : "test_sample_1 - ديدعتلا"

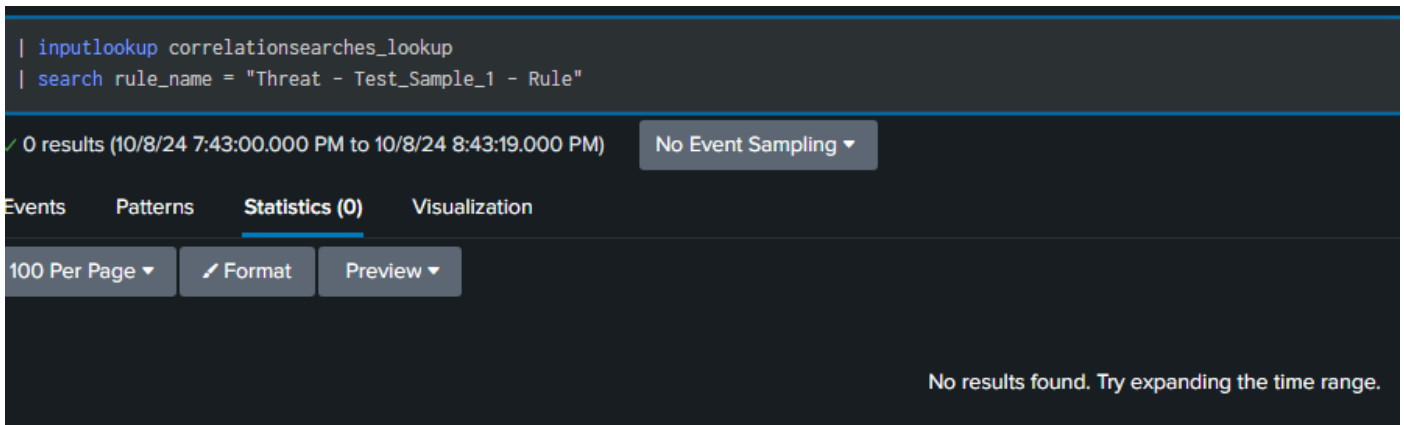
Description		
unknown		
Additional Fields	Value	Action
Disposition	Undetermined	▼
Owner	unassigned	▼
Security Domain	threat	▼
Severity	high	▼
Status	New	▼
Time	2024-10-09T22:37:03.000+05:30	
Title	Test_Sample_1	▼
Type	notable	
Urgency	medium	▼

ءالجتسا

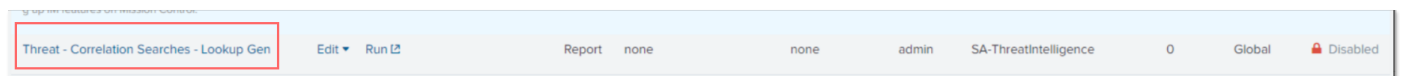
- جئاتن جتنن ةنرتقملا لوقحلا تناك اذا امم ققحتلل ايودي هاندأ ثحبلا ذيفنت مت 1. ةميقلا نم مغرلا ىلع ،"فورعم ريغ" ضرعي هناف ،"rule_description" لقحلا ةعجارم دنع .طابترالا نع ثحبلا عاشنإ ءانثأ انه يوكت متي يتلا

```
| savedsearch "Incident Review - Main" time_filter="" event_id_filter="" source_filter="" secur
| search
| eval _position=1
| accum _position
| eval _offset=_position - 1
```

2. تانايب ال علم م تي ناك اذا ام ققحت لل "correlationSearch_lookup" ثحب ال ذيفنت م ت
جئاتن يا اهنع جتنني ال نكلو "Rule - يداع ريغ WebDAV ذيفنت "Threat - [BDS] ةدعاق لل



3. Threat - Correlation Search - ثحب ال عاشن اب موقوي يذل ثحب ال ناك اذا ام ققحت ال م ت
لطم ثحب ال نأ دجوو ال مأ هنيكمت م ت "Lookup"



رارق

ةيلات ال تاوطخ ال ىل ع روثع ال ىجري، ةلكشم ال هذه ل حل:

1. تاهي بنت لالو رارق لالو ثحب ال تاي لم ع -> تاداع ال ال ل لقتنا
2. "Lookupgen" - طاب تر ن ع ثحب - ديهت ن ع ثحب ال.
3. نيكمت -> ريرحت قوف رقرن اب ثحب ال نيكمت ب م ق.

Name ↕	Actions	⚡	Type	Next Scheduled Time ↕	Display View ↕	Owner ↕	App ↕	Alerts ↕	Sharing ↕	Status ↕
Threat - Correlation Searches - Lookup Gen	Edit Run		Report	none	none	admin	SA-ThreatIntelligence	0	Global	⛔ Disabled
Edit Search Edit Permissions Edit Schedule Edit Acceleration Edit Summary Indexing Enable										

ثدحل ةعجارم تامولعم ةحول يف ةنرتقملا ىرخألا لوقحلاو فصولا علم مت ،كلذ دعب

Description		
Just a sample Description		
Additional Fields	Value	Action
Disposition	Undetermined	▼
Owner	unassigned	▼
Security Domain	threat	▼
Severity	high	▼
Status	New	▼
Time	2024-10-09T22:08:04.000+05:30	
Title	Test_Sample_1	▼
Type	notable	
Urgency	medium	▼

ةلص تاذا طباور

ةلصلا تاذا قئاتولا : [طابت رالا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا