

Das Beschreibungsfeld wird im Dashboard für die Incident-Prüfung der Notables nicht ausgefüllt.

Geltungsbereich

Splunk Enterprise Security - 7.3.x

Beschreibung

Das Problem scheint sich auf alle benutzerdefinierten Korrelationssuchen auszuwirken, da mehrere Felder im Dashboard für die Vorfallprüfung nicht ausgefüllt werden. Nachfolgend finden Sie ein Beispiel für eine benutzerdefinierte Korrelationssuche.

Korrelationssuche: "Bedrohung - Test_Sample_1"

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	▼

Untersuchung

1. Führen Sie die Suche unten manuell aus, um zu überprüfen, ob die zugehörigen Felder Ergebnisse liefern. Beim Überprüfen des Felds "rule_description" wird trotz des bei der Erstellung der Korrelationssuche konfigurierten Werts "unknown" angezeigt.

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

2. Die Suche "CorrelationSearchup_lookup" wurde ausgeführt, um zu überprüfen, ob die Daten für die Regel "Threat - [BDS] Abnormal WebDav Execution - Rule" aufgefüllt werden, es werden jedoch keine Ergebnisse ausgegeben.

The screenshot shows the Splunk search results page. At the top, the search query is displayed: `| inputlookup correlationsearches_lookup` and `| search rule_name = "Threat - Test_Sample_1 - Rule"`. Below the query, it states "0 results (10/8/24 7:43:00.000 PM to 10/8/24 8:43:19.000 PM)" and "No Event Sampling". The interface includes tabs for "Events", "Patterns", "Statistics (0)", and "Visualization". Below the tabs are buttons for "100 Per Page", "Format", and "Preview". At the bottom, a message reads: "No results found. Try expanding the time range."

3. Geprüft, ob die Suche "Bedrohung - Korrelationssuche - Nachschlagen" aktiviert wurde und ob die Suche deaktiviert war.

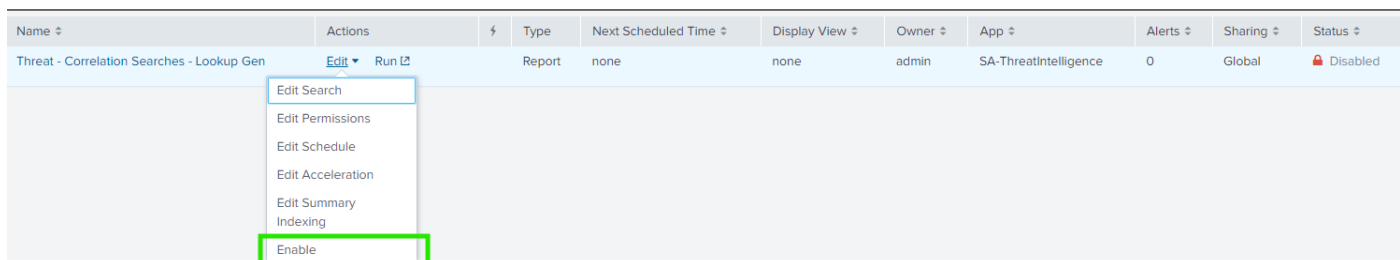
The screenshot shows the Splunk configuration page for the search "Threat - Correlation Searches - Lookup Gen". The page has a header with "Edit" and "Run" buttons. Below the header, there is a table with columns: "Report", "none", "none", "admin", "SA-ThreatIntelligence", "0", "Global", and "Disabled". The "Disabled" status is highlighted with a red icon.

Auflösung

Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Navigieren Sie zu Einstellungen -> Suchen, Berichte und Warnungen.

- Suchen Sie nach "Threat - Correlation searches - Lookupgen".
- Aktivieren Sie die Suche, indem Sie auf Bearbeiten -> Aktivieren klicken.



Nach dem Aktivieren der Suche werden die Beschreibung und die anderen zugehörigen Felder im Dashboard für die Incident-Prüfung angezeigt.

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	▼

Verwandte Links

Zugehörige Dokumentation: [Link](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.