

La voce "Esegui azioni di risposta adattive" non elenca tutte le azioni di allarme in Splunk.

Applicabilità

Componenti aggiuntivi applicazioni Splunk

Descrizione

Descrizione:

1. Installato TA-thehive & TA-PagerDuty su Splunk ES testa di ricerca.
2. Durante la modifica delle ricerche di correlazione ottengono le opzioni di avviso di queste app in Azioni di risposta adattiva. Ma nel pannello di revisione degli incidenti quando cercano di aggiungere l'"esecuzione dell'azione di risposta adattiva" ottengono solo le azioni di avviso predefinite, non l'hive e PagerDuty.

Trigger alert when Number of Results

is greater than 0

Throttling

Window duration 86300 second(s)

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by user change_type

Type the fields to consider for matching events for throttling. [Learn more](#)

Adaptive Response Actions

+ Add New Response Action

Category All

Search

 PagerDuty

Trigger incidents in PagerDuty

Category: [others](#) | Task: [others](#) | Subject: [others](#) | Vendor: [unknown](#)

 Ping

Runs the ping command

Category: [Information Gathering](#) | Task: [scan](#) | Subject: [device](#) | Vendor: [Operating System](#)

 Send To UBA

Forwards search results from Splunk Enterprise to UBA

Category: [Information Conveyance](#) | Task: [create](#) | Subject: [uba.anomaly](#) | Vendor: [Splunk](#)

 create THEHIVE alert(s) (alert action)

Create alerts in theHive

Category: [others](#) | Task: [others](#) | Subject: [others](#) | Vendor: [unknown](#)

>  Risk Analysis

Indagine

Architettura: ES v 5.3.1 | Splunk v 7.3.1

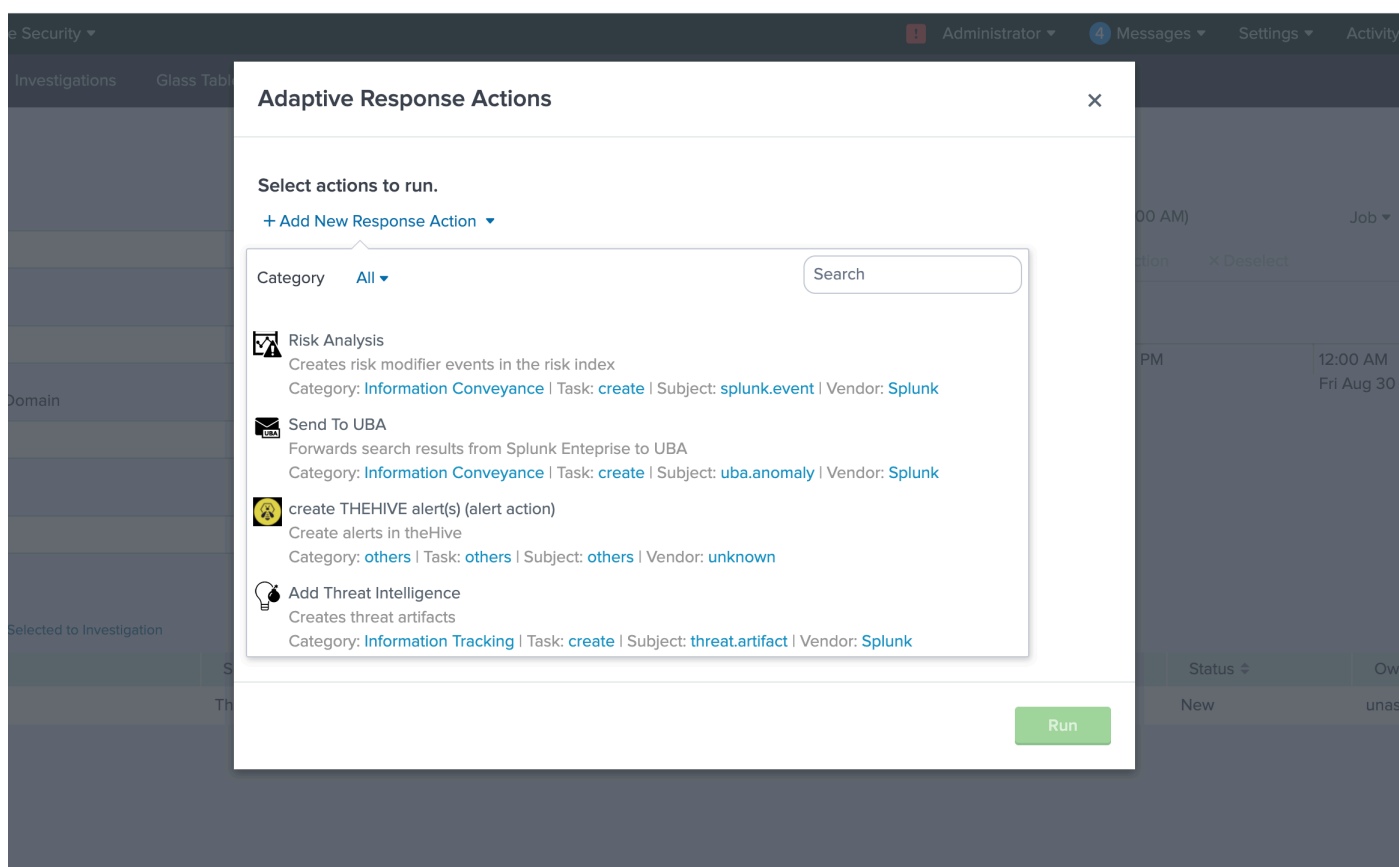
Osservazione: nel mio ambiente Splunk, ho installato gli stessi componenti aggiuntivi per controllare il comportamento Splunk, e ho trovato lo stesso.

Fasi di riproduzione:

1. Installare TA-thehive (<https://splunkbase.splunk.com/app/4380/>) e PagerDuty Addon (<https://splunkbase.splunk.com/app/3742/>) sull'installazione di ricerca ES.

2. Modificando la ricerca di correlazione e controllando le azioni di risposta adattive, verrà visualizzata l'azione di avviso the-hive & pagerduty.

3. Passare al pannello di esame degli incidenti. Fare clic su "Action" (Azione) davanti a qualsiasi notabile e selezionare * "run adaptive response action" (Esegui azione di risposta adattiva). le opzioni hive-hive e pagerduty non sono disponibili. *



Risoluzione

"This is as Designed" se non avete definito param._cam per l'azione di allarme. Inoltre, la revisione dell'incidente richiede che "supported_adhoc" sia impostato su true.

Per risolvere:

```
$Splunk_Home/etc/apps/TA-thehive/default[thehive_alert_create_alert]
is_custom = 1
label = create THEHIVE alert(s) (alert action)
description = Create alerts in theHive
icon_path = thehive_logo_small.png
payload_format = json
disabled = 0
```

NOTA: che l'azione sia denominata "thehive_alert_create_alert" e non abbia una definizione param._cam. Ho verificato che non viene visualizzato nella sezione Incident Review.

Successivamente, tutto quello che ho fatto è stato aggiungere un semplice param._cam definizione:

<#root>

```
[thehive_alert_create_alert]
is_custom = 1
label = create THEHIVE alert(s) (alert action)
description = Create alerts in theHive
icon_path = thehive_logo_small.png
payload_format = json
disabled = 0
```

```
param._cam = {"supports_adhoc": true}
```

NOTA: Apportare le modifiche in \$Splunk_Home/etc/apps/app_name/local

Security

Administrator Messages Settings Activity

InvestigationsGlass Table

Adaptive Response Actions

Select actions to run.

+ Add New Response Action

CategoryAll

Search

Risk Analysis

Creates risk modifier events in the risk index

Category: Information Conveyance | Task: create | Subject: splunk.event | Vendor: Splunk

Send To UBA

Forwards search results from Splunk Enterprise to UBA

Category: Information Conveyance | Task: create | Subject: uba.anomaly | Vendor: Splunk

create THEHIVE alert(s) (alert action)

Create alerts in theHive

Category: others | Task: others | Subject: others | Vendor: unknown

Add Threat Intelligence

Creates threat artifacts

Category: Information Tracking | Task: create | Subject: threat.artifact | Vendor: Splunk

Run

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).