

De "Adaptieve responsacties uitvoeren" bevat niet alle waarschuwingsacties in Splunk.

toepasbaarheid

Splunk Apps-add-ons

Beschrijving

Beschrijving:

1. Geïnstalleerd TA-thehive & TA-PagerDuty op Splunk ES zoekhoofd.
2. Tijdens het bewerken van de correlatiezoekopdrachten krijgen ze deze waarschuwingsopties voor apps onder Adaptieve responsacties. Maar in het incident review panel wanneer ze proberen om de "run adaptive response action" toe te voegen krijgen ze alleen de standaard waarschuwingsacties, niet de korf en 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

onderzoek

Architectuur: ES v 5.3.1 | Splunk v 7.3.1

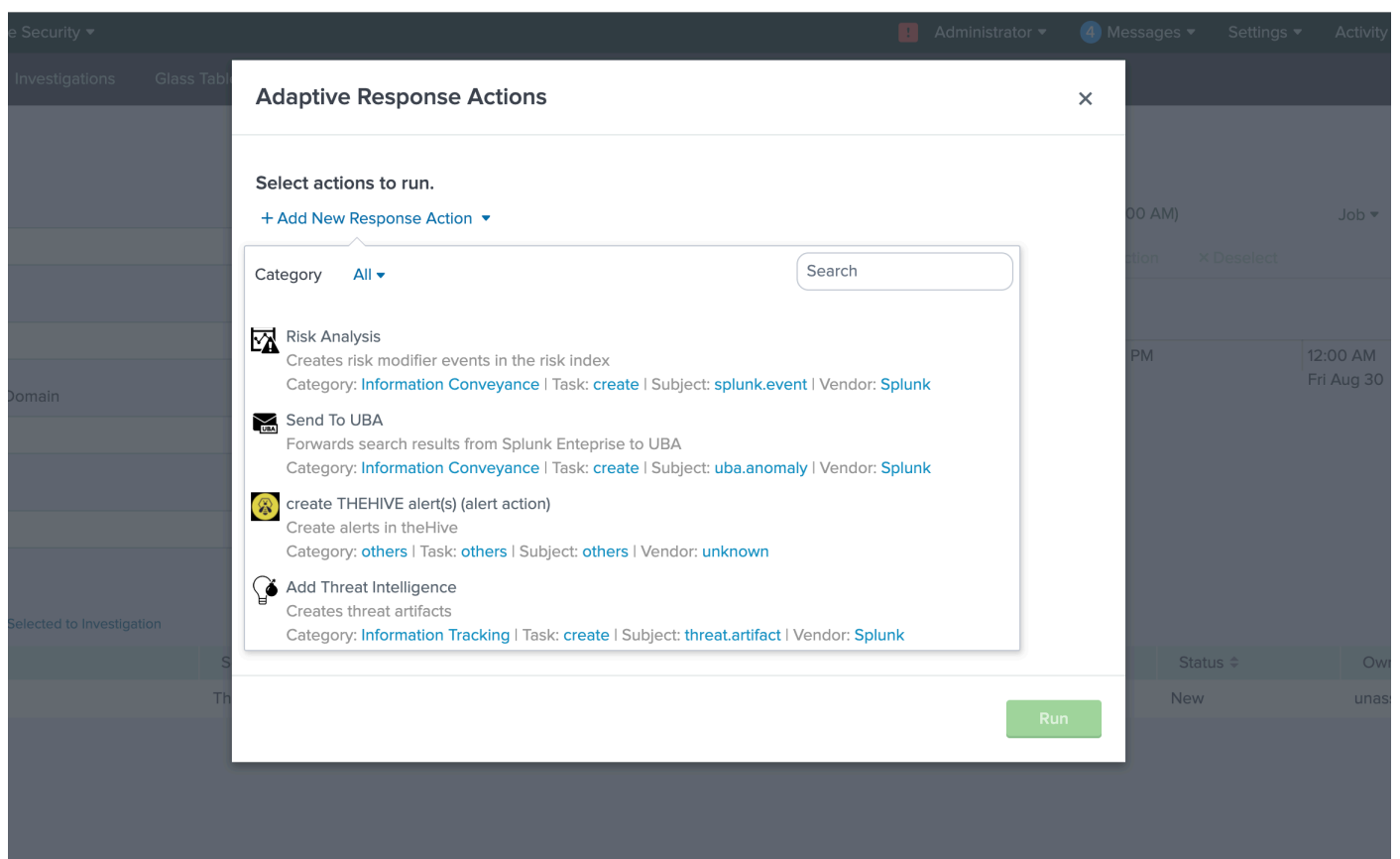
Waarneming: In mijn Splunk-omgeving installeerde ik dezelfde add-ons om het Splunk-gedrag te controleren, en ik vond hetzelfde.

Voortplantingsstappen:

1. Installeer TA-thehive (<https://splunkbase.splunk.com/app/4380/>) & PagerDuty Addon (<https://splunkbase.splunk.com/app/3742/>) op ES-zoekkop.

2. Bewerk de correlatie-zoekopdracht en controleer voor de Adaptive Response Actions, u ziet de hive- & pagerduty als een waarschuwingsactie.

3. Ga naar het panel voor incidentbeoordeling. Klik op "Actie" voor een opmerkelijke en selecteer * "Aangepaste responsactie uitvoeren". de opties voor bijenkorf- en pagerduty zijn niet beschikbaar. *



resolutie

"Dit is zoals ontworpen" als u geen param._cam hebt gedefinieerd voor uw waarschuwingsactie. De Incident Review vereist ook dat "supports_adhoc" is ingesteld op true.

Oplossen:

```
$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
```

OPMERKING: de actie heeft de naam "thehive_alert_create_alert" en heeft geen param._cam-definitie. Ik heb geverifieerd dat dit niet wordt weergegeven in Incident Review.

Vervolgens voegde ik alleen een eenvoudige param._cam-definitie toe:

<#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}
```

OPMERKING: Breng de wijzigingen aan 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.