

L'option « Exécuter des actions de réponse adaptative » ne répertorie pas toutes les actions d'alerte dans le Splunk.

Applicabilité

Modules complémentaires des applications Splunk

Description

Description:

1. Installé TA-thehive & TA-PagerDuty sur la tête de recherche Splunk ES.

2. Lors de la modification des recherches de corrélation, ils obtiennent ces options d'alerte des applications sous Actions de réponse adaptative. Mais dans le panneau de révision des incidents, lorsqu'ils tentent d'ajouter l'"action d'exécution de réponse adaptative", ils obtiennent uniquement les actions d'alerte par défaut, et non la ruche et 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 x change_type x

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

x

Enquête

Architecture : ES v 5.3.1 | Splunk v 7.3.1

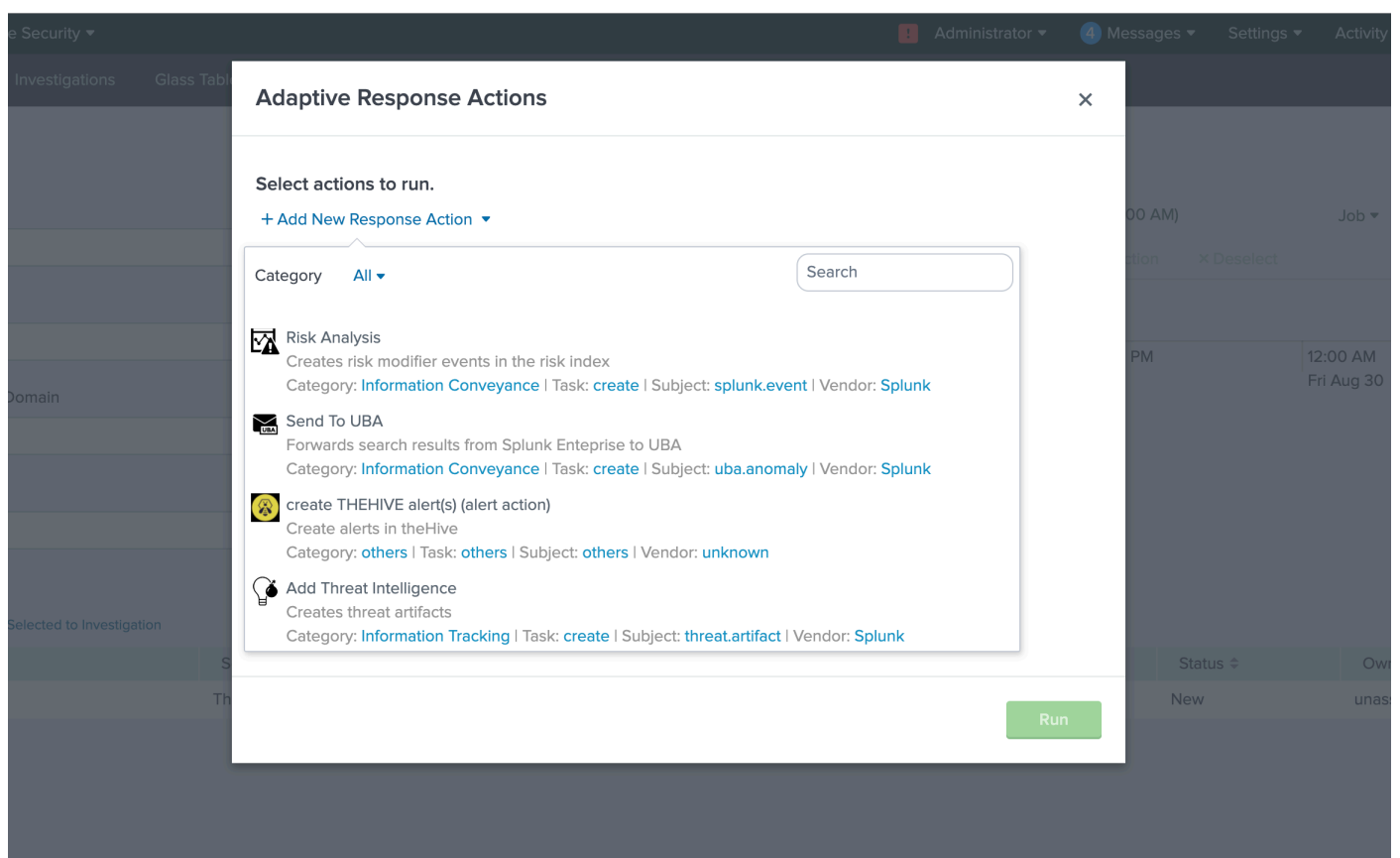
Observation : Dans mon environnement Splunk, j'ai installé le même module complémentaire pour vérifier le comportement Splunk et j'ai trouvé le même.

Étapes de reproduction :

1. Installez TA-thehive (<https://splunkbase.splunk.com/app/4380/>) et PagerDuty Addon (<https://splunkbase.splunk.com/app/3742/>) sur la tête de recherche ES.

2. Modifiez la recherche de corrélation et recherchez les actions de réponse adaptative. L'action d'alerte « the-hive & pagerduty » s'affiche.

3. Allez à la commission d'examen des incidents. Cliquez sur « Action » en regard de toute action notable et sélectionnez * « Exécuter une action de réponse adaptative ». les options de service de pager et de ruche ne sont pas disponibles. *



Résolution

"Ceci est conçu" si vous n'avez pas défini param._cam pour votre action d'alerte. En outre, la révision de l'incident nécessite que le paramètre « supports_adhoc » soit défini sur true.

Pour résoudre :

```
$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
```

NOTE: que l'action est nommée "thehive_alert_create_alert" et n'a pas de définition param._cam. J'ai vérifié que cette option n'apparaît pas dans l'analyse de l'incident.

Ensuite, tout ce que j'ai fait, c'est ajouter une définition simple de param._cam :

<#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}
```

NOTE: Effectuez les modifications dans \$Splunk_Home/etc/apps/app_name/local

Security

Administrator4 MessagesSettingsActivity

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.