

「Run Adaptive Response Actions」には、Splunkのすべてのアラートアクションが表示されません。

適用性

Splunkアプリケーションアドオン

説明

説明:

1. Splunk ES検索ヘッドにTA-thehiveとTA-PagerDutyをインストールしました。
2. 相関検索を編集している間、これらのアプリケーションは適応応答アクションの下にアラートオプションを取得しています。ただし、インシデントレビューパネルで「適応型応答アクションの実行」を追加しようとすると、デフォルトのアラートアクションのみが取得され、ハイズとPagerDutyは取得されません。

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

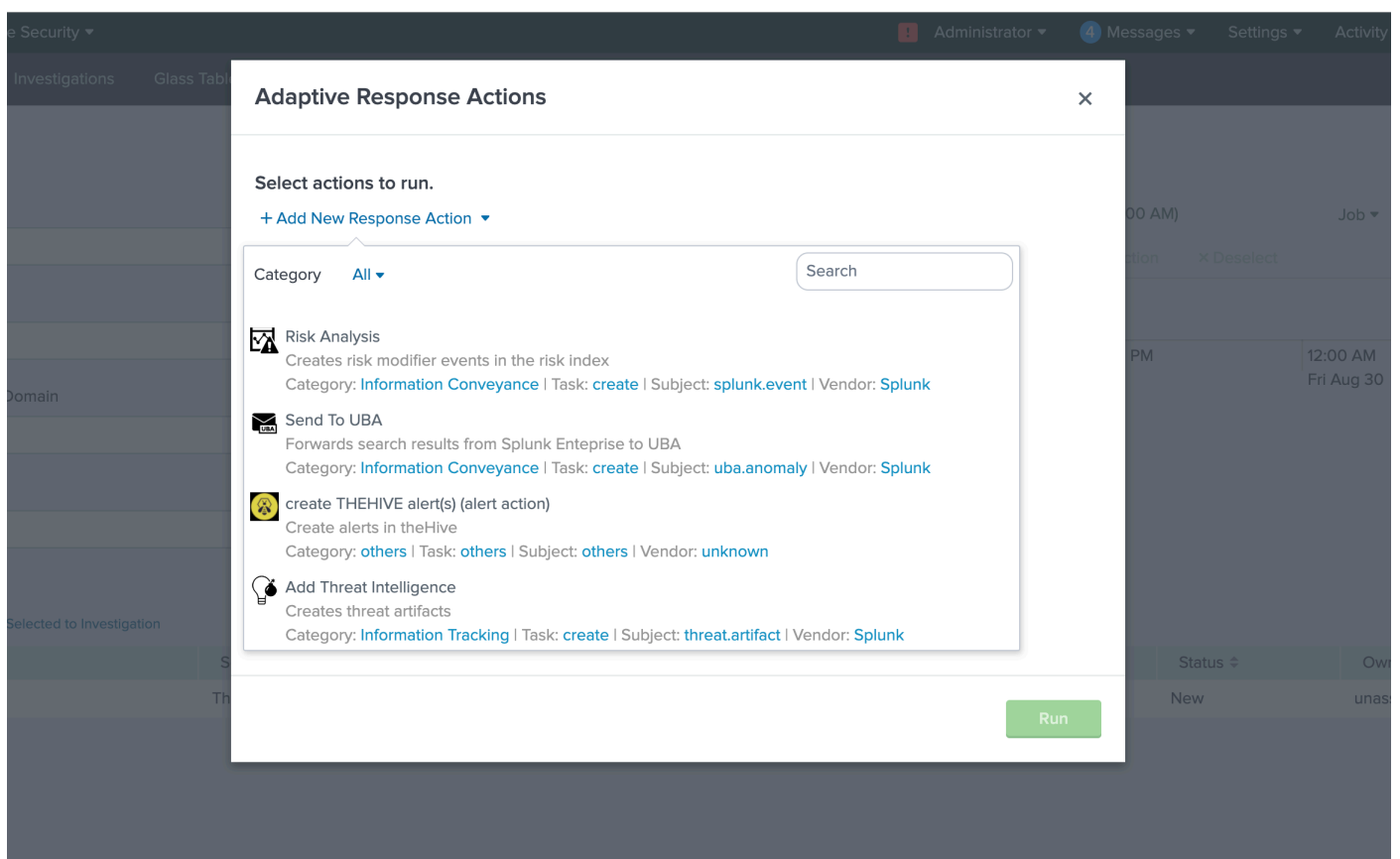
調査

アーキテクチャ : ES v 5.3.1 | Splunk v 7.3.1

確認 : Splunk環境に、Splunkの動作を確認するための同じアドオンをインストールしたところ、同じものが見つかりました。

再現手順：

1. ES検索ヘッドにTA-thehive (<https://splunkbase.splunk.com/app/4380/>)とPagerDuty Addon (<https://splunkbase.splunk.com/app/3742/>)をインストールします。
2. 相関検索を編集し、Adaptive Response Actionsを確認します。アラートアクションとしてThe-hive & pagerdutyが表示されます。
3. インシデントレビューパネルに移動します。任意の特筆すべき項目の前にある「アクション」をクリックし、*「適応型応答アクションの実行」を選択します。*



解決方法

アラートアクションにparam._camが定義されていない場合は、「This is as Designed」と表示されます。また、インシデントレビューでは「supports_adhoc」をtrueに設定する必要があります。

解決するには：

```
$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
```

注：アクションの名前は「thehive_alert_create_alert」で、param._cam定義がないことに注意してください。これがインシデントレビューに表示されないことを確認しました。

次に、単純なparam._cam定義を追加しました。

<#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}
```

注： \$Splunk_Home/etc/apps/app_name/localを変更します。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。