

“Run Adaptive Response Actions”未列出Splunk中的所有警报操作。

适用范围

Splunk应用加载项

描述

描述:

- 1.在Splunk ES搜索头上安装TA-theve & TA-PagerDuty。
- 2.编辑关联搜索时，他们在自适应响应操作(Adaptive Response Actions)下获取这些应用的警报选项。但在事件审核面板中，当他们在尝试添加“运行自适应响应操作”(run adaptive response action)时，他们仅获取默认警报操作，而不获取配置单元和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 x

调查

架构:ES v 5.3.1 | Splunk v 7.3.1

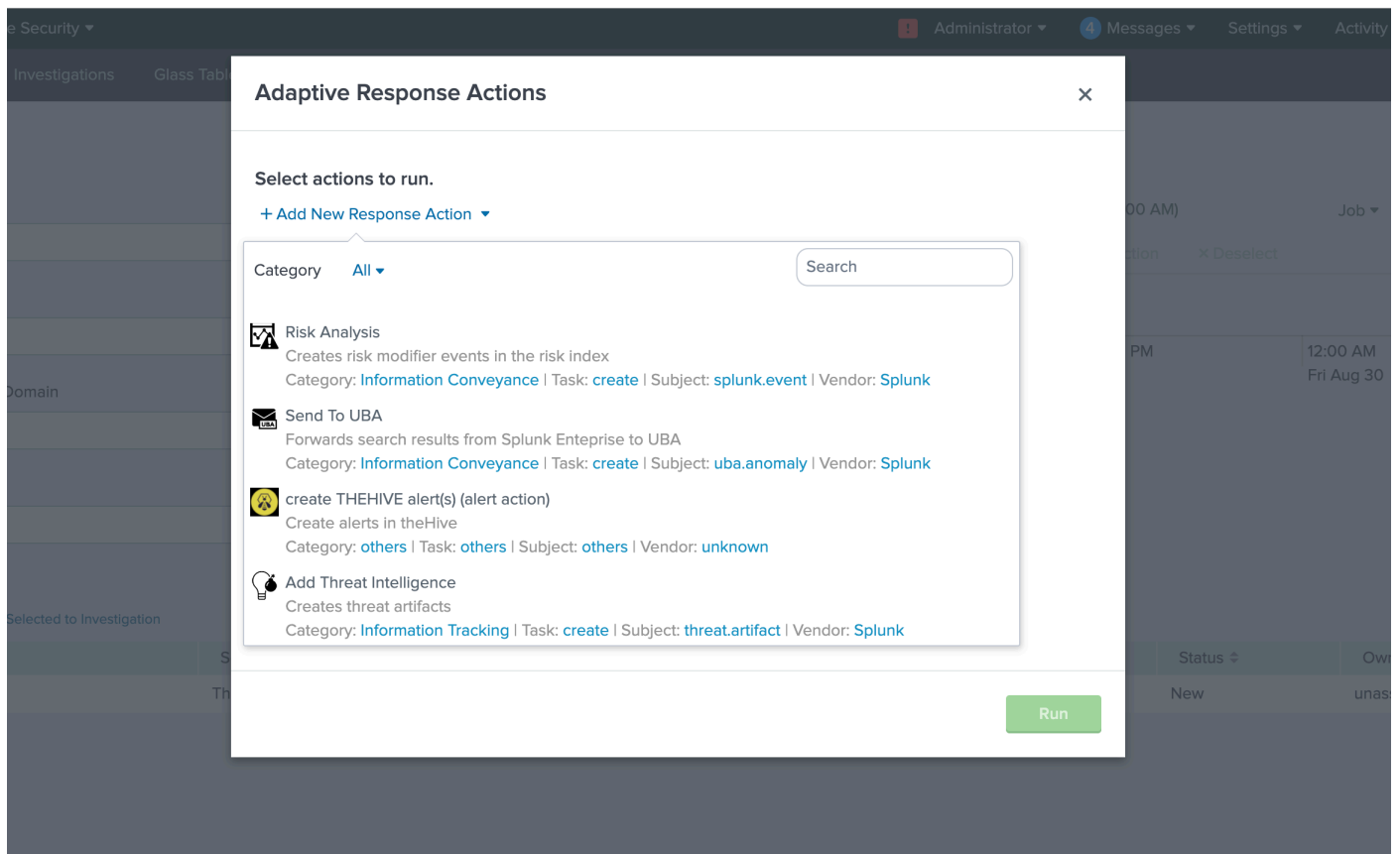
观察：在我的Splunk环境中，我安装了相同的插件来检查Splunk行为，结果发现相同。

复制步骤：

1.在ES搜索头上安装TA-themive(<https://splunkbase.splunk.com/app/4380/>)和PagerDuty Addon(<https://splunkbase.splunk.com/app/3742/>)。

2.编辑关联搜索并检查自适应响应操作，您将看到“配置单元与寻呼任务”作为警报操作。

3.转至事件审查面板。在任何值得注意的选项前面点击“Action”，然后选择*“run adaptive response action”。 - hive和pagerduty选项不可用。 *



分辨率

如果您没有为警报操作定义param._cam，则为“Designed”。此外，“事件检查”要求将“supports_adhoc”设置为true。

要解决：

```
$Splunk_Home/etc/apps/TA-themive/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:操作名为“thehive_alert_create_alert”，且没有param._cam定义。我验证这不会显示在“事件审核”中。

接下来，我只添加了一个简单的param._cam定义：

<#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:在\$Splunk_Home/etc/apps/app_name/local中进行更改

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。