

A opção "Executar ações de resposta adaptativa" não está listando todas as ações de alerta no Splunk.

Aplicabilidade

Complementos de Aplicativos Splunk

Descrição

Descrição:

1. Instalado TA-thehive & TA-PagerDuty no cabeçalho de pesquisa Splunk ES.

2. Durante a edição das pesquisas de correlação, eles recebem essas opções de alerta de aplicativos em Ações de resposta adaptativa. Mas no painel de revisão de incidentes, quando tentam adicionar a "ação de resposta adaptativa", eles recebem apenas as ações de alerta padrão, não a seção 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 x

Investigação

Arquitetura: ES v 5.3.1 | Splunk v 7.3.1

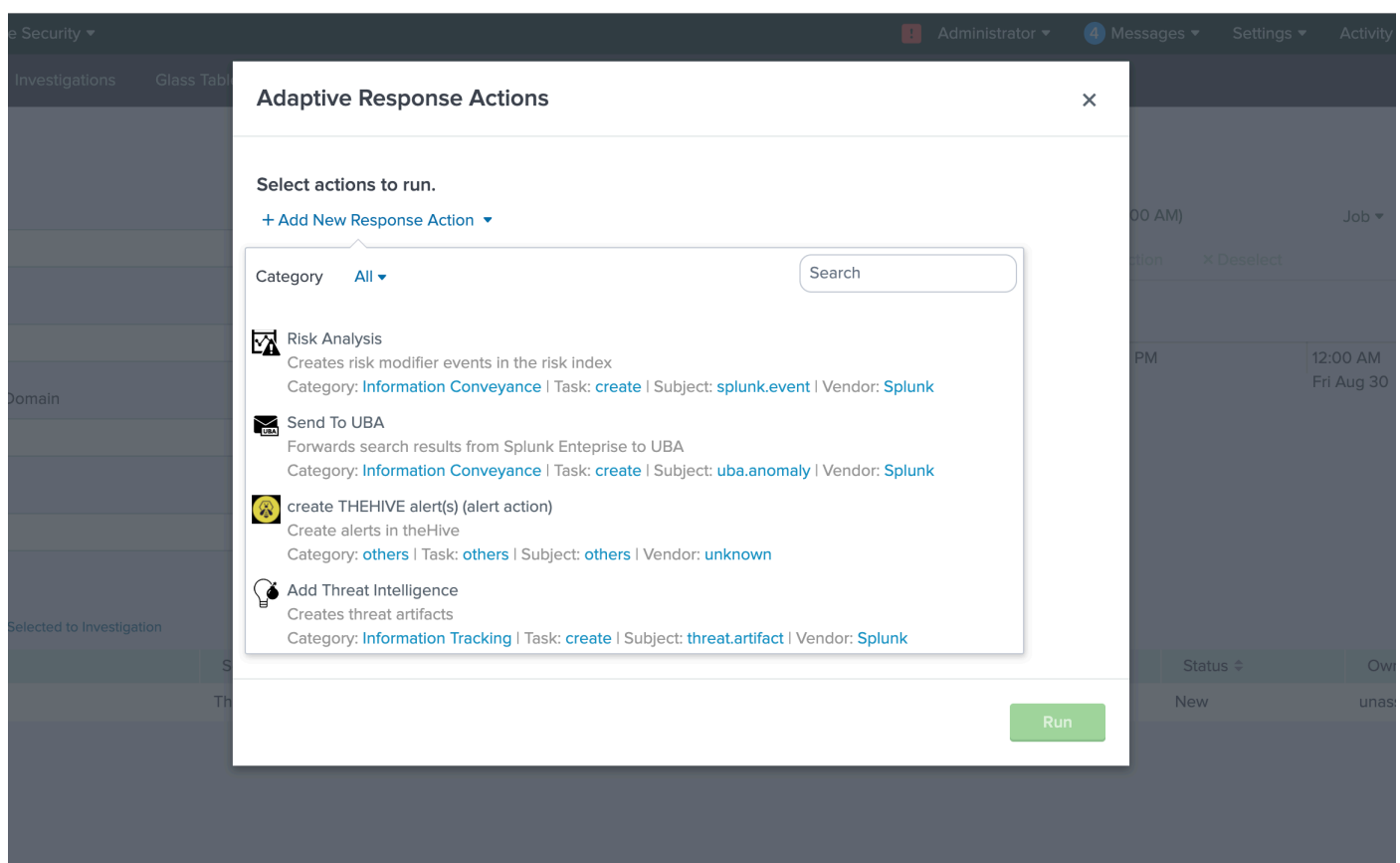
Observação: em meu ambiente de Splunk, instalei os mesmos complementos para verificar o comportamento de Splunk, e achei o mesmo.

Etapas da reprodução:

1. Instalar TA-thehive (<https://splunkbase.splunk.com/app/4380/>) & PagerDuty Addon (<https://splunkbase.splunk.com/app/3742/>) no cabeçalho de pesquisa ES.

2. Edite a pesquisa de correlação e verifique as Ações de Resposta Adaptativa, você verá o direito de colmeia e pager como uma ação de alerta.

3. Vá para o painel de revisão de incidentes. Clique em "Ação" na frente de qualquer item notável e selecione * "executar ação de resposta adaptativa". as opções de taxa de transmissão e taxa de pager não estão disponíveis. *



Resolução

"This is as Designed" se você não tiver param._cam definido para sua ação de alerta. Além disso, a Revisão do incidente requer que você tenha "supported_adhoc" definido como verdadeiro.

Para Resolver:

```
$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 a ação é chamada "thehive_alert_create_alert" e não tem nenhuma definição param._cam. Verifiquei que isso não aparece na Revisão de incidentes.

Em seguida, tudo o que fiz foi adicionar uma definição simples 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: Faça as alterações em \$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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.