

"Run Adaptive Response Actions(적응형 응답 작업 실행)"에 Splunk의 모든 경고 작업이 나열되어 있지 않습니다.

적용 가능성

Splunk Apps 추가 기능

설명

설명:

1. Splunk ES 검색 헤드에 TA-hive & TA-PagerDuty를 설치했습니다.
2. 상관관계 검색을 편집하는 동안 적응형 응답 작업에서 이러한 앱 알림 옵션을 가져옵니다. 하지만 인시던트 검토 패널에서 "적응형 응답 작업 실행"을 추가하려는 경우 hive 및 PagerDuty가 아닌 기본 알림 작업만 가져옵니다.

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

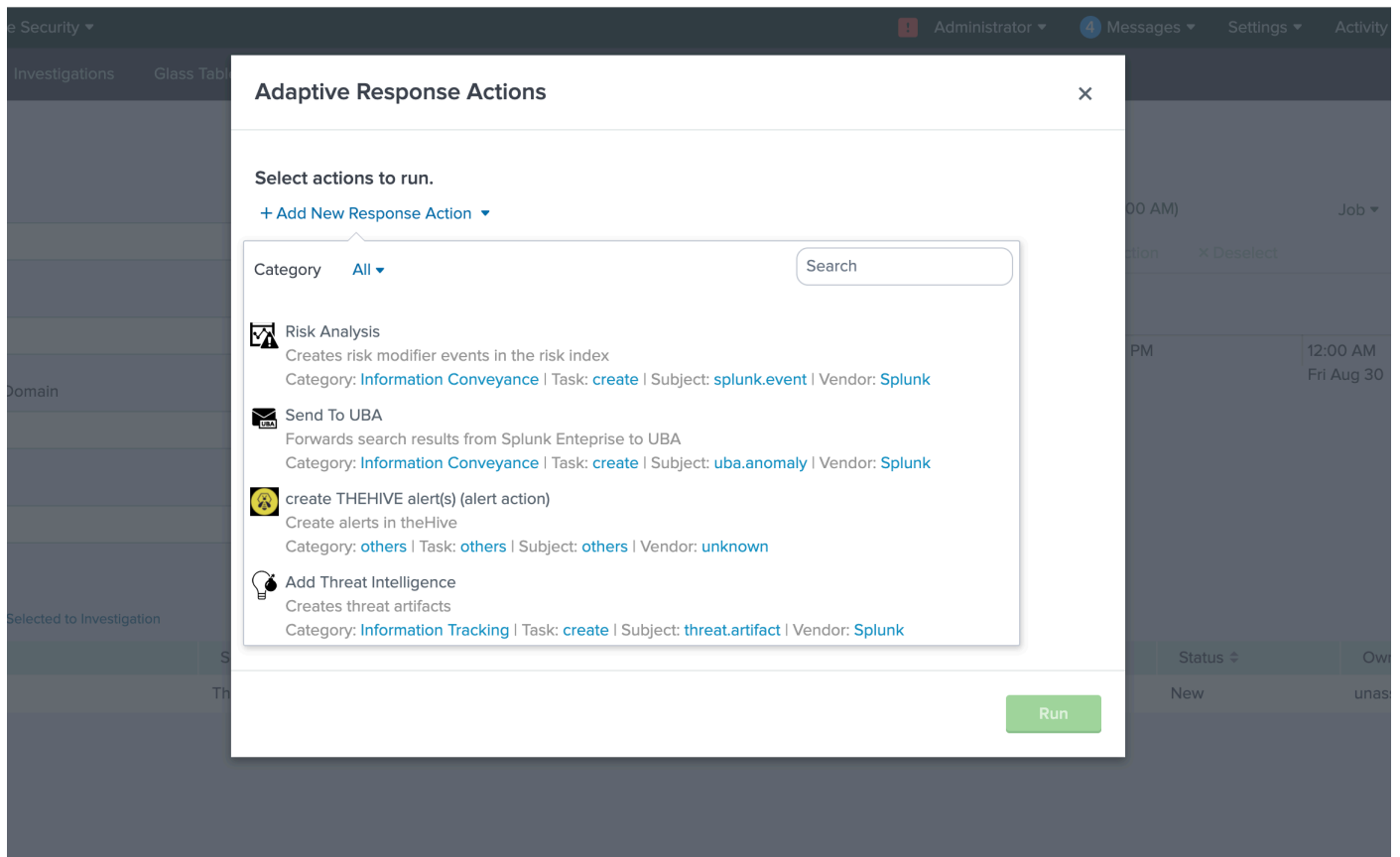
조사

아키텍처: ES v 5.3.1 | Splunk v 7.3.1

관찰: Splunk 환경에서 Splunk 동작을 확인하기 위해 동일한 애드온을 설치했는데 동일한 애드온을 찾았습니다.

재현 단계:

1. ES 검색 헤드에 TA-thehive(<https://splunkbase.splunk.com/app/4380/>) 및 PagerDuty Addon(<https://splunkbase.splunk.com/app/3742/>)을 설치합니다.
2. 상관관계 검색을 편집하고 적응 응답 작업을 확인합니다. 그러면 hive & pagerduty가 경고 작업으로 표시됩니다.
3. 인시던트 검토 패널로 이동합니다. 눈에 띄는 항목 앞에 있는 "Action(작업)"을 클릭하고 * "run adaptive response action(적응형 대응 작업 실행)"을 선택합니다. hive 및 pagerduty 옵션은 사용할 수 없습니다. *



해결

경고 작업에 대해 param._cam이 정의되지 않은 경우 "Designed"입니다. 또한 Incident Review(인시던트 검토)에서는 "supports_adhoc"를 true(참)로 설정해야 합니다.

해결 방법:

```
$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
```

참고: 작업의 이름이 "hive_alert_create_alert"이고 param._cam 정의가 없음을 나타냅니다. Incident Review(인시던트 검토)에 표시되지 않음을 확인했습니다.

다음으로, 간단한 매개변수(_Cam) 정의를 추가한 것뿐입니다.

<#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}
```

참고: \$Splunk_Home/etc/apps/app_name/local에서 변경

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.