IBM Security

IBM

IBM Security QRadar SOAR Add-on for Splunk User Guide V2.0.0

Date: June 2022

IBM Security QRadar SOAR
Add-on for Splunk User Guide

Version	Publication	Notes
2.0.0	June 2022	Rebranded add-on to: IBM Security QRadar SOAR Add-on for Splunk. Folder name changed to SA_QRadar_SOAR. Add SOAR case URL to Splunk ES History. Update splunklib to 1.6.20.
1.3.2	June 2022	Bug fix related to $ character in result tokens.
1.3.1	May 2022	Bug fix: Escape special characters in search result tokens.
1.3.0	November 2021	Support for creating multiple add-on instances via shell script. Use single quotes around multiselect fields containing commas. Use html format for incident description field. Max Artifacts Per Alert limit set to 99 on the Set up page. User Guide updates for Cloud Pak for Security and SaaS.
1.2.2	March 2021	Setup UI patch. Bug fix related to artifacts.
1.2.1	February 2021	Splunk Cloud compliance.
1.2.0	December 2020	Support for Resilient API keys. Ability to update an existing incident from Splunk ES. Permission for ess_analyst role to use the add-on.
1.1.0	August 2020	Added support for Python 3.
1.0.2	April 2018	Updated Splunk version number.
1.0.1	January 2018	Initial publication.

Table of Contents

Overview 5

Installation 6

- Requirements 6
- Installation and Setup 6
- Configuration 7

Escalating Splunk Alerts 9

- Adding a Splunk Alert Action 9
- Mapping Date and Datetime Fields 10
- Mapping Multiselect Fields 10
- Mapping Multiple Artifacts of the Same Type 11
- Updating the Default Case Mapping 11

Escalating Splunk ES Notable Events 12

- Adding an Adaptive Response Action 12
- Ad Hoc Invocation 14
- Show Escalated Notable Events 16
- Mapping Additional Fields 16
- Mapping Date and Datetime Fields 17
- Mapping Multiselect Fields 17
- Mapping Multiple Artifacts of the Same Type 19
- Mapping event_id for Notable Events 19
- Updating the Default Case Mapping 20

Troubleshooting 21

- Setup Screen 21
- Case Not Created 21
- Ad Hoc Invocation Failure 22

Support 23

Overview

The IBM Security QRadar SOAR Add-on for Splunk supports Splunk and Splunk ES. The add-on provides the capability of escalating a Splunk alert or Splunk ES notable event to a SOAR case, also called an incident.

The SOAR Add-on features include:

- **Easy Case Mapping**: Enables mapping of static values or search result tokens into custom fields in a SOAR case. You can map fields parsed from the event in the alert or notable event directly into any field. You also have custom case mapping rules for each saved alert or notable event.
- **Create Artifacts**: Maps result tokens into artifacts at the same time the case mapping is defined.
- **Custom Field Discovery**: Retrieves the case definition from SOAR so that all defined fields and field values are catalogued inside Splunk or Splunk ES. This allows you to add custom fields to SOAR, which are then available for mapping in Splunk or Splunk ES.
- **Automatic and manual escalation**: Escalates notable events from a correlation search or alerts from a saved search to SOAR cases (automatic escalation). For Splunk ES only, you can escalate notable events as an ad hoc action (manual escalation).

A Conversion Script package converts an instance of the add-on into a different instance with a user specified name. You can import the new instance into an on-premises Splunk installation and configure it to run with a different SOAR organization or platform. The package can be downloaded from the IBM App Exchange.

Installation

Requirements

The following lists the system requirements

- Splunk version 8.0 or later.
- Splunk ES 6.1.0 or later (only if working with Notable Events).
- Splunk CIM Framework.

  Note: The add-on depends on Splunk CIM. Install CIM before installing the add-on.
- QRadar SOAR platform version 35 or later.
- Ability to connect directly from Splunk to your QRadar SOAR platform with HTTPS on port 443.
- A dedicated SOAR Administrator or equivalent account on the SOAR platform. This can be any account that has the permission to create incidents and simulations, and view and modify administrator and customization settings. You need to know the account username and password.

  or

  A dedicated API key/secret pairing with equivalent permissions. This can be any API key that has the permission to create incidents and simulations, and view and modify administrator and customization settings. You need to know both the API key and secret.

  Note: Should you later change the dedicated SOAR account or API key, the new credentials must also have the permission to edit incidents, in addition to the permission to create incidents and simulations and view and modify administrator and customization settings. The edit permission is necessary so that the integration can continue to modify or synchronize the incidents escalated by the original user account.

  You can refer to the Playbook Designer Guide for more information about simulations.
- Splunk admin role for the user who installs and sets up QRadar SOAR Add-on for Splunk. Both the admin and ess_analyst roles may use the add-on as an Alert Action or an Adaptive Response Action for a correlation search.

Installation and Setup

If upgrading SA_QRadar_SOAR, clear your browser cache after installing the upgrade.

For Splunk Cloud and Splunk ES Cloud users, contact Splunk Support to create a ticket for installing the QRadar SOAR Add-on for Splunk.

If you have installed Splunk or Splunk ES on-premises, you can download and install the add-on from Splunkbase. Alternatively, you can request an installer from IBM QRadar SOAR.

After installing the add-on in a standalone or a search head cluster environment and restarting Splunk, navigate back to the Apps Manager screen. Click **Set up** in the SA_QRadar_SOAR row. Fill out the required attributes for your SOAR and click **Submit**. When you **Submit**, the Set Up program performs the following:

- Retrieves the case definition from SOAR so that all fields, including custom fields, are catalogued.

Note: If a SOAR administrator adds custom fields after you run **Set up**, you need to run **Set up** again to capture the new fields.

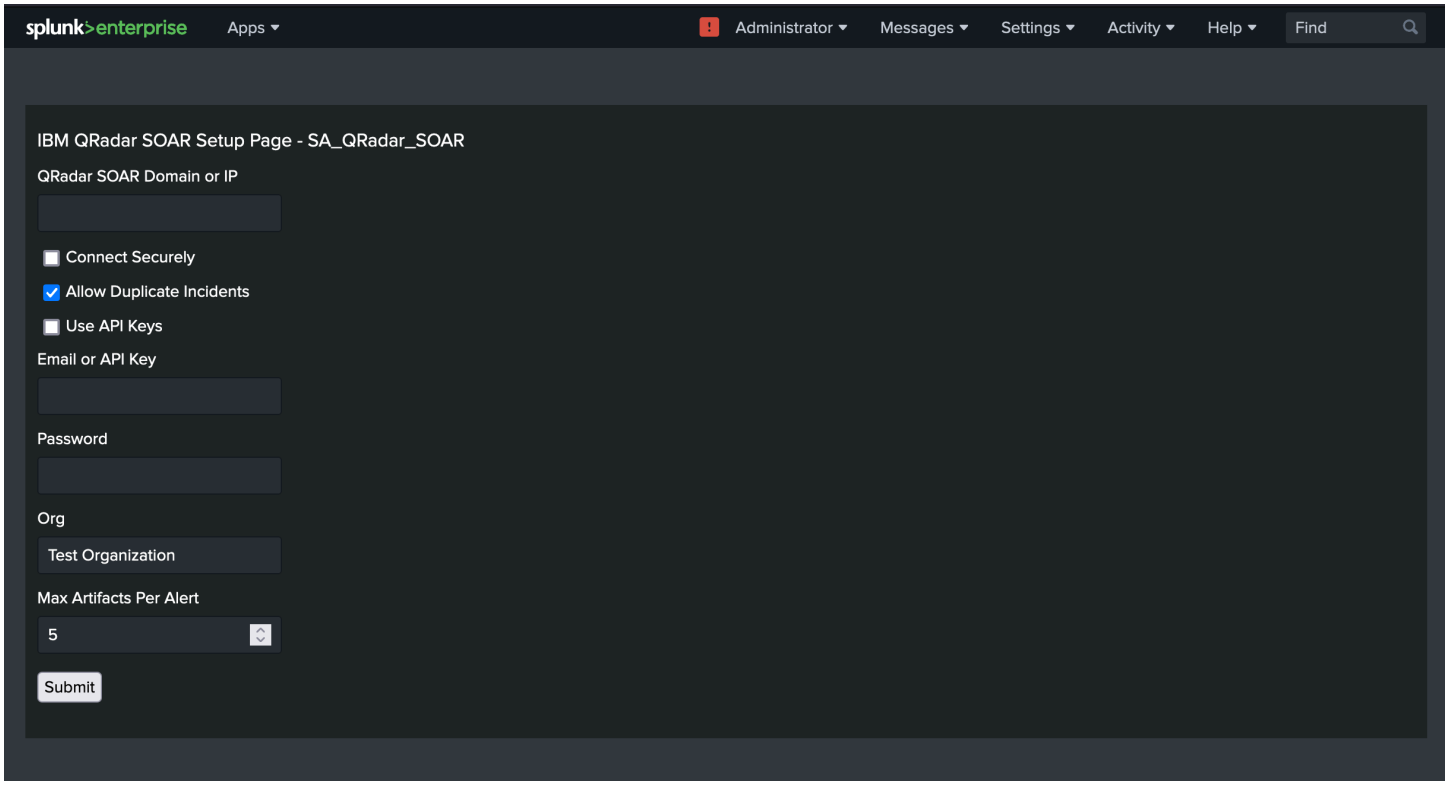
Note: If running in a search head cluster environment, **Set up** needs to be executed on one search head member only. **Set up** information is replicated to each of the other search head members after hitting **Submit** with successful completion.

- Tests the configuration to verify that the connection is successful. If the configuration saves successfully, you are up and running.

Refer to the Troubleshooting section if you encounter a problem.

Configuration

Configure the QRadar SOAR Add-on for Splunk to access your SOAR on the Setup Page pictured below. Navigate to this page from the **Apps Manager** screen.



Guidelines for configuring the **Set Up** Page parameters:

- **QRadar SOAR Domain or IP**: Hostname or IP for your SOAR. Do not include the https:// prefix.

  Note: If configuring for Cloud Pak for Security, prefix the hostname with **cases-rest.**

  For example: cases-rest.cp4s-domain.com

  If configuring for Cloud Pak for Security SaaS, contact CP4S SaaS Support for the cases rest and stomp endpoints.

  For DNS Mapping, the user should save the IP and domain name in the file **/etc/hosts** on the Splunk server.

- **Connect Securely**: Do not check if using self-signed certificates on your SOAR.
- **Allow Duplicate Incidents**: If **unchecked**, the add-on searches for an existing open case or incident in SOAR and, if found, updates that case. If there is no match, a new case is created. If this box is **checked**, a new case is created every time the action is triggered.

  Note: Updating existing cases or incidents in SOAR requires use of Splunk ES and the splunk_notable_event_id custom field. See Mapping event_id for Notable Events.
- **Use API Keys**: **Check** to authenticate with SOAR using an API key and secret. **Uncheck** to authenticate with SOAR using an email and password.

  Note: If configuring for Cloud Pak for Security, API key must be used.
- **Org**: The name of the SOAR organization.

  Note: If configuring for Cloud Pak for Security, the Org name must be in UUID format.
- **Email or API key**: Email address or API key ID you use when authenticating with SOAR.

  Note: If configuring for Cloud Pak for Security, API key must be used.
- **Password**: Password for the SOAR account or API key secret for the SOAR API key. This is a mandatory field, and the value must be entered before clicking **Submit**.
- **Max Artifacts per alert**: Maximum number of artifacts you may need to map into a single SOAR case from any given Splunk alert or Splunk ES notable event. This field takes an integer.

Note: Wait a few moments after clicking **Submit** to allow the setup process to complete. Your browser displays a pop-up dialog with the results of the setup process when completed. Once you have successfully configured the add-on, the setup page displays the last successful configuration in the form, except for **Password**, which you must enter.

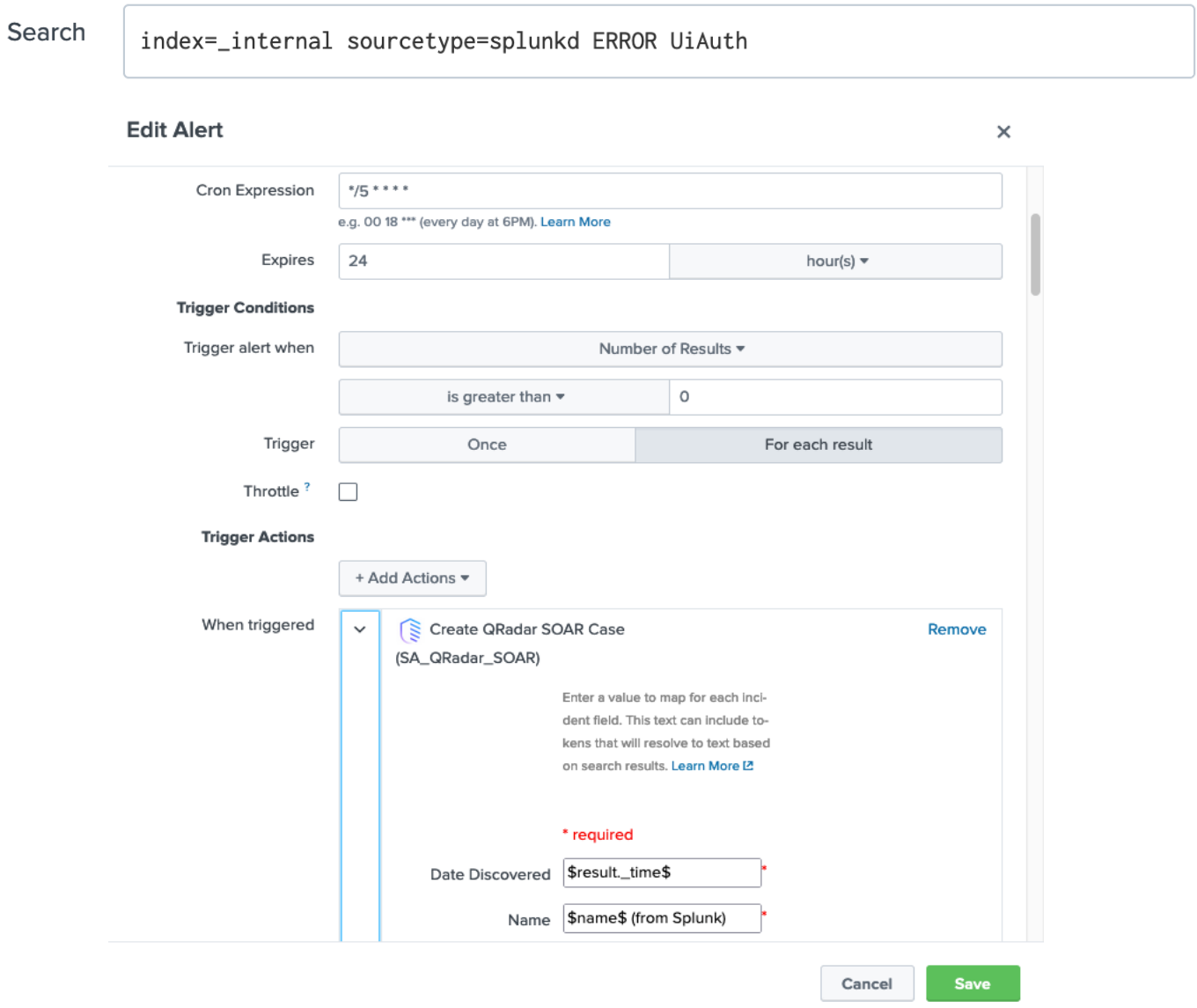
Escalating Splunk Alerts

Adding a Splunk Alert Action

To add a SOAR escalation to an alert, go to the **Alerts** tab in the Search & Reporting app and find the alert for which you want to create a SOAR case. Click **Edit** and select **Edit Actions**. Click **+ Add Actions** and select **Create QRadar SOAR Case (SA_QRadar_SOAR)**. Update the fields to indicate how you want them mapped. You can use static values or tokens from the alert data. In addition to the fields parsed in your particular alert search, the Splunk documentation has a list of the default tokens available in any search.

Be sure to map a valid value for the Date Discovered field, which is always required.

A sample alert, failed_splunk_login_send_to_qradar_soar, is included. If you enable this alert, a SOAR case is created each time there is a failed login attempt to Splunk. If you have added custom required fields to your SOAR, you need to edit the mapping on the alert action screen to include them before triggering the example.



Mapping Date and Datetime Fields

If mapping values from Splunk to Date Picker or Date Time Picker fields in SOAR, the formatting of those values in the mapping must meet certain requirements. If you are parsing the date/datetime value from the Splunk search using a token, the value is already properly formatted and there is no additional action required. However, if you are providing a static value for the mapping, dates must be formatted as *YYYY/MM/DD*. Similarly, datetime values must be provided as *YYYY/MM/DD HH:MM:SS ±xxxx*. The *±xxxx* following the time is the UTC offset value. For example, the value for Cambridge, Massachusetts, United States is *–0500*. Be sure to include a leading zero if your offset value is a single-digit number of hours.

In Python3, you may include a colon between the hour and minute values (in the Cambridge example this is *–05:00*). However, in Python2 the UTC offset must be only the directional sign and exactly four digits. This value is optional when providing a static datetime. If you do not provide a UTC offset value, the datetime object is assumed to be in Greenwich Mean Time (GMT).

Mapping Multiselect Fields

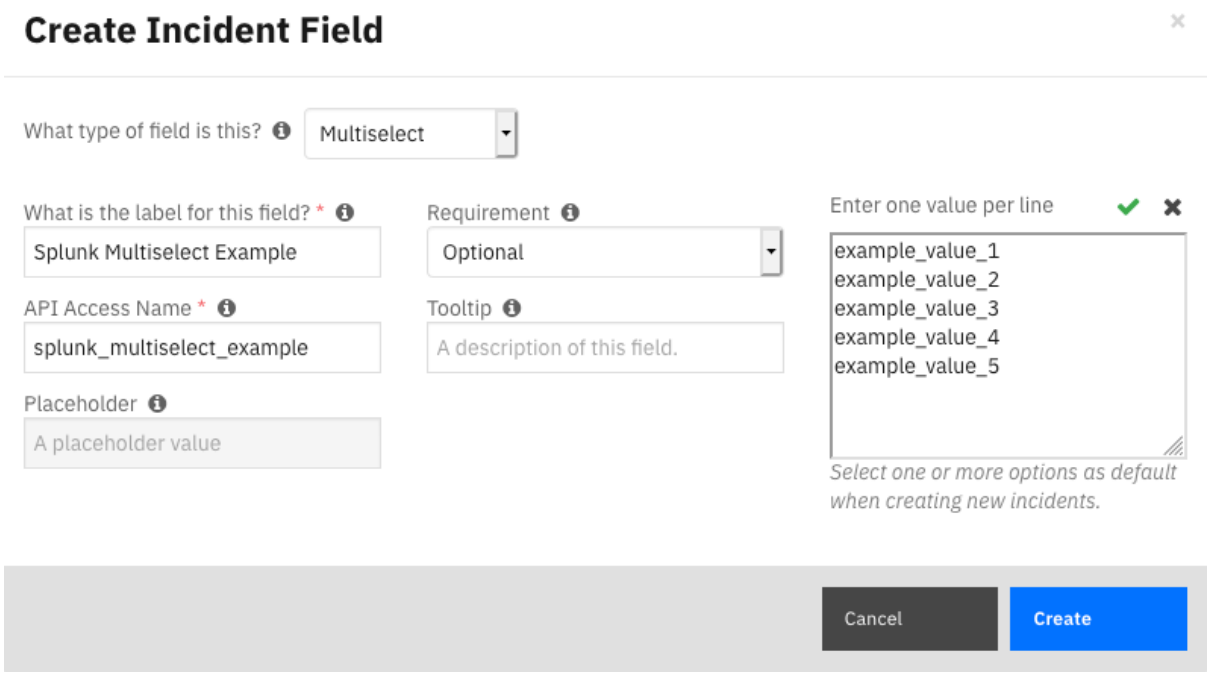
If mapping values from Splunk to Multiselect field in SOAR, these values must be supplied as comma separated values (CSV) with no spaces. For example, two valid value formats to map are:

- *1,2,3*
- *$result.value1$,$result.value2$,$result.value3$*

The following introduction of spaces **generates errors** when creating the case in SOAR.

- *1, 2,3*
- *$result.value1$,$result.value2$, $result.value3$*

These examples assume that values 1, 2, 3 and the values returned from Splunk after evaluating $result.value1$, $result.value2$, and $result.value3$ are valid selections for the multiselect field you desire to fill or update in SOAR. You need to define these accepted values manually.



Note: Use single quotes around any multiselect value that contains comma or special characters.

Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the SOAR UI, you can add multiple artifacts of the same type at once as long as the artifact type allows multiple values. This setting can be found under **Customization Settings > Artifacts** in SOAR. URLs need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

Updating the Default Case Mapping

You can change the default mapping when you configure the action. If the case mapping for most of your alerts will be very similar, you may want to override the default mapping where all the alerts start. Create an alert_actions.conf in *$SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/local* and override the default mappings.

Escalating Splunk ES Notable Events

Adding an Adaptive Response Action

To add a SOAR escalation to a correlation search, go to the **Configure** tab in the Enterprise Security App, and select **Content Management**. Click the correlation search for which you want to create a SOAR case and scroll down to the **Adaptive Response Actions** section. Click **+ Add New Response Action** and select **Create QRadar SOAR Case (SA_QRadar_SOAR)**. Update the case fields to indicate how you want them mapped.

To create a new correlation search, go to the **Configure** tab in the Enterprise Security App and select **Content Management**. Click **Create New Content** and select **Correlation Search**. Create a new correlation. A sample correlation search failed_splunk_login_ES_send_to_qradar_soar, is included, which you can find in **Content Management**.

Correlation Search

Search Name: failed_splunk_login_ES_send_to_qradar_soar

App: QRadar SOAR Case Creation from Splunk

UI Dispatch Context: Select...

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description: Create a case when login to splunk server failed.

Mode: Guided | Manual

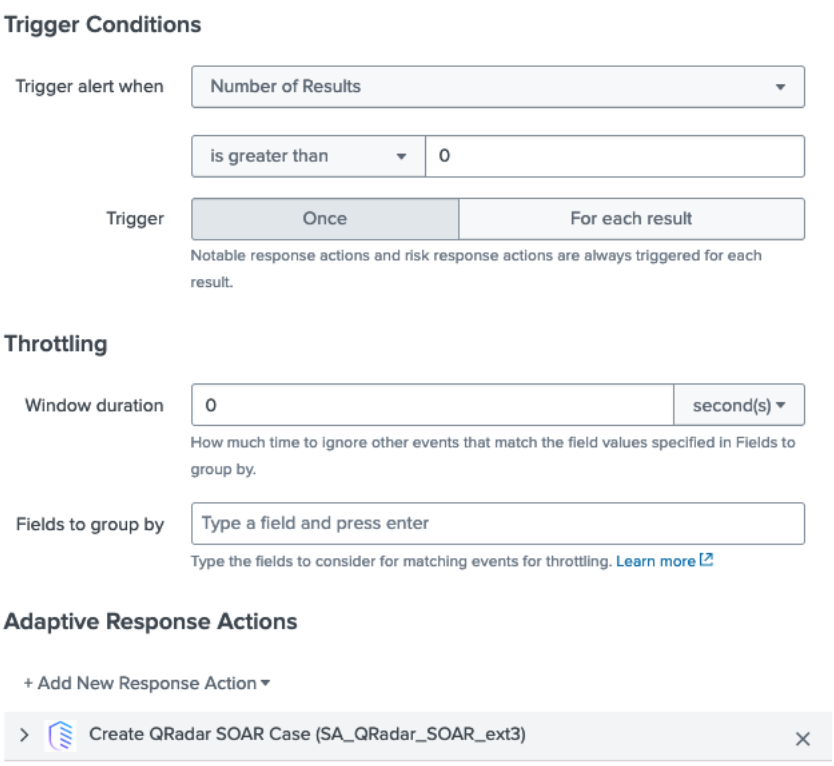
Search:

```
index=_internal sourcetype=splunkd ERROR UiAuth | `get_event_id`
```

Annotations

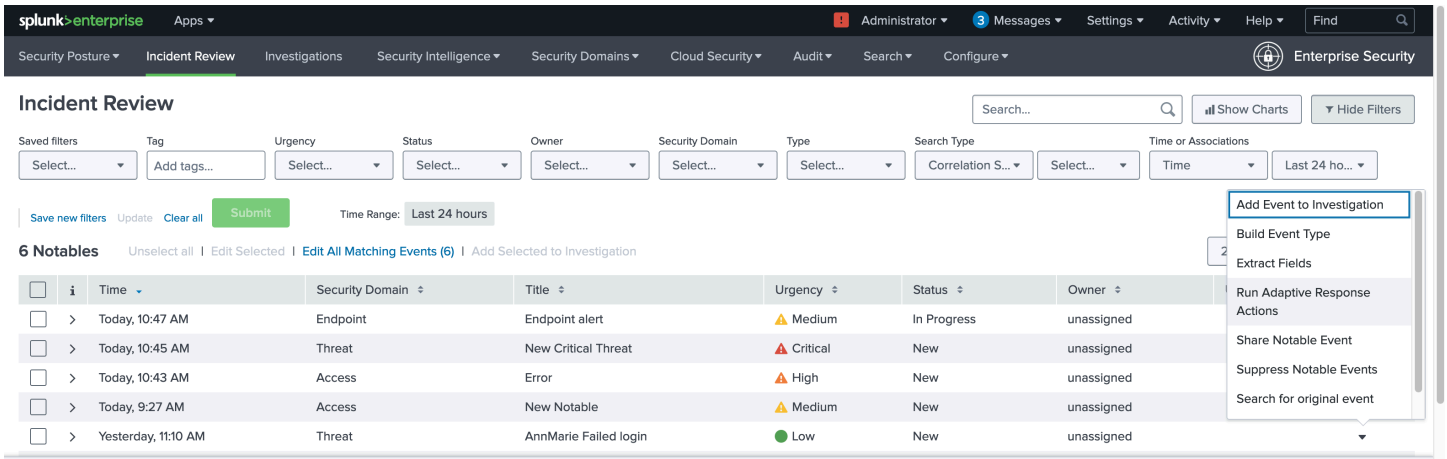
CIS 20: Type an attribute and press enter

Scroll down to the Adaptive Response Actions section and view that the QRadar SOAR Add-on has been added as a response in this sample correlation search. You can change the default configuration.

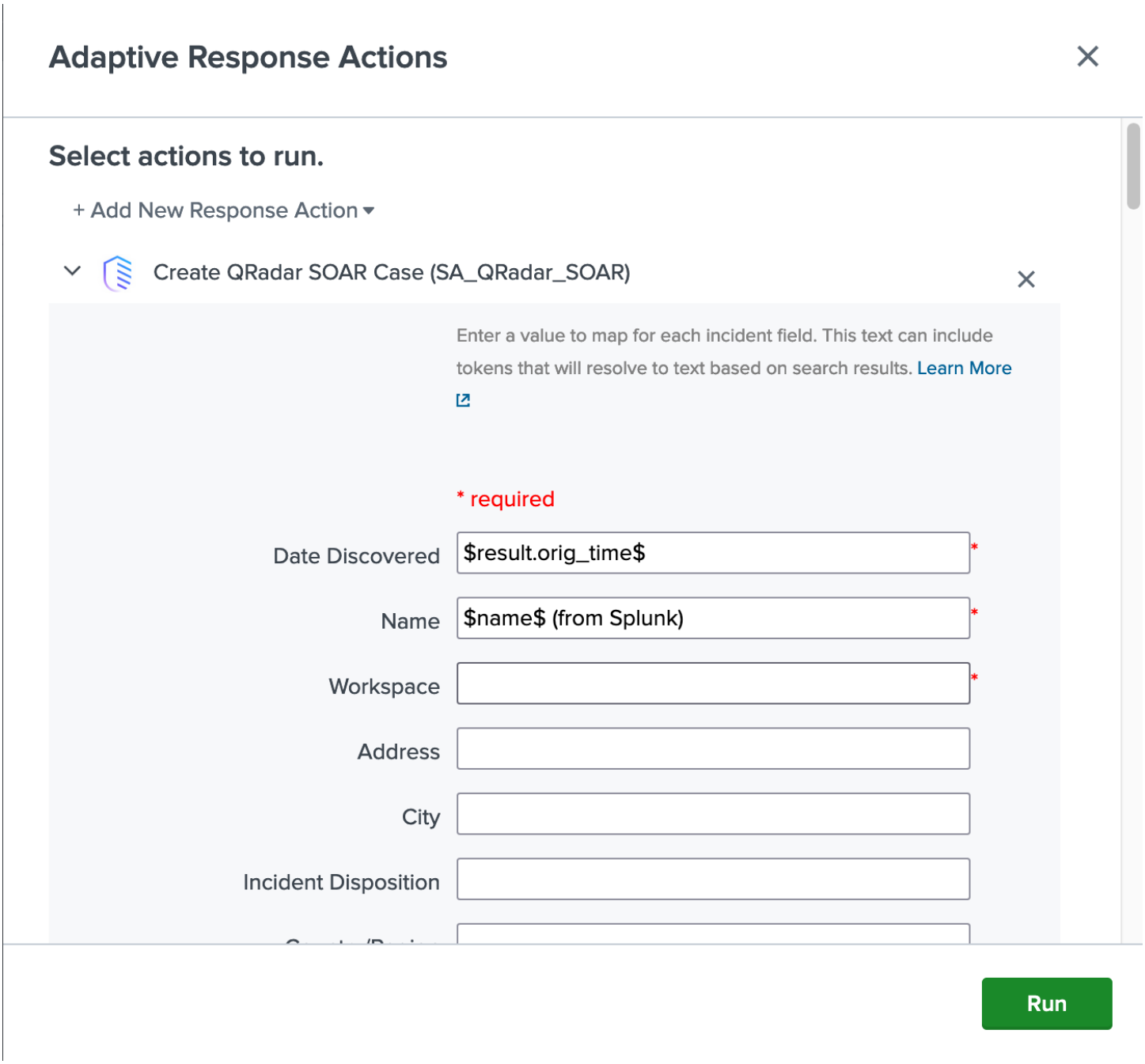


Ad Hoc Invocation

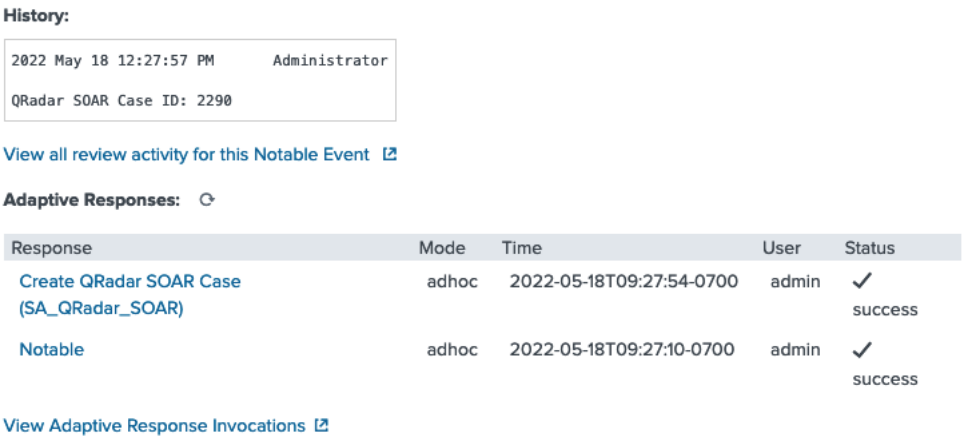
You can dispatch QRadar SOAR Add-on as an ad hoc invocation. To escalate a notable event, go to the Incident Review tab of Enterprise Security. Locate the notable event that you wish to escalate and select **Run Adaptive Response Actions** in the Actions column.



Click **+ Add New Response Action** and select **Create QRadar SOAR Case (SA_QRadar_SOAR).** Update the case fields to indicate how you want them mapped.

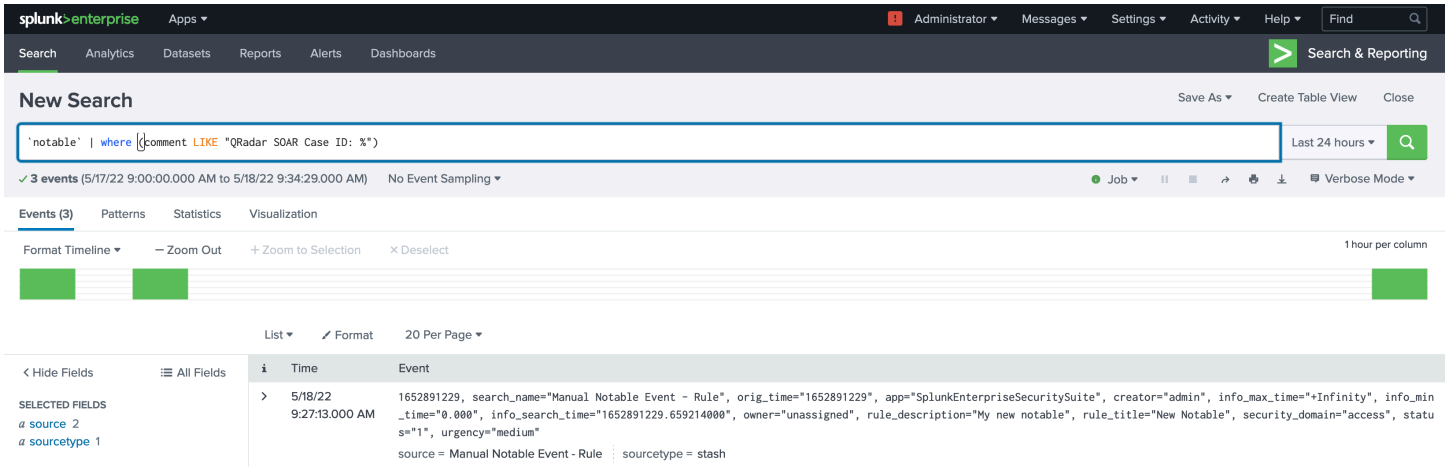


Click **Run** to escalate. Once completed, refresh the page to see the updated notable event. The comment contains the Case ID for the case created. The **Adaptive Responses** field, shown below, displays a success status for **Create QRadar SOAR Case**.



Show Escalated Notable Events

Each time a notable event is escalated successfully, the corresponding SOAR Case ID is added to the comment field of the notable event. This allows Splunk ES users to easily search for all the notable events escalated successfully. To perform a search, enter the search parameter, such as **`notable` | where (comment LIKE "QRadar SOAR Case ID: %")**, in the **Search** tab of **Enterprise Security**. For example:



Mapping Additional Fields

You can customize Splunk ES notable events by adding additional fields, as described in the Splunk documentation. The additional fields can be used in mapping as the following token:

```
$result.additional_field_label$
```

The **additional_field_label** is the label used for the additional field.

Mapping Date and Datetime Fields

If mapping values from Splunk to Date Picker or Date Time Picker fields in SOAR, the formatting of those values in the mapping must meet certain requirements. If you are parsing the date/datetime value from the Splunk search using a token, the value is already properly formatted and there is no additional action required. However, if you are providing a static value for the mapping, dates must be formatted as *YYYY/MM/DD*. Similarly, datetime values must be provided as *YYYY/MM/DD HH:MM:SS ±xxxx*. The *±xxxx* following the time is the UTC offset value. For example, the value for Cambridge, Massachusetts, United States is *–0500*. Be sure to include a leading zero if your offset value is a single-digit number of hours.

In Python3, you may include a colon between the hour and minute values (in the Cambridge example this is *–05:00*). However, in Python2 the UTC offset must be only the directional sign and exactly four digits. This value is optional when providing a static datetime. If you do not provide a UTC offset value, the datetime object is assumed to be in Greenwich Mean Time (GMT).

Mapping Multiselect Fields

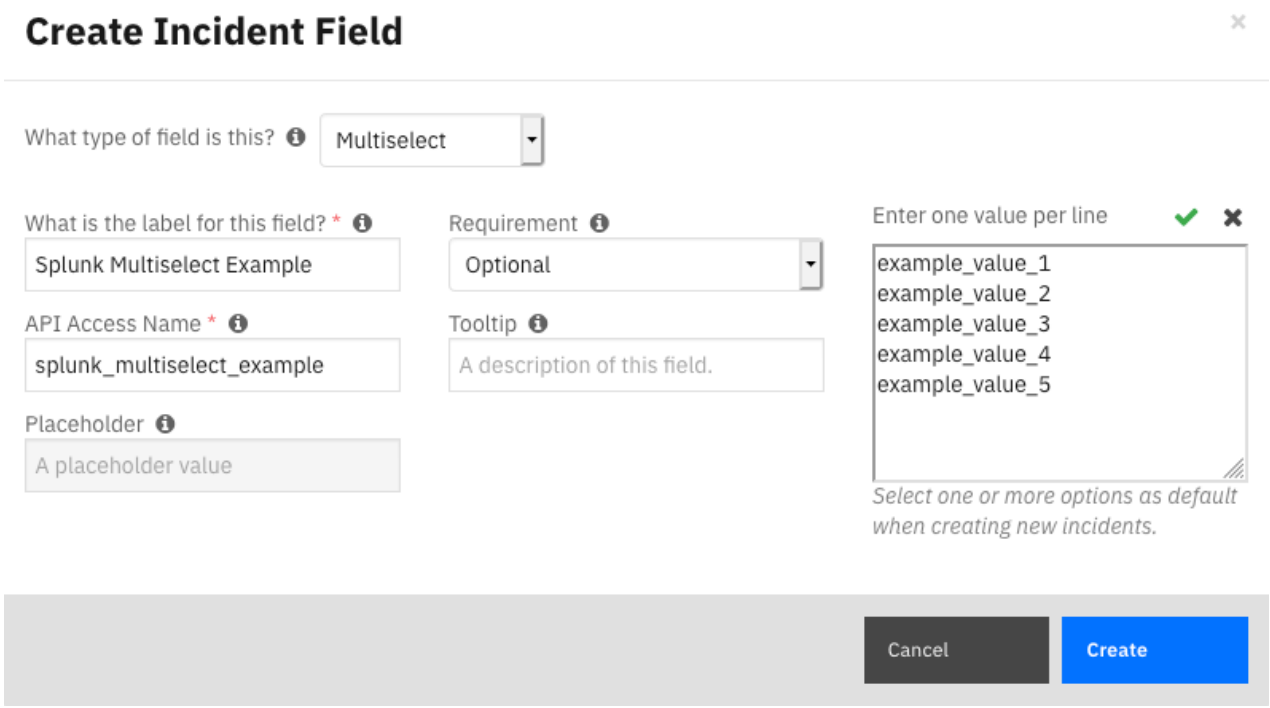
If mapping values from Splunk to Multiselect field in SOAR, these values must be supplied as comma separated values (CSV) with no spaces. For example, two valid value formats to map are:

- *1,2,3*
- *$result.value1$,$result.value2$,$result.value3$*

The following introduction of spaces generates errors when creating the case in SOAR.

- *1, 2,3*
- *$result.value1$,$result.value2$, $result.value3$*

These examples assume that values 1, 2, 3 and the values returned from Splunk after evaluating $result.value1$, $result.value2$, and $result.value3$ are valid selections for the multiselect field you desire to fill or update in SOAR. You need to define these accepted values manually.


Create Incident Field
What type of field is this?
Multiselect
What is the label for this field? *
Splunk Multiselect Example
API Access Name *
splunk_multiselect_example
Placeholder
A placeholder value
Requirement
Optional
Tooltip
A description of this field.
Enter one value per line
example_value_1
example_value_2
example_value_3
example_value_4
example_value_5
Select one or more options as default when creating new incidents.
Cancel
Create

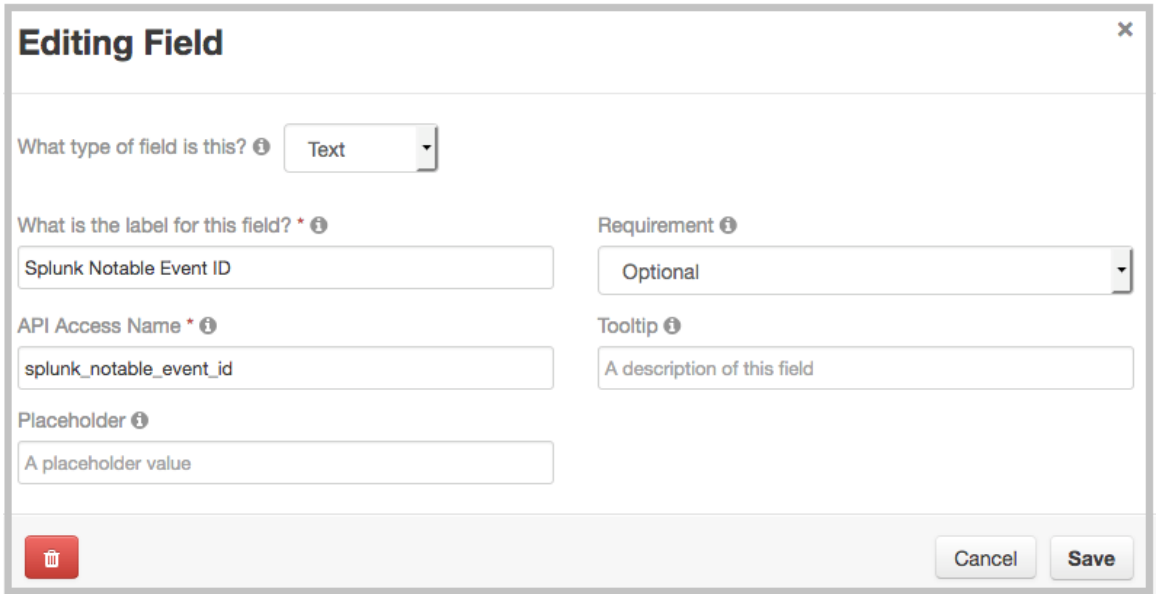
Mapping Multiple Artifacts of the Same Type

Similar to adding artifacts manually through the SOAR UI, you can add multiple artifacts of the same type at once if the artifact type allows multiple values. This setting can be found under **Customization Settings > Artifacts** in SOAR. URL's need to be separated by a space and IP addresses must be comma-separated. Artifacts can also be mapped individually.

Mapping event_id for Notable Events

In SOAR, it is recommended that you create a customized field in the SOAR case for the Splunk notable event_id. In the following example, the splunk_notable_event_id of a notable event is mapped to the customized field. Refer to the *SOAR Playbook Designer Guide* for details.

Note: To use the update case capability and avoid creating duplicate cases, this field must have an API name of exactly splunk_notable_event_id as shown below.



Updating the Default Case Mapping

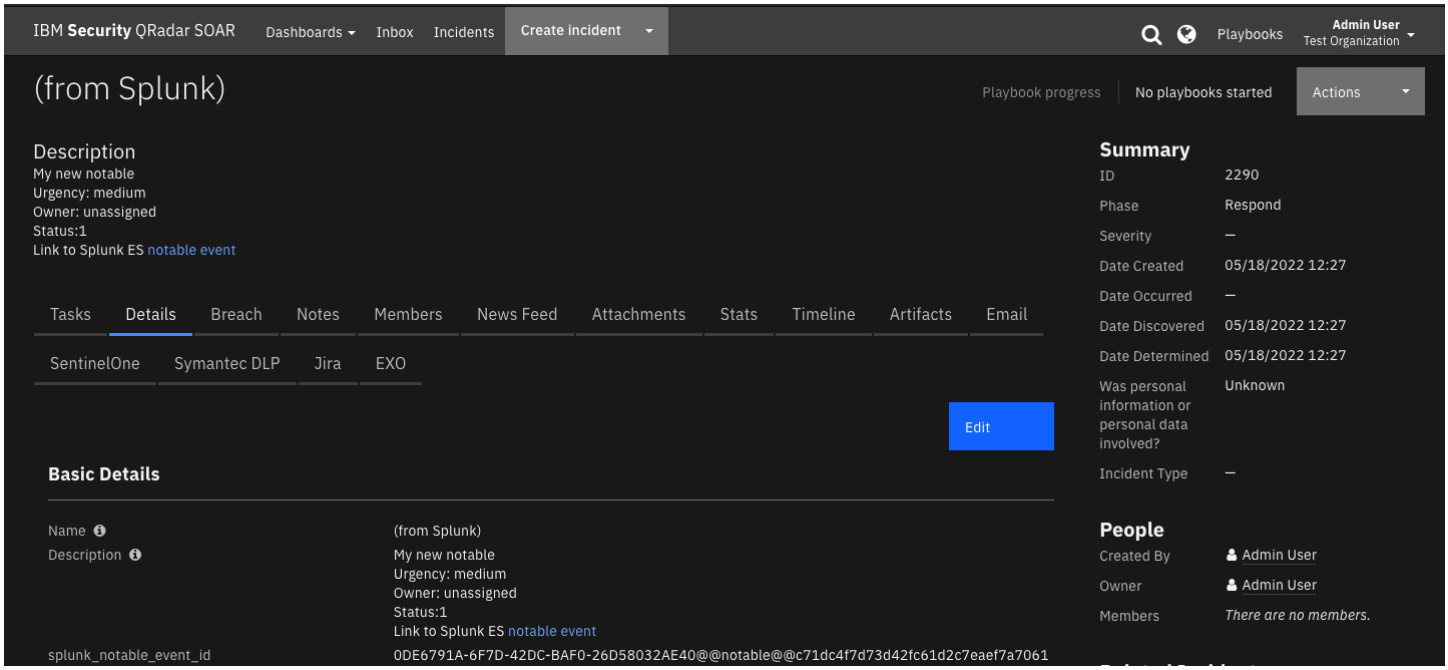
Default mapping is provided in:

```
$SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/default/alert_actions.conf
```

This default mapping includes the following tokens. The mapping also includes a hyperlink to the notable event from Splunk ES.

Field	Token
Title of the notable	$result.rule_title$
Urgency	$result.urgency$
Owner	$result.owner$
Notable description	$result.rule_description$
Status	$result.status$

The following is an example of a case created in SOAR from the mapping.

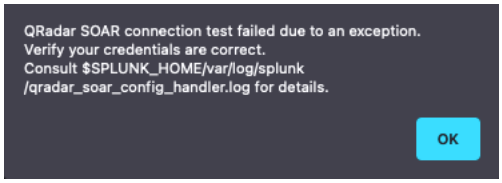


You can change the default mapping when you configure the action.

Troubleshooting

Setup Screen

When you click **Submit** on the QRadar SOAR Setup screen in Splunk, the app attempts to make a connection to your SOAR to verify that everything is configured correctly and to update the stored case definition. If this connection fails, you see an alert error that looks like this:



After a few seconds, the Splunk messages tab updates with detailed information about the cause of the failure.

Further information is logged to the following locations in Splunk:

- $SPLUNK_HOME/var/log/splunk/qradar_soar_config_handler.log
- $SPLUNK_HOME/var/log/splunk/splunkd.log
- $SPLUNK_HOME/var/log/splunk/python.log

Some common causes of these issues include:

- Forgot to uncheck the “Connect securely?” box for self-signed certificate.
- Port 443 is blocked.

Case Not Created

If an alert or automatic escalation for correlation search fails to create a case, a message should be logged into the Splunk messages tab informing you of the issue. Further information is logged to the following location in Splunk:

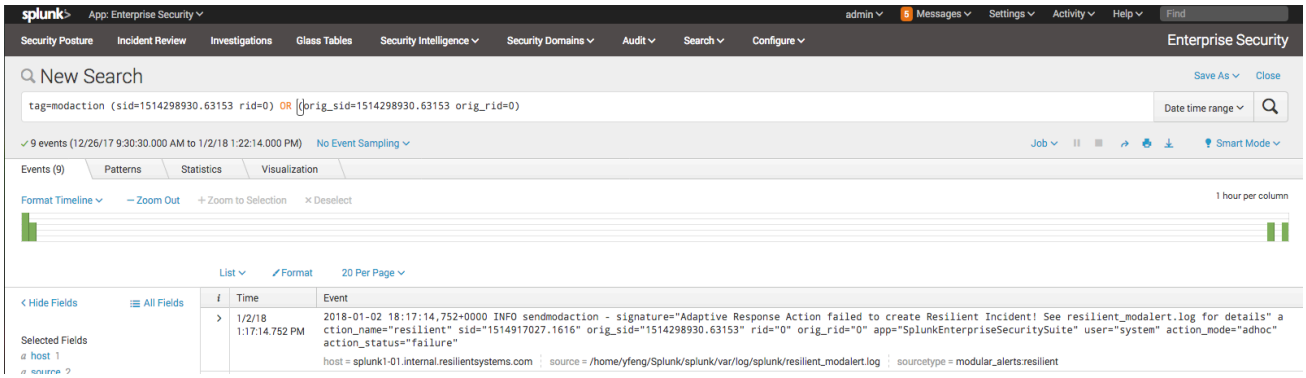
- $SPLUNK_HOME/var/log/splunk/qradar_soar_modalert.log

Some common causes of these issues include:

- Insufficient permissions to create a case, incident, or simulation.
- Missing mappings for required fields.
- Fields mapped with invalid values.
- Connection unavailable.

Ad Hoc Invocation Failure

You can view the status of an ad hoc invocation when you refresh the Adaptive Response page. If it fails, click **View Adaptive Response Invocations**. In the search result, you should see a message, “See qradar_soar_modalert.log for details.”



You can then open $SPLUNK_HOME/var/log/qradar_soar_modalert.log to look for details about the failure.

If the Splunk UI dispatches an error in the UI during an adhoc invocation that reads:

“*SA_QRadar_SOAR could not be dispatched: ModularActionException: Invalid parameter for adhoc modular action*”

It is likely that a .conf file has been edited by a person or app other than SA_QRadar_SOAR. To resolve this issue, try running the setup process for SA_QRadar_SOAR again. If the manual action still fails to complete after re-running the setup process, you may need to manually delete all entries in $SPLUNK_HOME/etc/apps/SA_QRadar_SOAR/local/alert_actions.conf and run the setup process one more time to bring in the SOAR field definitions from scratch.

Support

For additional support, go to https://ibm.com/mysupport.

Including relevant information will help us resolve your issue:

- version of Splunk / Splunk Cloud
- version of Enterprise Security Add-On
- version of QRadar SOAR Add-on for Splunk
- if using Splunk 8 - which Python interpreter your server is using
- steps/screenshots that will help us reproduce your issue

Including log files located in $SPLUNK_HOME/var/log/splunk:

- splunkd.log
- python.log
- qradar_soar_config_handler.log
- qradar_soar_modalert.log