# Splunk® Enterprise Security
# Administer Splunk Enterprise Security 7.0.1

## Configure adaptive response actions for a correlation search in Splunk Enterprise Security

Generated: 6/13/2022 9:54 am

# Configure adaptive response actions for a correlation search in Splunk Enterprise Security

As a Splunk Enterprise Security admin, you can configure which adaptive response actions that a correlation search triggers.

Analysts can run some adaptive response actions on an ad hoc basis from Incident Review. See Included adaptive response actions with Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Splunk Enterprise Security includes several adaptive response actions, and you can obtain additional ones from add-ons available on Splunkbase.

## Included adaptive response actions

Splunk Enterprise Security includes several adaptive response actions.

- Create a notable event.
- Modify a risk score with a risk modifier.
- Send an email.
- Run a script.
- Start a stream capture with Splunk Stream.
- Ping a host.
- Run Nbtstat.
- Run Nslookup.
- Add threat intelligence.
- Create a Splunk Web message.

Search commands and adaptive response actions such as ping, nbtstat, and nslookup can no longer send results to customized indexes. Results from search commands and adaptive response actions such as ping, nbtstat, and nslookup are written to the default index.

## Create a notable event

Create a **notable event** when the conditions of a correlation search are met.

1. On the Splunk Enterprise Security menu bar, click **Configure > Content > Content Management**.
2. Click an existing correlation search, or click **Create New > Correlation Search**.
3. Click **Add New Response Action** and select **Notable** to add a notable event.
4. Type a **Title** of the notable event on the **Incident Review** dashboard. Supports variable substitution from the fields in the matching event.
5. Type a **Description** of the notable event. Supports variable substitution from the fields in the matching event
6. Select the **Security Domain** of the notable event from the drop-down list.
7. Select the **Severity** of the notable event from the drop-down list. The severity is used to calculate the **Urgency** of a notable event.
8. (Optional) Change the default owner of the notable event from the system default, **unassigned**.
9. (Optional) Change the default status of the notable event from the system default, **New**.
10. Type a drill-down name for the **Contributing Events** link in the notable event.

11. Type a drill-down search for the **Contributing Events** link in the notable event.
12. In the **Drill-down earliest offset** field, type the amount of time before the time of the triggering event to look for related events for the **Contributing Events** link in the notable event.
    For example **2h** to look for contributing events 2 hours before the triggering event.
13. In the **Drill-down latest offset** field, type the amount of time after the time of the triggering event to look for related events for the **Contributing Events** link in the notable event.
    For example, **1h** to look for contributing events 1 hour after the triggering event.
14. (Optional) Add **Investigation Profiles** that apply to the notable event.
    For example, add an investigation profile that fits a use case of "Malware" to malware-related notable events.
15. (Optional) Add fields that contain assets in **Asset Extraction** to extract the field values and add them to the investigation workbench as artifacts when the notable event is added to an investigation.
16. (Optional) Add fields that contain identities in **Identity Extraction** to extract the field values and add them to the investigation workbench as an artifact when the notable event is added to an investigation.
17. Type **Next Steps** for an analyst to take after triaging a notable event. Type text or click **Insert Adaptive Response Action** to reference a response action in the text of the next steps. You can only type plain text and links to response actions in the next steps field. Use next steps if you want to recommend response actions that should be taken in a specific order.
    For example, ping a host to determine if it is active on the network. If the host is active, increase the risk score by 100, otherwise, increase the risk score by 50.
18. Select **Recommended Actions** to complement the next steps. From the list of all adaptive response actions, click the name of an action that you recommend as a triage or investigation step for this notable event to add it to the list of recommended actions that analysts can take for this notable event. You can add as many recommended actions as you like. Use recommended actions to recommend response actions that do not need to be taken in a specific order.
    For example, increase the risk score on a host and perform an nslookup on a domain name.

In Splunk Enterprise Security versions lower than 6.1.1, correlation searches can produce a notable event with an "invalid" severity, resulting in a less than ideal urgency calculation. In Splunk Enterprise Security 6.1.1 and higher, notable event severity is validated as one of "critical," "high," "medium," "low," or "informational." If it is not one of the aforementioned values, the severity is set to "unknown." From there, normal urgency calculations apply. See How urgency is assigned to notable events in Splunk Enterprise Security.

## Modify a risk score with a risk modifier

Modify a risk score as a result of a correlation search or in response to notable event details with the **Risk Analysis** adaptive response action. The risk adaptive response action creates a risk modifier event. You can view the risk modifier events on the Risk Analysis dashboard in Enterprise Security.

1. Click **Add New Response Action** and select **Risk Analysis**.
2. Click **+** to add a risk modifier.
    1. Type a positive or a negative integer or a decimal number in the **Risk Score** field to assign a value to the risk object.
    2. In the **Risk Object Field**, type the name of a field that exists in the correlation search to apply the risk score to the field.
       For example, type **src** to specify the source field.
    3. In the **Risk Object Type** field, select the name of an object type to specify wether the entity is a system, user, or other. The list is shown based on results from the `|`risk_object_types`` macro. For example, **host_artifacts** for an asset.
3. Click **+** to add additional risk modifiers and follow the previous steps a-c to assign different risk scores to different fields.

This view is unique to the correlation search editor. You do not see it, for example, in the adaptive response actions through Incident Review.

See Assign risk to an object in *Use Splunk Enterprise Security* for other ways to modify risk scores.

## Add a threat object to modify an adaptive response action

Modify an adaptive response action by adding a threat object and correlating it with a risk modifier.

1. In the Correlation Search Editor, scroll down to **Adaptive Response Actions** and expand **Risk Analysis**.
2. Click **+** to add a Threat Object.
3. Populate the **Threat Object Field** by typing in a description of the threat object. For example: `payload`
4. Populate the **Threat Object Type** with the type of the threat object. For example: `file_hash`
5. Click **+** to add additional threat objects.

You may also modify an adaptive response action to add threat objects from the Incident Review dashboard. You may also add a threat object to an ad hoc risk entry to correlate threat objects with risk events and make adjustments to the risk score.

## Send an email

Send an email as a result of a correlation search match.

### Prerequisite

Make sure that the mail server is configured in the Splunk platform before setting up this response action.

- For Splunk Enterprise, see Configure email notification settings in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud Platform, see Configure email notification settings in the Splunk Cloud Platform *Alerting Manual*.

### Steps

1. Click **Add New Response Action** and select **Send email**.
2. In the **To** field, type a comma-separated list of email addresses to send the email to.
3. (Optional) Change the priority of the email. Defaults to **Lowest**.
4. Type a subject for the email. The email subject defaults to "Splunk Alert: $name$", where $name$ is the correlation search **Search Name**.
5. Type a message to include as the body of the email. Defaults to "The scheduled report '$name$' has run."
6. Select the check boxes of the information you want the email message to include.
7. Select whether to send a plain-text or HTML and plain-text email message.

If you're using the **Override Email Alert Action** in the general settings, the `subject="$action.email.subject$"` is passed explicitly. The default `useNSSubject` for use in local savedsearches `$action.email.subject.alert$` and `$action.email.subject.report$` is ignored. See Configure general settings for Splunk Enterprise Security.

When using "'Send email'" from the adaptive response actions through Incident Review, token replacement is not supported based on event fields. For example, you cannot use an email subject such as "Splunk Alert: $name$", where $name$ is the correlation search name. Since this is an ad-hoc adaptive response action rather than a scheduled saved search, the $name$ token does not apply. Token replacement is supported from the adaptive response actions

through the correlation search editor.

## Configure trigger conditions for notables

Configure trigger conditions for notables so that the appropriate number of notables are generated during a correlation search. **Steps**

1. On the Splunk Enterprise Security menu bar, click **Configure > Content > Content Management**.
2. Click **Create New > Correlation Search**.
   This opens the correlation search editor.
3. Scroll down to the section on **Trigger Conditions**
4. Select the frequency of notifications that you want based on alert search results.
5. Select one of two options: **Once** or **For each result**.

When the event pattern occurs, the alert can trigger just once or one time for each result in the pattern. You can choose an option depending on the notification or other alert action behavior that you want. However, selecting either of the options does not impact the Notable Adaptive response actions, such as **Send Email**.
For **Send Email**, if you select **Once** as the trigger frequency option, you will trigger the alert only once for each time the search results match the specified condition and receive a single notification in your inbox. If you select **For each result**, you will trigger multiple notifications but with the same number of notables. Trigger condition for **Send Email** is an exception and does not impact the total number of notables that are generated. Even if you receive multiple email notifications, many of the notables might just be duplicates.

## Run a script

Run a script stored in `$SPLUNK_HOME/bin/scripts`.

1. Click **Add New Response Action** and select **Run a script**.
2. Type the file name of the script.

More information about scripted alerts can be found in the Splunk platform documentation.

- For Splunk Enterprise, see Configure scripted alerts in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud Platform, see Configure scripted alerts in the Splunk Cloud Platform *Alerting Manual*.

## Start a stream capture with Splunk Stream

Start a stream capture to capture packets on the IP addresses of the selected protocols over the time period that you select. You can view the results of the capture session on the Protocol Intelligence dashboards.

A stream capture will not work unless you integrate Splunk Stream with Splunk Enterprise Security. See Integrate Splunk Stream with Splunk Enterprise Security.

1. Click **Add New Response Action** and select **Stream Capture** to start a packet capture in response to a correlation search match.
2. Type a **Description** to describe the stream created in response to the correlation search match.
3. Type a **Category** to define the type of stream capture. You can view streams by category in Splunk Stream.
4. Type the comma-separated event fields to search for IP addresses for the Stream capture. The first non-null field is used for the capture.
5. Type the comma-separated list of protocols to capture.

6. Select a **Capture duration** to define the length of the packet capture.
7. Type a **Stream capture limit** to limit the number of stream captures started by the correlation search.

## Ping a host

Determine whether a host is still active on the network by pinging the host.

1. Click **Add New Response Action** and select **Ping**.
2. Type the event field that contains the host that you want to ping in the **Host Field**.
3. Type the number of maximum results that the ping returns. Defaults to 1.
4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud Platform ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud Platform ES search head. See Set up an adaptive response relay from a Splunk Cloud Platform Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

## Run nbtstat

Learn more about a host and the services that the host runs by running nbtstat.

1. Click **Add New Response Action** and select **Nbtstat**.
2. Type the event field that contains the host that you want to run the nbtstat for in the **Host Field**.
3. Type the number of maximum results that the nbtstat returns. Defaults to 1.
4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud Platform ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud Platform ES search head. See Set up an adaptive response relay from a Splunk Cloud Platform Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

## Run nslookup

Look up the domain name of an IP address, or the IP address of a domain name, by running nslookup.

1. Click **Add New Response Action** and select **Nslookup**.
2. Type the event field that contains the host that you want to run the nslookup for in the **Host Field**.
3. Type the number of maximum results that the nslookup returns. Defaults to 1.

4. (Optional) Select an index from the drop-down list to save the results to an existing index or a custom index. Defaults to main.
5. (Optional) Select a worker set from the drop-down list to use for executing adaptive response actions on a Splunk Cloud Platform ES search head.

Custom indexes are configurable for the adaptive response actions of ping, nbtstat, and nslookup so that you can separate those out from the main index for access restrictions, retention policies, or search purposes. See Create custom indexes in the Splunk Enterprise *Managing Indexers and Clusters of Indexers* manual.

The worker set drop-down menu is specific to adaptive response actions on a Splunk Cloud Platform ES search head. See Set up an adaptive response relay from a Splunk Cloud Platform Enterprise Security search head to an on-premises device in the *Administer Splunk Enterprise Security* manual.

## Add threat intelligence

Create threat artifacts in a threat collection.

1. Click **Add New Response Action** and select **Add Threat Intelligence**.
2. Select the **Threat Group** to attribute this artifact to.
3. Select the **Threat Collection** to insert the threat artifact into.
4. Type the **Search Field** that contains the value to insert into the threat artifact.
5. Type a **Description** for the threat artifact.
6. Type a **Weight** associated with the threat list. Defaults to 1.
7. Type a number of **Max Results** to specify the number of results to process as threat artifacts. Each unique search field value counts as a result. Defaults to 100.