Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Set up Adaptive Response actions in Splunk Enterprise Security

Generated: 6/13/2022 9:54 am

Set up Adaptive Response actions in Splunk Enterprise Security

Adaptive Response actions allow you to gather information or take other action in response to the results of a correlation search or the details of a notable event. Splunk Enterprise Security includes several Adaptive Response actions. See Included Adaptive Response actions.

You can add Adaptive Response actions and alert actions to correlation searches, or run Adaptive Response actions from notable events on the Incident Review dashboard. Collect information before you start your investigation to save time at triage by adding Adaptive Response actions to correlation searches. Take action at triage time by running Adaptive Response actions from the Incident Review dashboard.

The Adaptive Response actions that ship out of the box for ping, nbtstat, and nslookup are modified to support Splunk Cloud Platform. Additional setup is required before configuring Adaptive Response actions from Splunk Cloud Platform to on-premises infrastructure and services. See Set up an Adaptive Response relay from Splunk Cloud Platform to an on-premises device.

Add new Adaptive Response actions

To add new Adaptive Response actions, you can install add-ons with Adaptive Response actions or create your own Adaptive Response actions. See Create an Adaptive Response action on the Splunk developer portal for information on creating Adaptive Response actions. See Deploy add-ons included with Splunk Enterprise Security in the *Install and Upgrade Manual*.

Audit Adaptive Response actions

Audit all Adaptive Response actions on the Adaptive Response Action Center.

Configure permissions for Adaptive Response actions

Restrict certain Adaptive Response actions to certain roles by adjusting the permissions for Adaptive Response actions in the alert actions manager. You can find information about the alert actions manager in the Splunk platform documentation.

- For Splunk Enterprise, see Using the alert actions manager in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud Platform, see Using the alert actions manager in the Splunk Cloud Platform *Alerting Manual*.

In order to run Adaptive Response actions from the Incident Review dashboard that have credentials stored in the credential manager, you must have the appropriate capability.

- For Splunk platform version 6.5.0 and later, `list_storage_passwords`.
- For earlier Splunk platform versions, `admin_all_objects`.

Add an Adaptive Response action to a correlation search

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 the response action you want to add.
4. Complete the fields for the action. If you want, add another response action.
5. Click **Save** to save all changes to the correlation search.

For instructions on configuring each of the Adaptive Response actions included with Splunk Enterprise Security, see Configure Adaptive Response actions for a correlation search in Splunk Enterprise Security. For instructions on configuring a custom Adaptive Response action, see the documentation for the app or add-on that supplied the Adaptive Responsee action.

Troubleshoot why an Adaptive Response action is not available to select

If an Adaptive Response action is not available to select on the correlation search editor or Incident Review, several things could be the cause.

- Your role may not have permissions to view and use the Adaptive Response action. See Using the alert actions manager in the *Alerting Manual*.
- Check the alert actions manager to determine if the Adaptive Response actions exist in Splunk platform. See Using the alert actions manager in the *Alerting Manual*.
- If the Adaptive Response actions from an add-on do not appear in Splunk Enterprise Security, but do appear in the alert actions manager, make sure that the add-on is being exported globally. See Make Splunk knowledge objects globally available in the Splunk Enterprise *Admin Manual*.
- If you can select the Adaptive Response action on the correlation search editor, but not on Incident Review, the Adaptive Response action might be an ordinary alert action, or the response action does not support ad hoc invocation. See Determine whether your action supports ad hoc invocation on the Splunk developer portal.