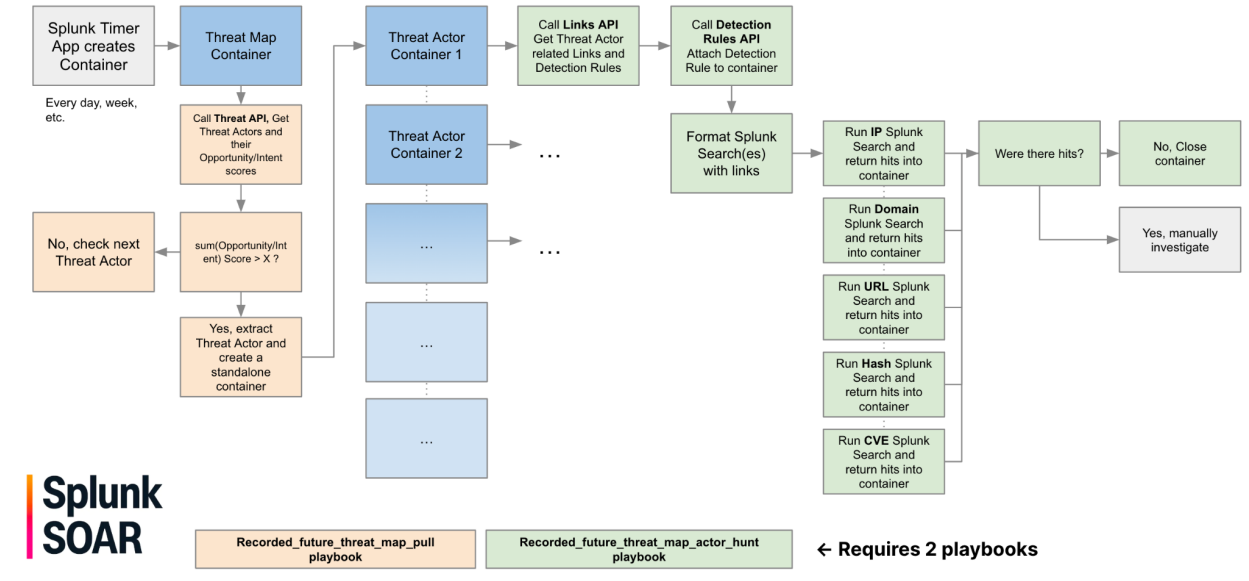
Splunk SOAR: Automated Hunting with Recorded Future Threat Maps

Created by: *Recorded Future Professional Services*

This document will instruct setting up and configuring Splunk SOAR to run automatic threat hunts based on Recorded Future's threat maps with Splunk SIEM.

Dataflow



This workflow will begin by having the Splunk SOAR timer app create an empty Splunk SOAR container and apply a label. The applied label will automatically run **recorded_future_threat_map_pull** which will query the Recorded Future Threat Map and return a list of Threat Actors. Threat Actors with an intent or opportunity score greater than 90 will be extracted and used to create a new Splunk SOAR container.

Each new Splunk SOAR container will call **recorded_future_threat_map_actor_hunt** which will query Recorded Future for Links relating to the threat actor, format a Splunk search query with IP, Domain, URL, Hash, and Vulnerability IoCs, and run a Splunk search to look for any hits. Any Sigma, YARA, or Snort rules associated with the threat actor will also be downloaded and attached to the Splunk SOAR container.

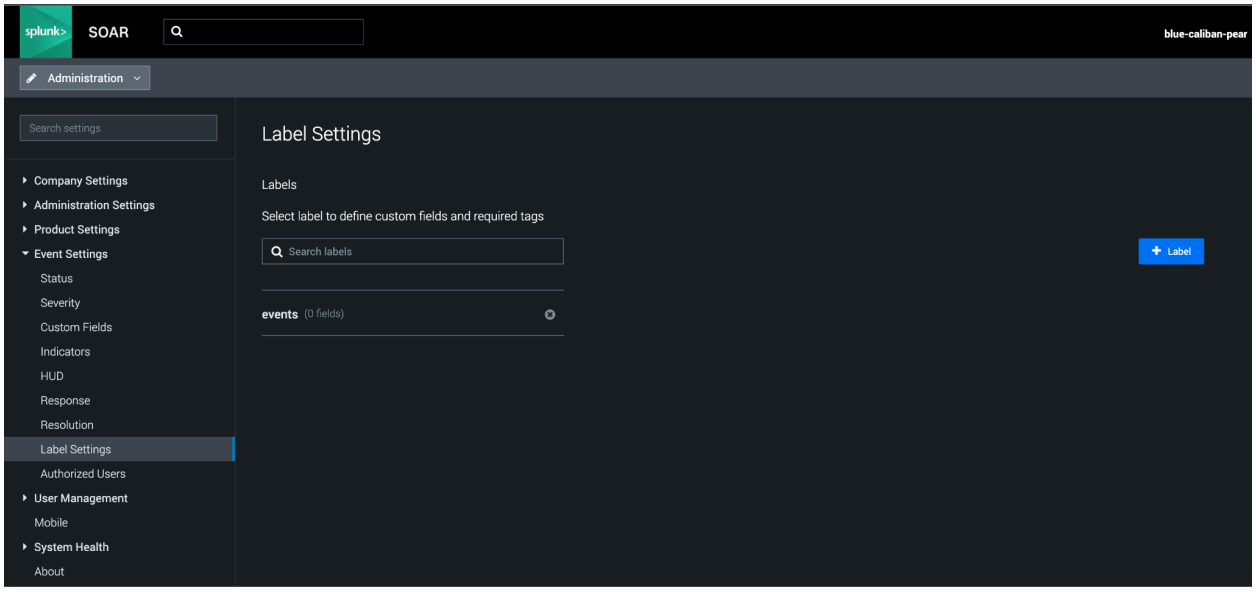
Downloads

Playbooks are available on the Recorded Future support site.

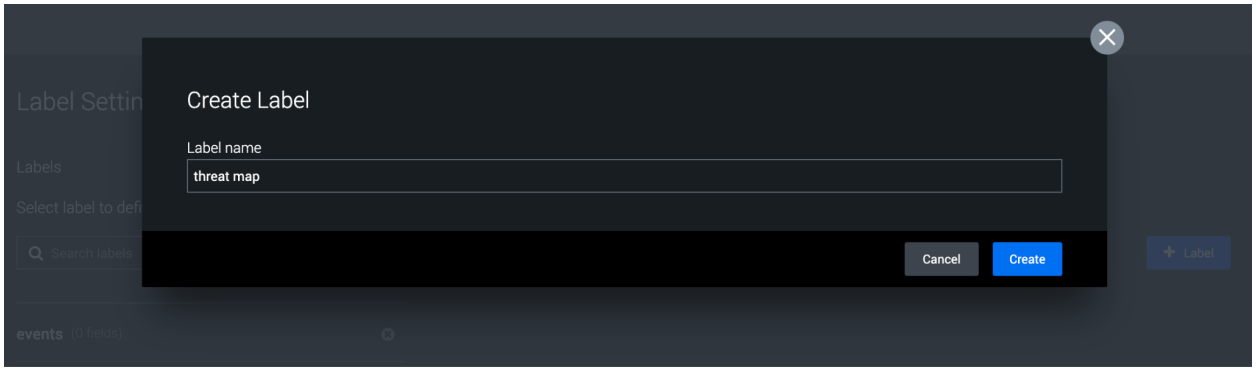
Configuration Instructions

This playbook requires configuring a Timer app to create and apply labels to a container which will automatically run the Threat Actor Hunting playbook on a scheduled basis. The following instructions will detail this process.

1. Navigate to Administration → Event Settings → Label Settings → and click + Label.

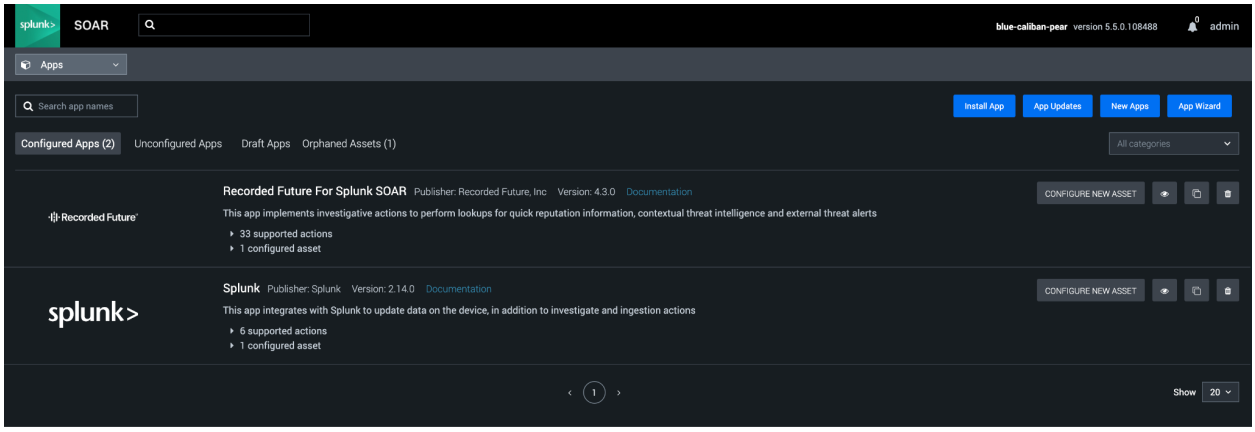


2. Name the label threat map or a name of your own preference. This label will be applied to the container that will pull the Recorded Future threat map. Click create.

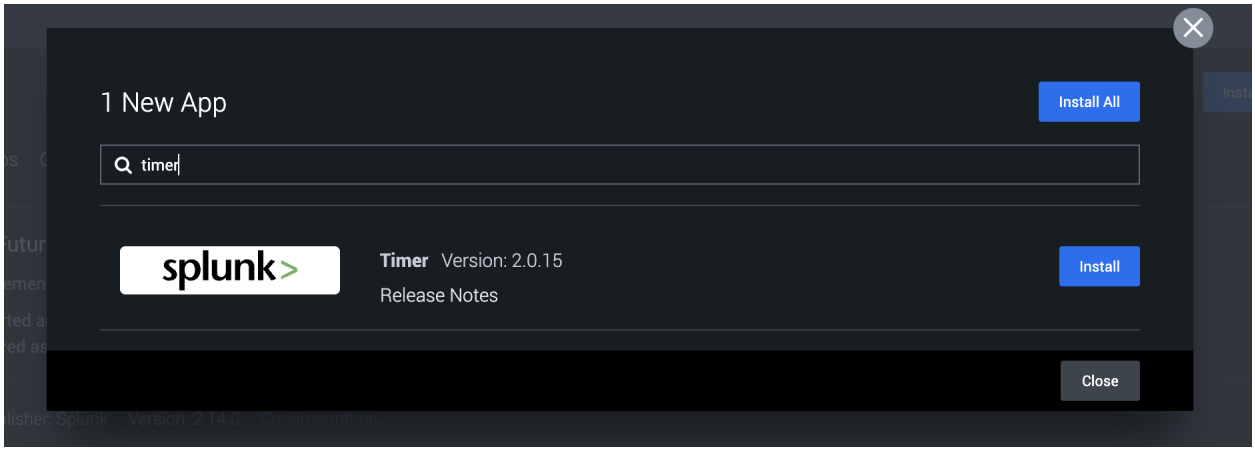


3. Do the same for another label called **threat actor**.

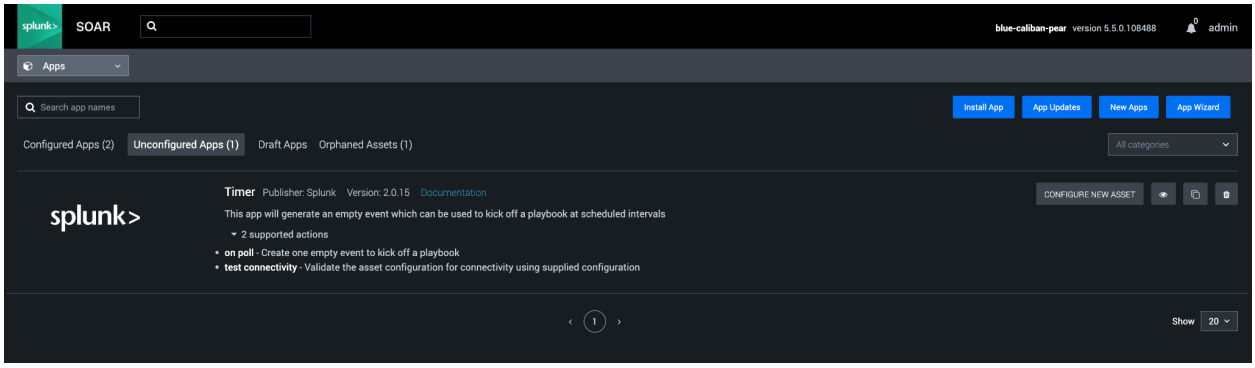
4. Navigate to apps and click New Apps. If you already have the Timer app installed you can skip this and step 5.



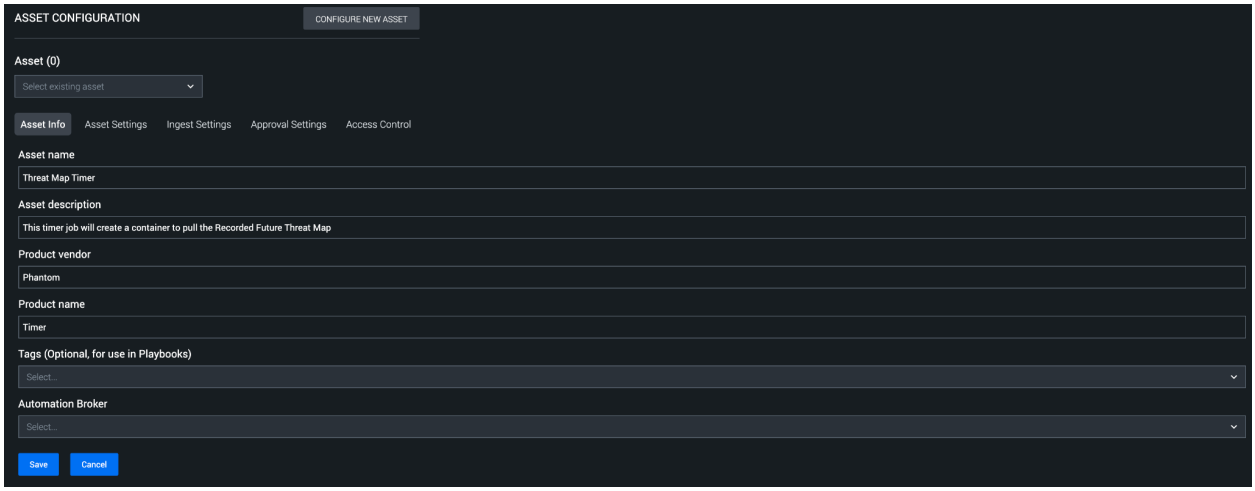
5. Search for Timer and click install.



6. Navigate to Apps → Unconfigured Apps and click Configure New Asset for the Timer app.



7. Under Asset Info, give the asset a name and a description.



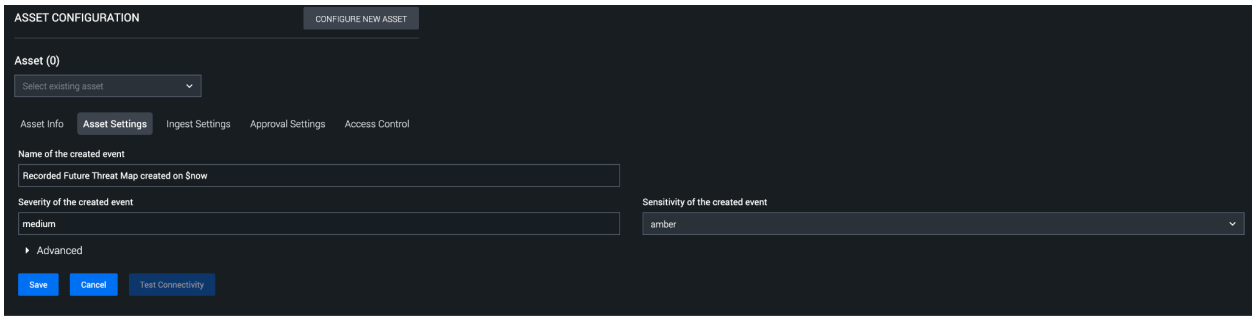
8. Under Asset Settings, set the Name of the created event to Recorded Future Threat Map created on $now.

   The Name of the created event configuration option will be used as the name of each newly created event. Optionally, there are two possible values that you can put into this in order to have dynamic names.

   - $label
   - $now

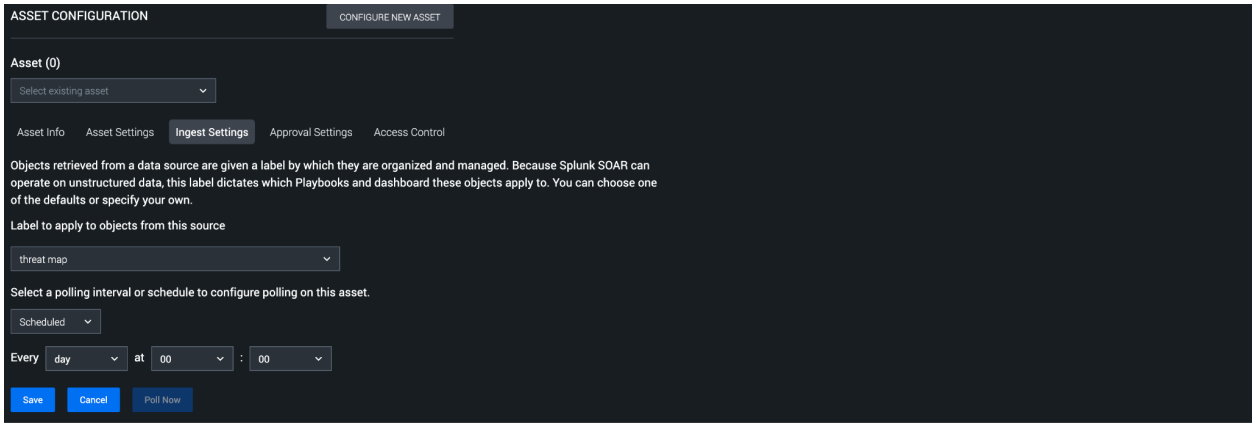
   These will be appropriately substituted. For example, if you set **Named of the created event** to "$label event, created on $now", then a created event could have the name "Email event, created on 2023-06-21T20:02:56.139008+00:00". This timestamp will always be in UTC.

   Set the Severity of the created event and Sensitivity of the created event to your preference.



9. Under ingest settings, set the Label to apply to objects from this source to the label you created earlier threat map and set the polling interval to scheduled at

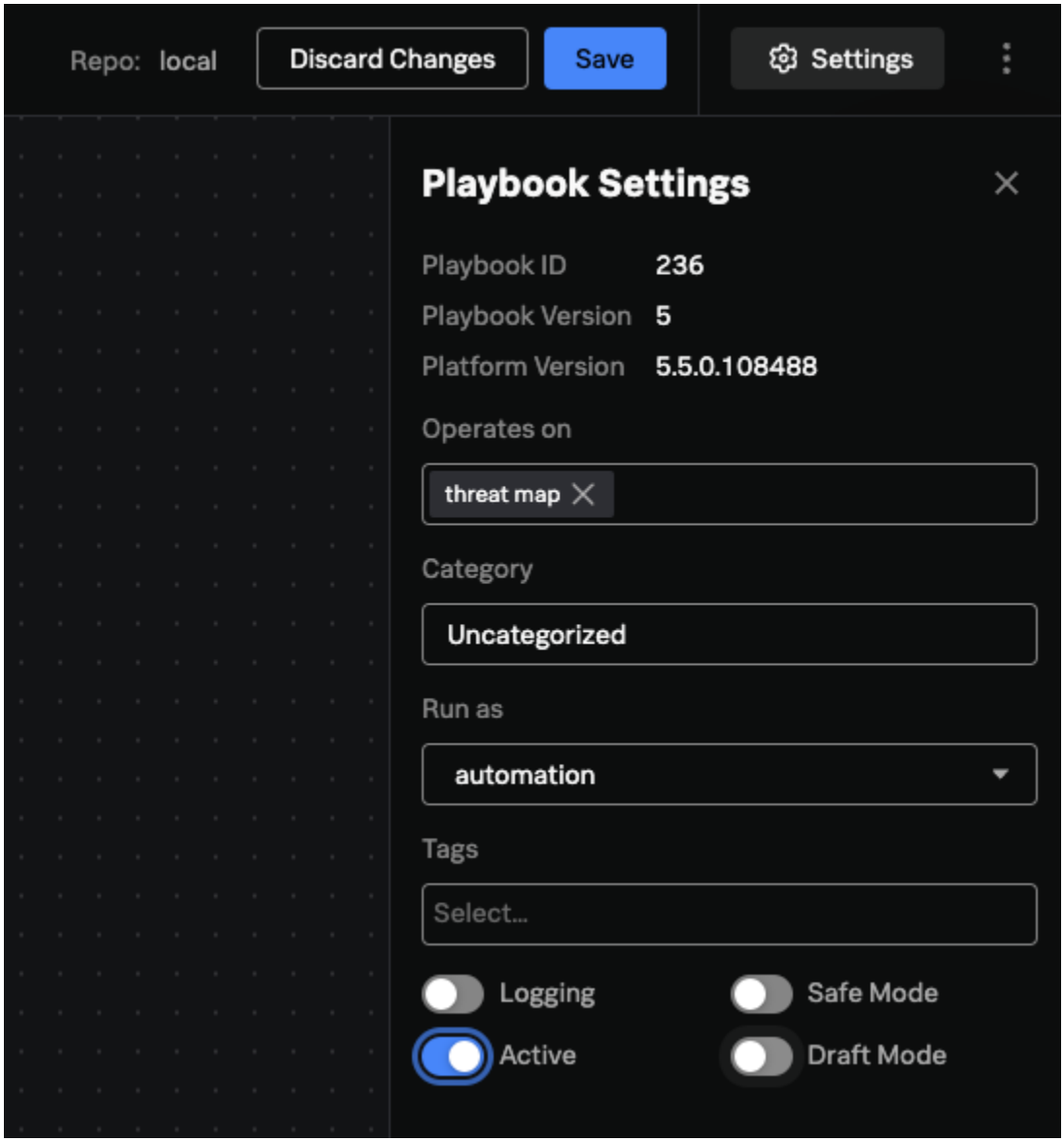
every day or your preference.



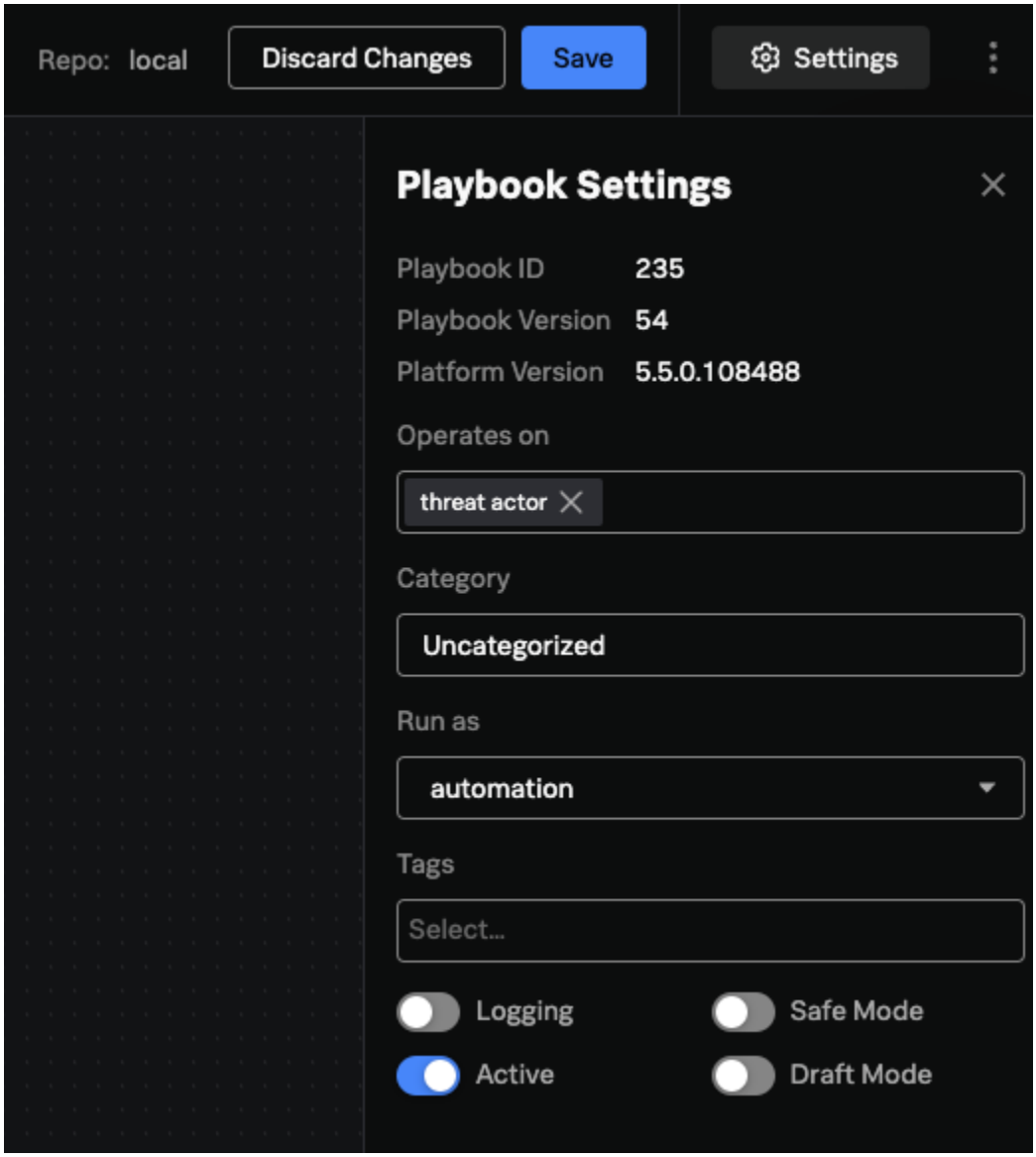
Playbook Instructions

1. Download the playbooks from Recorded Future's support site: https://support.recordedfuture.com/hc/en-us/articles/12294483605523-Splunk-SOAR-Template-Playbooks-Library

2. Import the recorded_future_threat_map_pull playbook. Within it, enable it to operate on threat map labels and turn it Active:



3. Import the recorded_future_threat_map_actor_hunt playbook. Within it, enable it to operate on threat map labels and turn it Active.



4. Your playbooks will now run and automatically generate events.