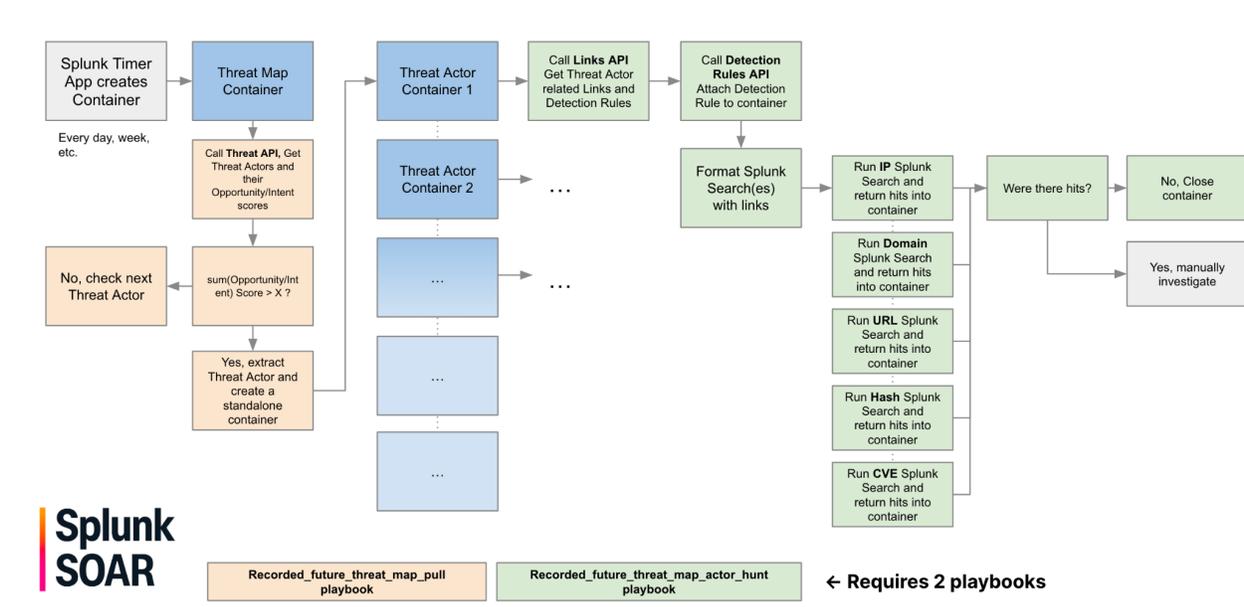


# Splunk SOAR: Automated Hunting with Recorded Future Threat Maps

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.

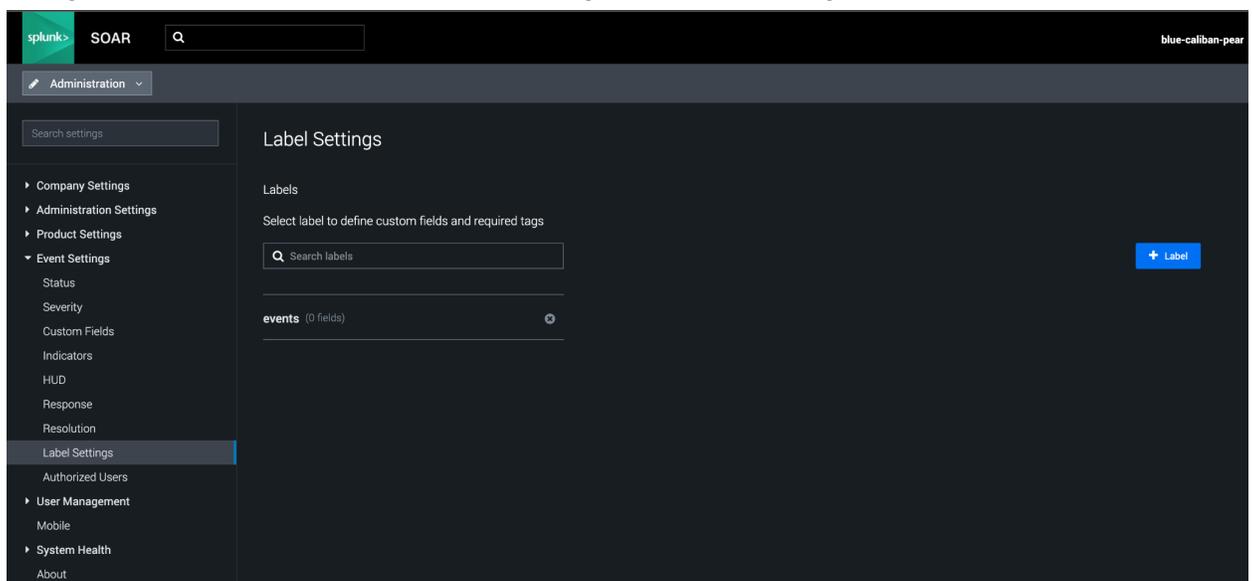
# Downloads

Playbooks are [available](#) on the Recorded Future support site.

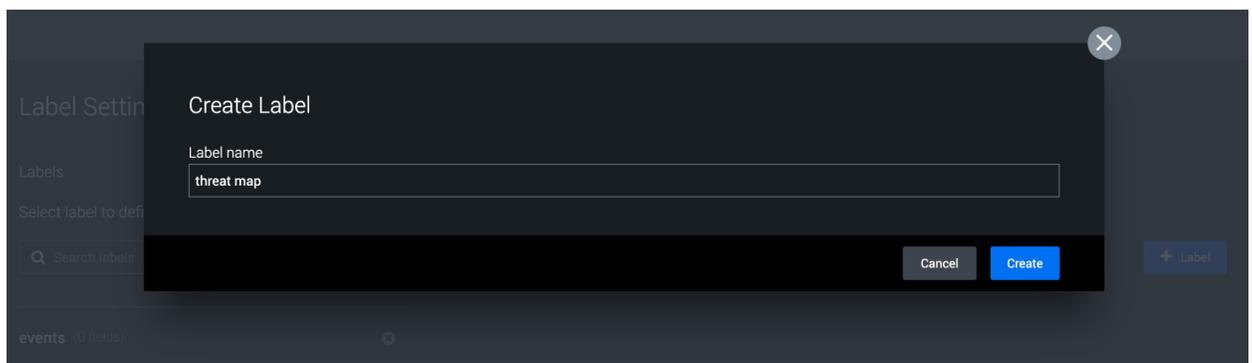
## Configuration Instructions

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.

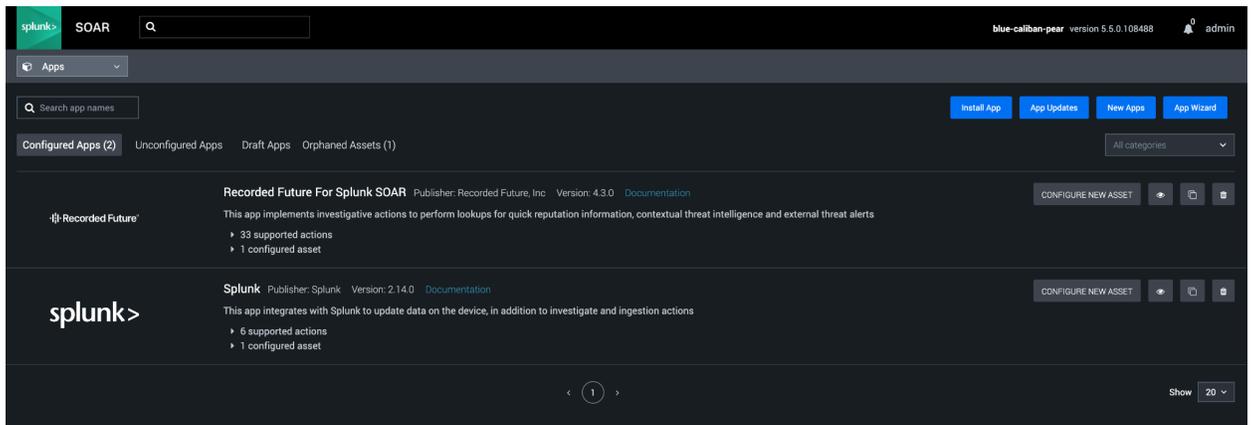


2. Name the label threat map or a name of your own preference. This label will be applied to the container that will pull the Recorded Future threat map. Click create.

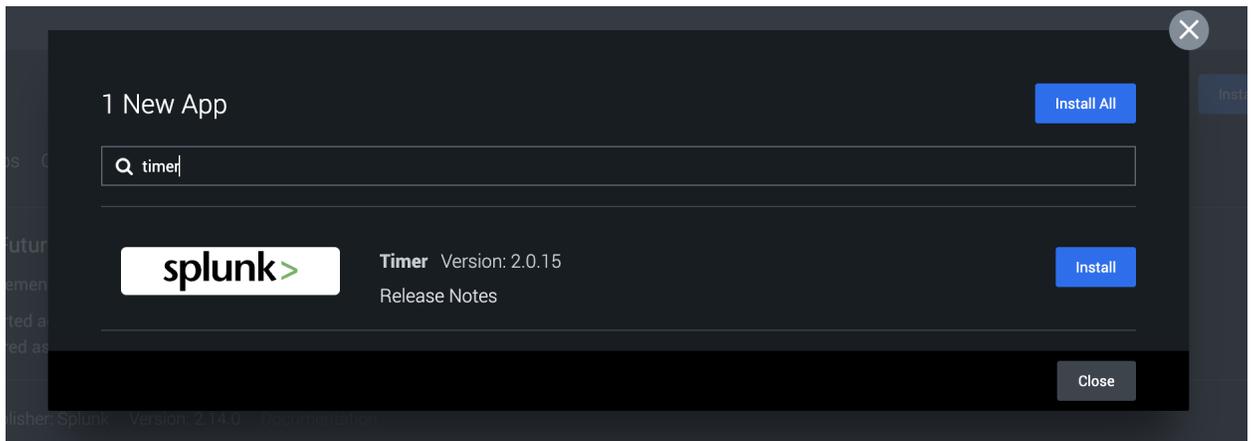


3. Do the same for another label called **threat actor**.

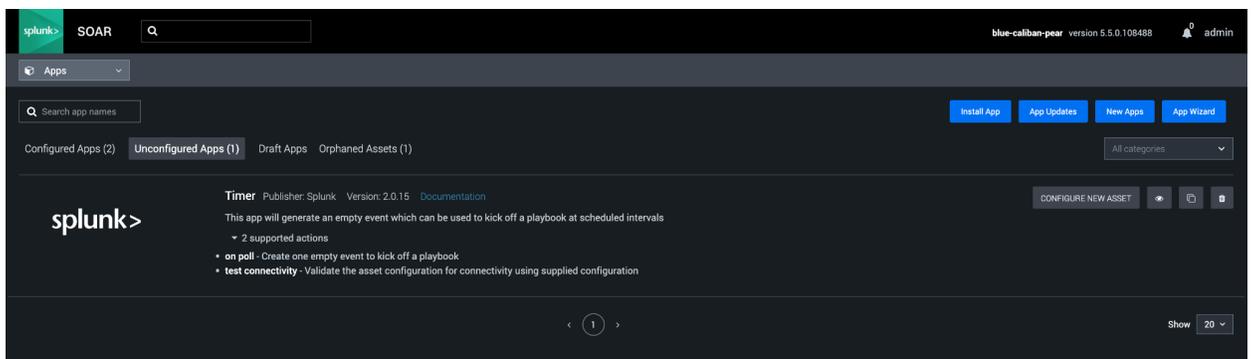
4. Navigate to apps and click New Apps. If you already have the Timer app installed you can skip this and step 5.



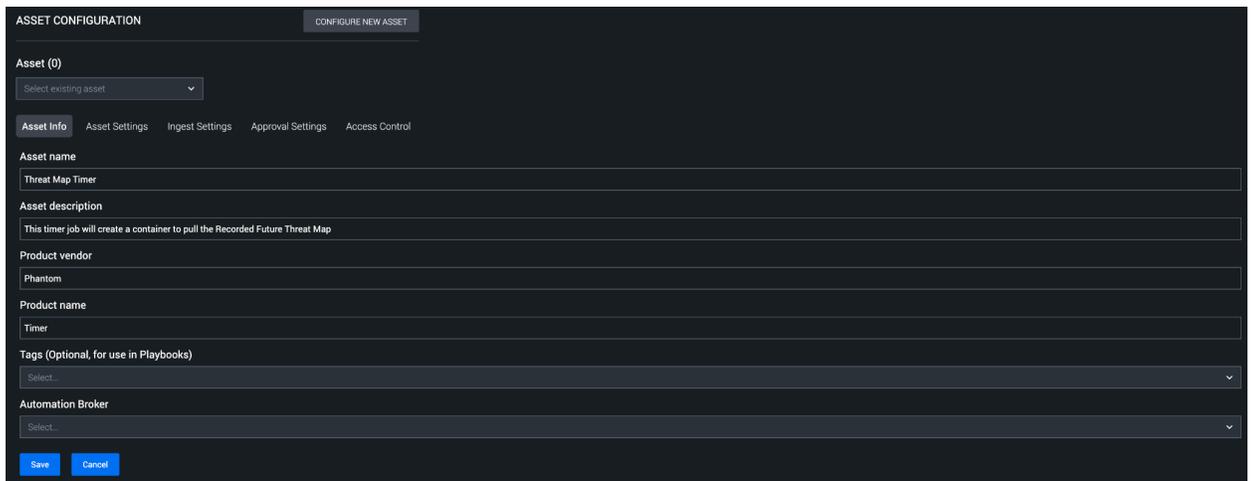
5. Search for Timer and click install.



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



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



The screenshot shows the 'ASSET CONFIGURATION' interface with the 'CONFIGURE NEW ASSET' button. The 'Asset (0)' dropdown is set to 'Select existing asset'. The 'Asset Info' tab is active, showing fields for 'Asset name' (containing 'Threat Map Timer'), 'Asset description' (containing 'This timer job will create a container to pull the Recorded Future Threat Map'), 'Product vendor' (containing 'Phantom'), 'Product name' (containing 'Timer'), 'Tags (Optional, for use in Playbooks)' (set to 'Select...'), and 'Automation Broker' (set to 'Select...'). 'Save' and 'Cancel' buttons are at the bottom.

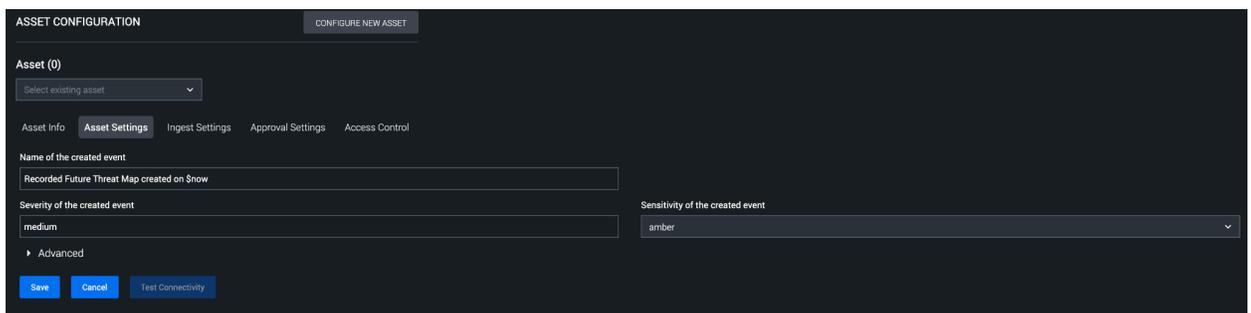
- Under Asset Settings, set the Name of the created event to Recorded Future Threat Map created on \$now.

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.



The screenshot shows the 'ASSET CONFIGURATION' interface with the 'CONFIGURE NEW ASSET' button. The 'Asset (0)' dropdown is set to 'Select existing asset'. The 'Asset Settings' tab is active, showing fields for 'Name of the created event' (containing 'Recorded Future Threat Map created on \$now'), 'Severity of the created event' (set to 'medium'), and 'Sensitivity of the created event' (set to 'amber'). There is also an 'Advanced' section with a right-pointing arrow. 'Save', 'Cancel', and 'Test Connectivity' buttons are at the bottom.

- 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.

The screenshot shows the 'ASSET CONFIGURATION' interface with a 'CONFIGURE NEW ASSET' button. Under 'Asset (0)', there is a dropdown menu for 'Select existing asset'. Below this are tabs for 'Asset Info', 'Asset Settings', 'Ingest Settings' (which is active), 'Approval Settings', and 'Access Control'. A paragraph explains that objects are given a label for organization and management, and that this label affects which playbooks and dashboards apply. Below this is a section 'Label to apply to objects from this source' with a dropdown menu set to 'threat map'. Another section 'Select a polling interval or schedule to configure polling on this asset.' has a dropdown set to 'Scheduled'. At the bottom, there is a scheduling field: 'Every' followed by a dropdown 'day', 'at' followed by a dropdown '00', a colon, and another dropdown '00'. At the very bottom are three buttons: 'Save', 'Cancel', and 'Poll Now'.

## 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:

The screenshot shows the 'Playbook Settings' dialog for a playbook. At the top, there are buttons for 'Repo: local', 'Discard Changes', 'Save', and 'Settings'. The main content area is divided into sections: 'Playbook ID' (236), 'Playbook Version' (5), and 'Platform Version' (5.5.0.108488). The 'Operates on' section has a text input field containing 'threat map'. The 'Category' section has a text input field containing 'Uncategorized'. The 'Run as' section has a dropdown menu set to 'automation'. The 'Tags' section has a text input field containing 'Select...'. At the bottom, there are four toggle switches: 'Logging' (off), 'Active' (on), 'Safe Mode' (off), and 'Draft Mode' (off).

Repo: local   Discard Changes   Save   Settings

### Playbook Settings

Playbook ID   236  
Playbook Version   5  
Platform Version   5.5.0.108488

Operates on  
threat map

Category  
Uncategorized

Run as  
automation

Tags  
Select...

Logging    Safe Mode  
 Active    Draft Mode

3. Import the recorded\_future\_threat\_map\_actor\_hunt playbook. Within it, enable it to operate on threat map labels and turn it Active.

The screenshot shows a dark-themed interface for editing a playbook. At the top, there are buttons for 'Repo: local', 'Discard Changes', 'Save', and 'Settings'. The main content area is titled 'Playbook Settings' and contains the following information:

- Playbook ID: 235
- Playbook Version: 54
- Platform Version: 5.5.0.108488
- Operates on: threat actor (with a close icon)
- Category: Uncategorized
- Run as: automation (dropdown menu)
- Tags: Select...
- Logging:
- Active:
- Safe Mode:
- Draft Mode:

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

The screenshot displays the Splunk SOAR interface for an investigation titled "BlueBravo". The interface is divided into several sections:

- HUD (Header User Dashboard):** Contains four red boxes representing different types of hits:
  - Domain Hits:** ["avsvmcloud.com"]
  - IP Hits:** ["141.255.164.11", "198.252.107.14", "79.124.60.173", "193.36.119..."]
  - Vulnerability Hits:** ["CVE-2021-27065", "CVE-2021-26855", "CVE-2020-14882", "CVE-2019-7..."]
  - Hash Hits:** ["b422ba73f389a6e5ef9411cf4484c840c7c82f2731c6324b5b24be6f8c08477d"]
- EVENT INFO:** A navigation bar with tabs for Activity, Workbook, and Guidance. It also includes a Timeline, Artifacts, Evidence, Files, Approvals, and Reports section.
- Recent Activity:** A list of automation tasks performed on "Sun at 12:00 am", including "recorded\_future\_threat\_map\_a...", "threat\_actor\_intelligence\_1", "detection\_rule\_search\_1", and various "search\_splunk\_for\_" tasks.
- ARTIFACTS (1):** A table showing one artifact with ID 5469, labeled "threat\_actor", named "threat\_actor", with a severity of "HIGH".
- Widgets:** A section containing a "Recorded Future" widget. This widget displays a list of IP intelligence items (e.g., "141.255.164.11 [recorded future qa]") and a detailed view for the IP "141.255.164.11". The detailed view shows a Risk Score of 95, 8 of 71 Risk Rules triggered, and an Intelligence Card status of "Open".