Recorded Future®

SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Automated Hunting with Recorded Future Threat Maps

Use Case

The Threat Actor threat map provides a structured, repeatable method of identifying and prioritizing threat actors relevant to your enterprise and plotting them based on their values for potential intent and estimated opportunity. These threat actors are often associated with indicator links which can be used to hunt for activity in your environment.

Issue

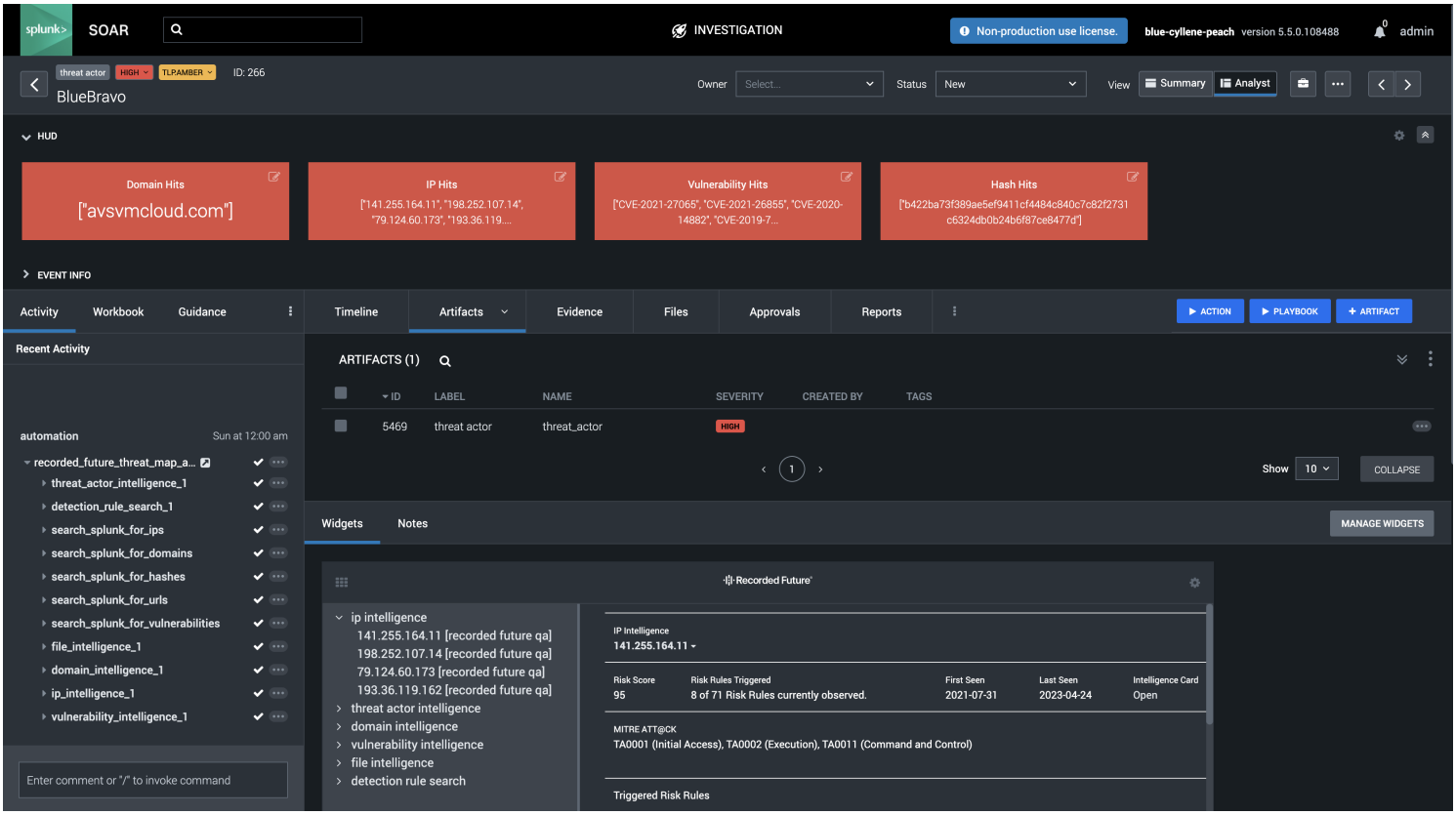
With a shortage of resources, most security teams face challenges justifying the time involved with proactive threat hunting. Oftentimes, a single threat actor may have dozens of indicators linked to them. Strained for resources, it can be time consuming running dozens of Splunk searches manually.

Solution

With two playbooks, you can automatically hunt for threat actor activity using Recorded Future's threat map in combination with Splunk SOAR and Splunk SIEM.

The first playbook is designed to ingest the Recorded Future threat map into Splunk SOAR. An event will populate and store the entire Threat Map. Then individual events will be created for each threat actor whose opportunity or intent score satisfies a threshold for hunting. These events will trigger the second playbook.

The second playbook will enrich each Threat Actor with technical links and then format the links into Splunk search queries to run across your Splunk instance. Results will be fetched and returned to Splunk SOAR. If available, YARA, Sigma, and Snort detection rules will download and attach to the vault.



Technical

From a technical perspective the integration will need the following configured:

- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**
- The Splunk app for Splunk SOAR app installed and configured **https://splunkbase.splunk.com/app/5848**
- The Timer app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/5940**
- 2 Playbooks downloaded and configured: **recorded_future_threat_map_pull** and **recorded_future_threat_map_actor_hunt**

This service will require the SecOps or Threat Intelligence Module, the Vulnerability Intelligence Module (for hunting vulnerabilities) and the Splunk SOAR Integration. The playbooks are available on the Recorded Future support site.