Recorded Future®

SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Recorded Future Phishing Email Sandbox Detonation

Use Case

Phishing emails are often reported by end users in organizations for security analysts to investigate. These emails tend to report to a designated email inbox, often within Exchange. These emails will at times include attachments and URLs which are dangerous to visit or investigate manually. The Recorded Future Sandbox allows analysts to submit these files and URLs for analysis.

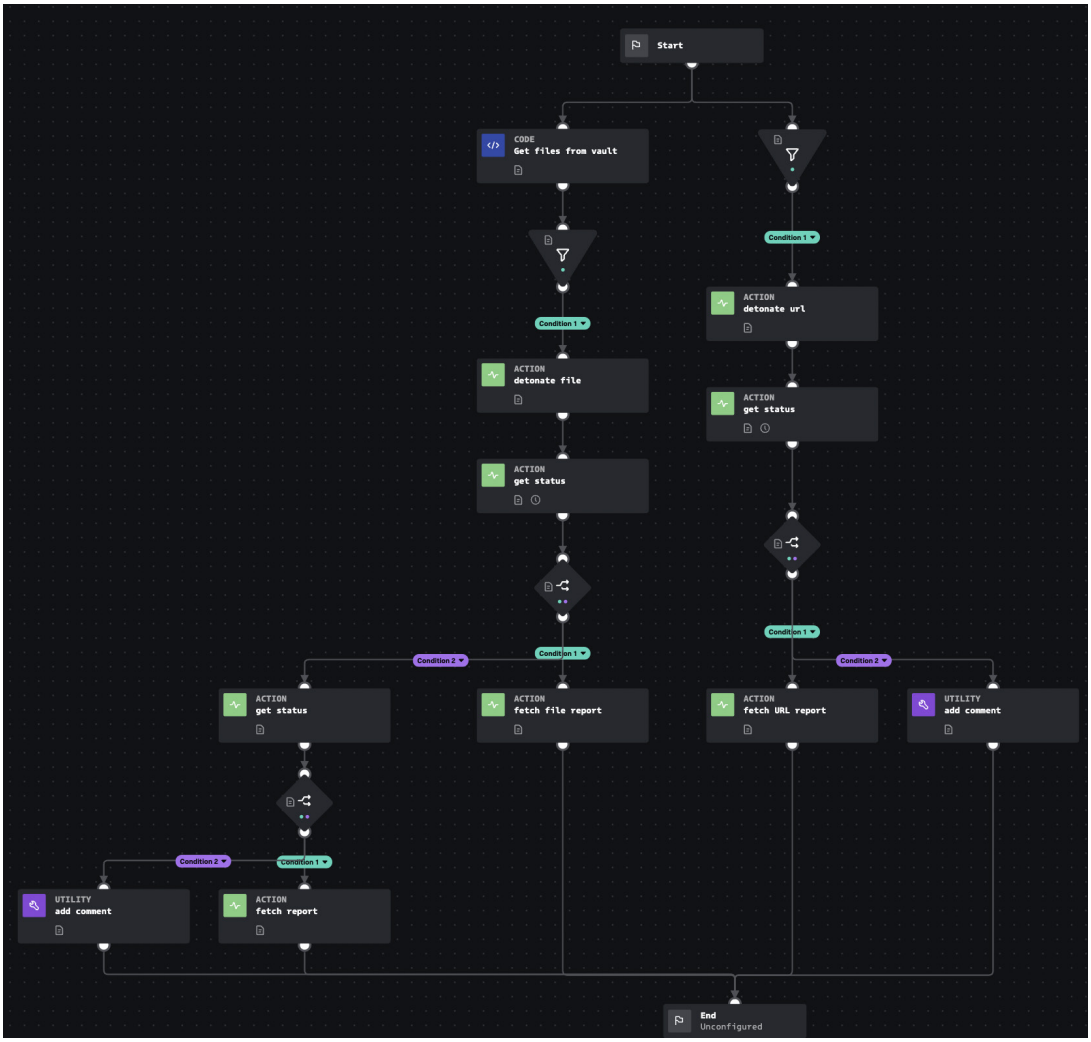
Issue

Manually submitting a handful of file submissions per day doesn't pose a problem, but as the threshold of files needed to investigate rises, this process can consume hours of analyst cycle time per day. Keeping up with phishing email submissions can be a tedious, mundane, and manual task. Often, these submissions are ignored although they can contain critical warnings to an incoming breach.

Solution

By utilizing the poll capability with the Exchange for EWS app within Splunk, phishing emails can be automatically ingested into Splunk SOAR and converted into artifacts including email headers, bodies, and files attachments. This playbook responds to these incoming emails.

The playbooks extracts any files that are added from the phishing email to the vault and uploads them to the Recorded Future Sandbox API for analysis. After waiting for the submission report to complete, all results are returned to the Splunk SOAR container. The same is accomplished for any URLs referenced in the phishing email. These results can be used to determine the maliciousness of the email and passed into further automations such as mass searches throughout the organization for similar emails, blocking related URLs and IP addresses from end users systems, or starting endpoint scans or quarantines.



Technical

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

- EWS for Office 365 installed and configured on Splunk SOAR **https://splunkbase.splunk.com/app/5829**
- Recorded Future Sandbox app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6637**

This service will require the Recorded Future SecOps or TI Intelligence Module and the Recorded Future Splunk SOAR Integration. The playbook will be included with the Recorded Future Sandbox App on the Splunk SOAR marketplace.