SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Recorded Future Typosquat Handling Playbook

Use Case

Typosquatting is when a third-party registers a domain deliberately similar to another domain. The third-party may be a malicious actor who is using the technique to fool employees, customers, or partners of the organization that owns the domain, in order to steal passwords and hijack accounts, infect visitor's computers with malware, etc.

Recorded Future's Typosquat alerts inform companies when their domain is being used in the above scenario and provides the first step of taking action.

Issue

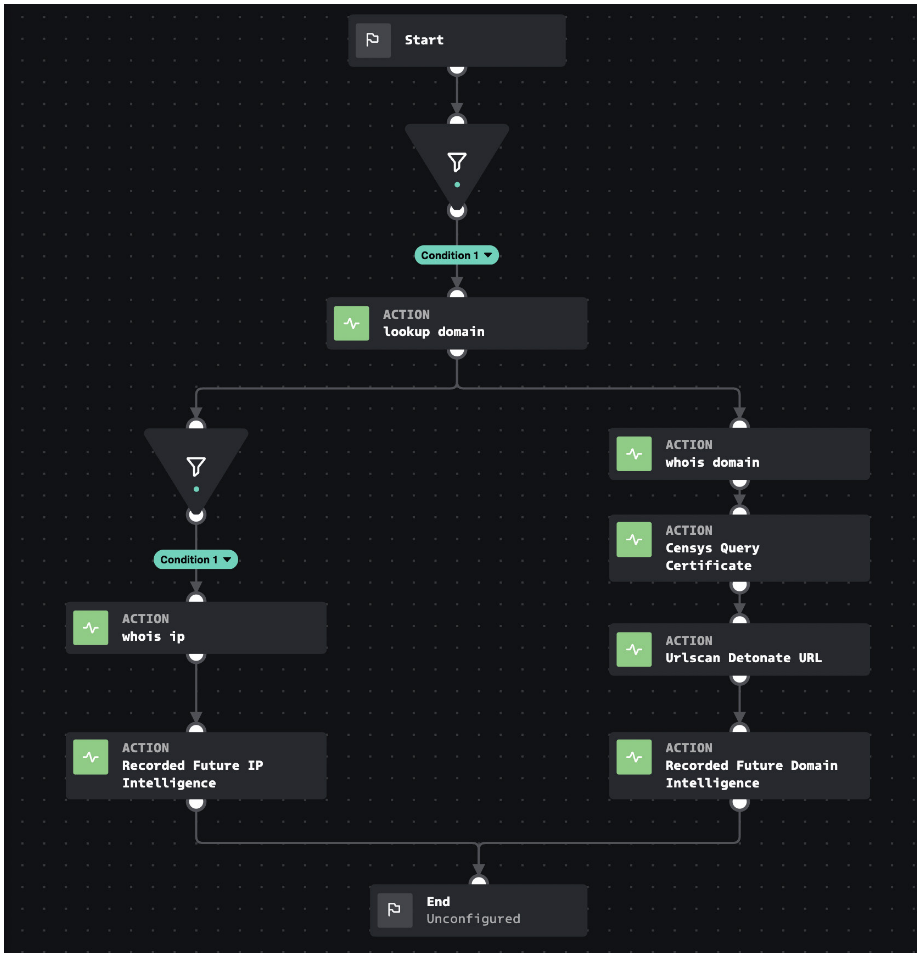
The typical course of actions required when responding to a typosquat alert include several enrichment steps, some of which are done within Recorded Future, others with outside resources:

- DNS lookups
- IP lookups
- Domain references
- Query certificates

Solution

This playbook responds to Recorded Future Typosquat detection alerts. The domain is first passed through a simple DNS lookup. Any returned IP addresses are passed into a Recorded Future IP enrichment action and a whois search. The domain is then passed into an additional whois search, a Censys certificate query, a URL detonation with urlscan, and a Recorded Future domain enrichment action.

All enrichment data is returned into the Splunk SOAR container. This JSON data can then be queried against internal white-listed IP addresses, domains, and known certificate registration information to verify if the domain needs to be taken action against.



Technical

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

- The LDAP app installed with read/write permissions (delegated permissions for password resets are recommended) from Splunk SOAR **https://splunkbase.splunk.com/app/5908**
- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**

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