Threat Hunting Dashboard

Use Case
Recorded Future's Insikt Group tracks and profiles hundreds of the top threat actors on an ongoing basis to discover new indicators, targets, and attack patterns. This dataset contains hashes, IP addresses, domains, and URLs that have been reported by Insikt Group cumulatively over time. Each indicator is mapped back to a report, so if there is a hit in your environment you will be able to compare it directly with the source data to see if there is sufficient evidence to indicate an attack by a certain threat actor. The recommended use for this data is to add these indicators to your threat hunting solution in your SIEM, network, or endpoint tools to correlate indicators against live and historical telemetry data.

Issue
- Correlating information from multiple IOC types to investigate and determine whether your network has been compromised by a specific threat actor
- Lack of context and curation around malicious indicators

Solution
Recorded Future Professional Services offers an enhanced capability using the hunt packages dataset that allows you to choose a threat actor hunt package and field from your logs to correlate against. Any matches will include the relevant Insikt Note Name, giving you greater context around hits in your network and potential compromises.
Technical

From a technical perspective the integration will include and need configured:

- Threat Hunting Dashboard XML Code
- Hunt package fusion files of interest added to your Splunk instance as lookup table files

This service will require the SecOps Module, Splunk Integration, and Two (2) Professional Service Credits for implementation. On-going support covered by Integration or Premium Support.