PROFESSIONAL SERVICES SOLUTION

Threat Hunting Dashboard

Use Case

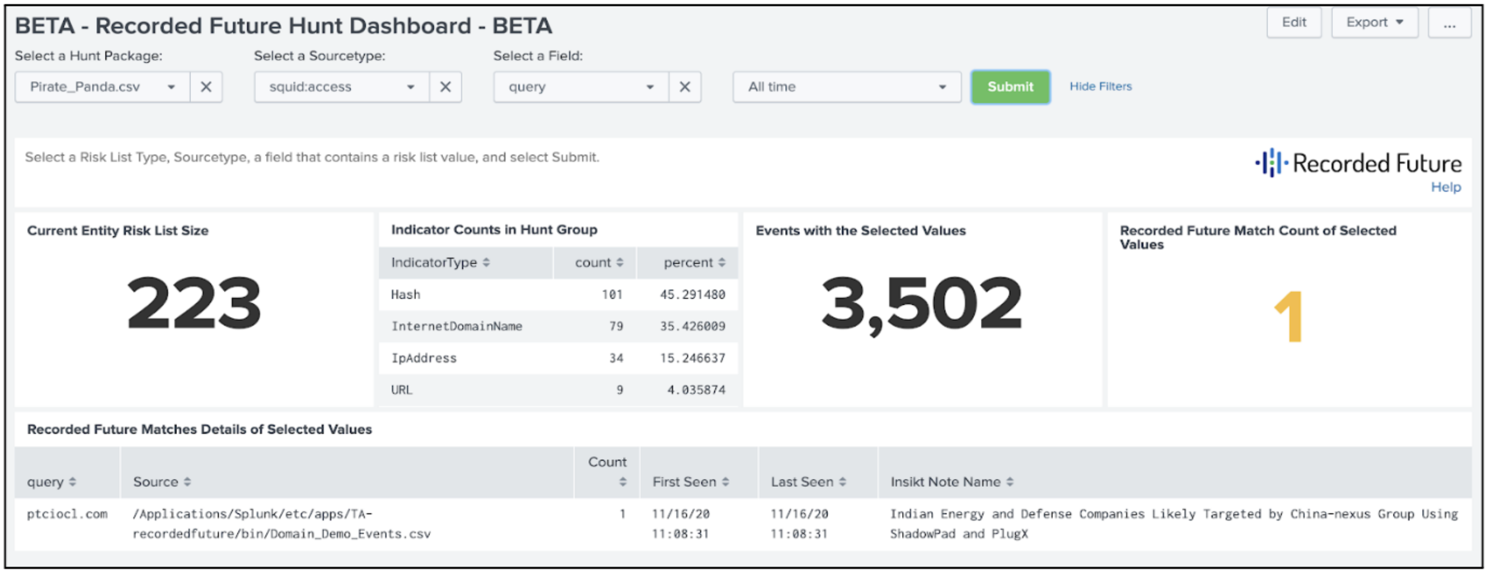
Recorded Future's Insikt Group tracks and profiles hundreds of the top threat actors on an ongoing basis to discover new indicators, targets, and attack patterns. This dataset contains hashes, IP addresses, domains, and URLs that have been reported by Insikt Group cumulatively over time. Each indicator 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.



BETA - Recorded Future Hunt Dashboard - BETA

Select a Hunt Package: Pirate_Panda.csv

Select a Sourcetype: squid:access

Select a Field: query

All time

Select a Risk List Type, Sourcetype, a field that contains a risk list value, and select Submit.

Current Entity Risk List Size: 223

Indicator Counts in Hunt Group

IndicatorType	count	percent
Hash	101	45.291480
InternetDomainName	79	35.426009
IpAddress	34	15.246637
URL	9	4.035874

Events with the Selected Values: 3,502

Recorded Future Match Count of Selected Values: 1

Recorded Future Matches Details of Selected Values

query	Source	Count	First Seen	Last Seen	Insikt Note Name
ptciocl.com	/Applications/Splunk/etc/apps/TA-recordedfuture/bin/Domain_Demo_Events.csv	1	11/16/20 11:08:31	11/16/20 11:08:31	Indian Energy and Defense Companies Likely Targeted by China-nexus Group Using ShadowPad and PlugX

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.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture