Optiv Threat Intel

Splunk App

Author: Derek Arnold

Version Number: 3.20

Date: 12.4.2016

Overview

Optiv Threat Intel is a Splunk App that automatically correlates your data with several popular open threat lists. After a few mouse clicks we can start hunting for log sources that are beaconing out or being attacked by known bad IP ranges. The app can provide increased visibility to potentially malicious activity going on in the organization.

Features:

- Threat list visualization feature that shows where most of the attackers are located on a globe.
- Easily choose indexes, sourcetypes, or hosts for log entries that match threat list destination IPs.
- IP search feature that displays threat list activity.
- RSS feed which will poll several information security news sites and consolidate the stories on one page.
- Updated information is pulled down from the web every 8 hours.
- Threat list visualization that shows where most of the attackers are located on a globe.

- Easily choose indexes, sourcetypes, or hosts for log entries that match threat list destination IPs, URLs and domains.
- Email alerting feature to notify you of a threat list match that is correlated against your organization's machine data.
- IP search feature that displays threat list activity.
- Domain search feature that displays threat list activity.

This document serves as a guide to both the Optiv_TA_threat app as well as the Optiv Threat Intel app, as they go hand-in-hand.

Optiv Threat Intel is the app, installed on the search head(s), which visualizes the data collected. Optiv_TA_threat is the threat list collection engine which is installed on a forwarder server that makes the web requests. Both apps are to be installed on only one node in a Splunk environment. There is no need to install multiple copies anywhere.

Splunk Role Matrix:

Role	App to install
Search heads	Optiv Threat Intel
Indexers	N/A
Heavy or Universal Forwarder	Optiv_TA_threat
Other Splunk roles	N/A

For a distributed environment that does not contain heavy or universal forwarders, installing Optiv_TA_threat on the search head is acceptable.

Optiv Threat Intel Application characteristics:

Characteristic	
Has index-time operations	False
Must be installed on indexers*	False
Create an index	True
Implements summarization	True

Optiv_TA_threat Application characteristics:

Characteristic	
Has index-time operations	True
Must be installed on indexers*	False
Create an index	True
Implements summarization	False

***An “optiv” index is required** on each indexer for the app to function.

Prerequisites

- Splunk 6.3.x, 6.4.x or 6.5.x
- Linux or Windows Operating System
- If there is a distributed environment, install each app as indicated above.
- Web access is required to several threat list and news RSS sites.
- For the Globe visualization, install the Custom Visualizations app found at:

  https://splunkbase.splunk.com/app/2717/

Install

- Login to Splunk as an administrator.
- Go to Apps->Manage apps
- Click **Install app from file.**
- Browse to the file folder with the app zip file.
- Choose the file and click OK
- After the app is uploaded and installed, restart Splunk.

Upgrade Instructions

- Stop Splunk
- Remove the app from the directory structure:

```
rm -rf /opt/splunk/etc/apps/optiv_threat_intel
rm -rf /opt/splunk/etc/apps/optiv_TA_threat
```

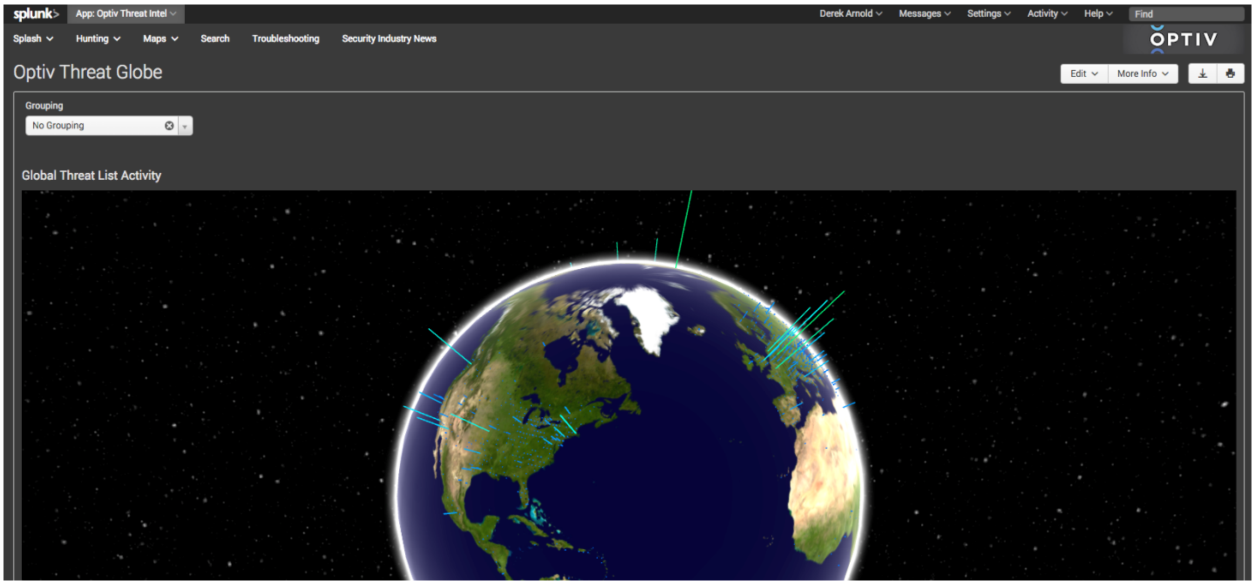
- Start Splunk
- Install using the steps shown in the Install section.

Support

Support is provided as a best effort basis. For best results post on Splunk Answers.

License

Screenshots

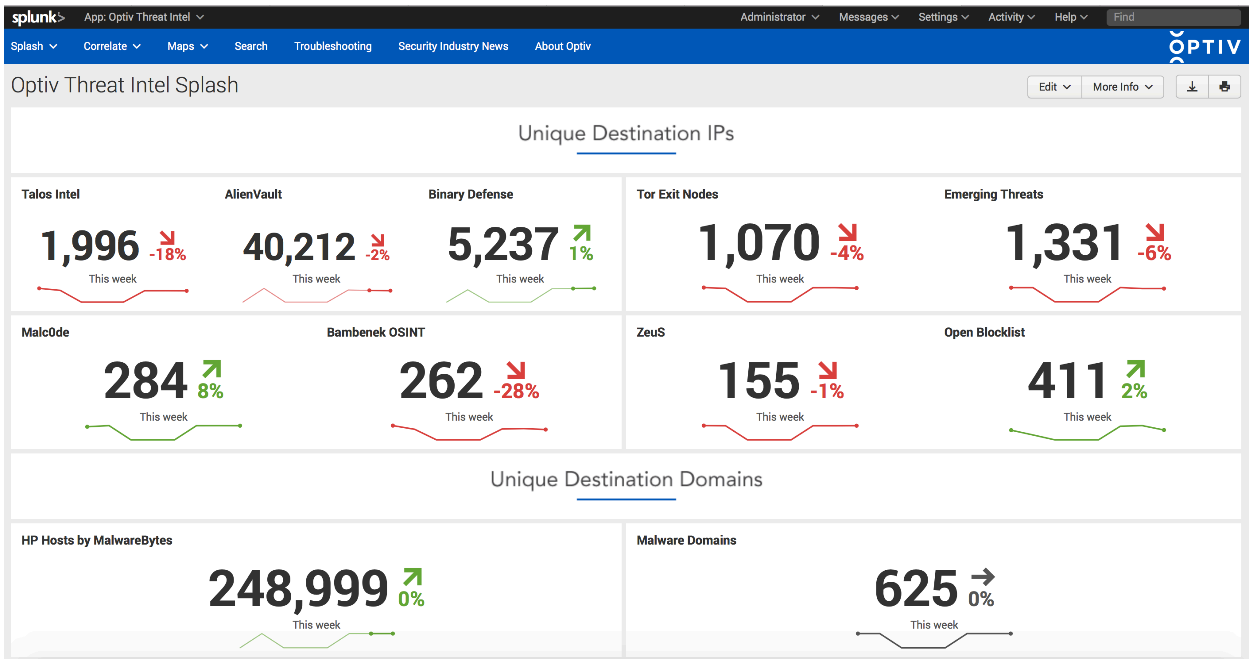


Optiv Threat Globe

Grouping: No Grouping

Global Threat List Activity

Figure 1: Optiv Threat Globe



Optiv Threat Intel Splash

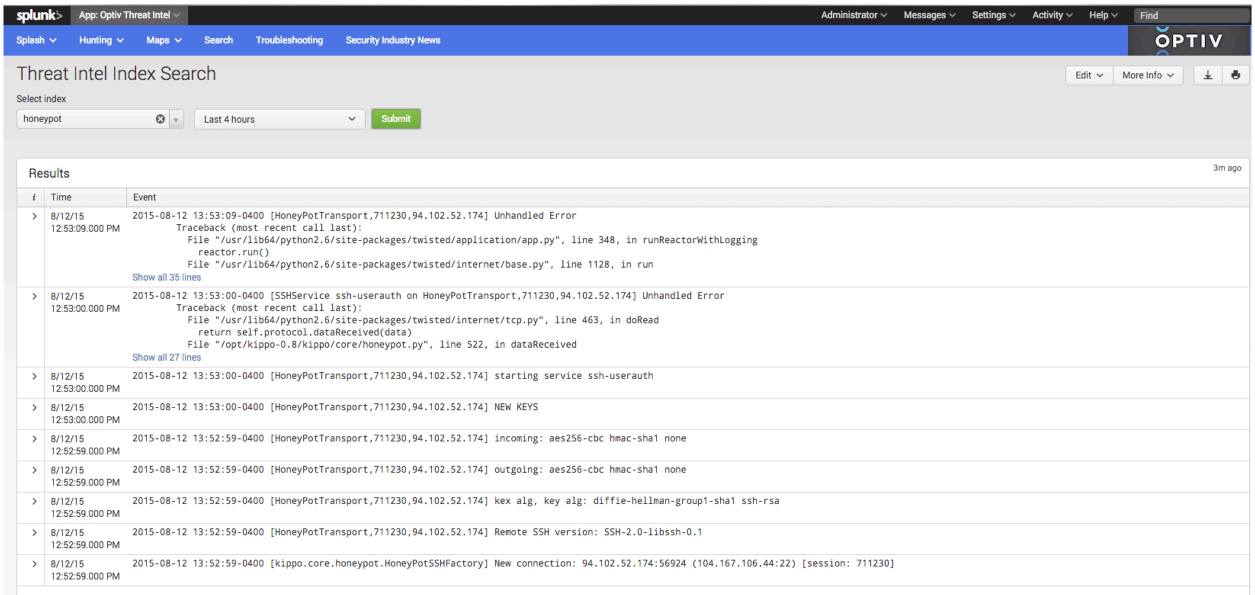
Unique Destination IPs

Talos Intel	1,996	-18% This week
AlienVault	40,212	-2% This week
Binary Defense	5,237	1% This week
Tor Exit Nodes	1,070	-4% This week
Emerging Threats	1,331	-6% This week
Malc0de	284	8% This week
Bambenek OSINT	262	-28% This week
ZeuS	155	-1% This week
Open Blocklist	411	2% This week

Unique Destination Domains

HP Hosts by MalwareBytes	248,999	0% This week
Malware Domains	625	0% This week

Figure 2: Optiv Threat Intel Splash



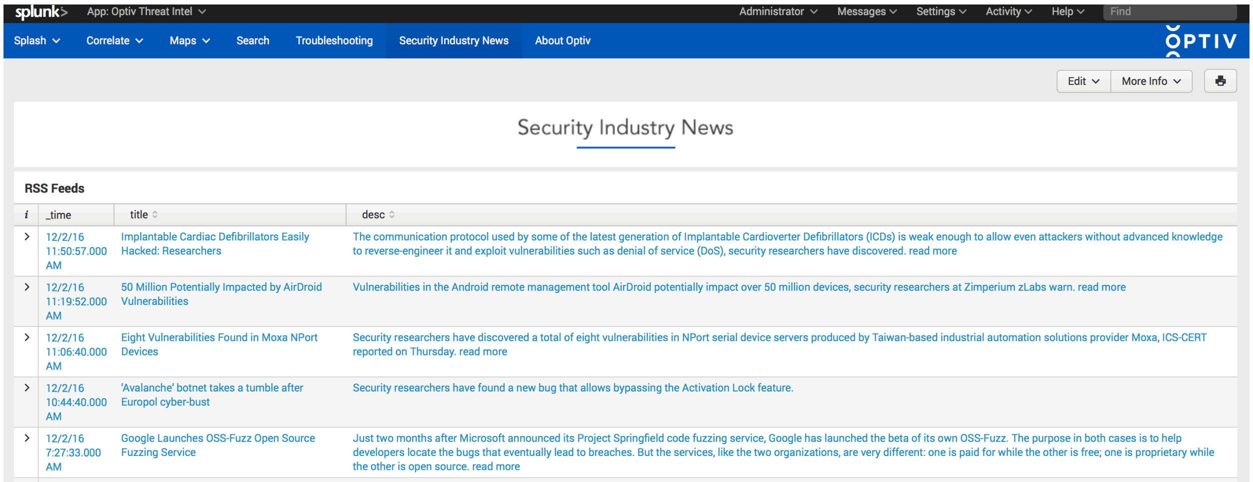
Threat Intel Index Search

Select index: honeypot — Last 4 hours — Submit

Results (3m ago)

```
i  Time            Event
>  8/12/15         2015-08-12 13:53:09-0400 [HoneyPotTransport,711230,94.102.52.174] Unhandled Error
   12:53:09.000 PM         Traceback (most recent call last):
                             File "/usr/lib64/python2.6/site-packages/twisted/application/app.py", line 348, in runReactorWithLogging
                               reactor.run()
                             File "/usr/lib64/python2.6/site-packages/twisted/internet/base.py", line 1128, in run
                   Show all 35 lines
>  8/12/15         2015-08-12 13:53:00-0400 [SSHService ssh-userauth on HoneyPotTransport,711230,94.102.52.174] Unhandled Error
   12:53:00.000 PM         Traceback (most recent call last):
                             File "/usr/lib64/python2.6/site-packages/twisted/internet/tcp.py", line 463, in doRead
                               return self.protocol.dataReceived(data)
                             File "/opt/kippo-0.8/kippo/core/honeypot.py", line 522, in dataReceived
                   Show all 27 lines
>  8/12/15         2015-08-12 13:53:00-0400 [HoneyPotTransport,711230,94.102.52.174] starting service ssh-userauth
   12:53:00.000 PM
>  8/12/15         2015-08-12 13:53:00-0400 [HoneyPotTransport,711230,94.102.52.174] NEW KEYS
   12:53:00.000 PM
>  8/12/15         2015-08-12 13:52:59-0400 [HoneyPotTransport,711230,94.102.52.174] incoming: aes256-cbc hmac-sha1 none
   12:52:59.000 PM
>  8/12/15         2015-08-12 13:52:59-0400 [HoneyPotTransport,711230,94.102.52.174] outgoing: aes256-cbc hmac-sha1 none
   12:52:59.000 PM
>  8/12/15         2015-08-12 13:52:59-0400 [HoneyPotTransport,711230,94.102.52.174] kex alg, key alg: diffie-hellman-group1-sha1 ssh-rsa
   12:52:59.000 PM
>  8/12/15         2015-08-12 13:52:59-0400 [HoneyPotTransport,711230,94.102.52.174] Remote SSH version: SSH-2.0-libssh-0.1
   12:52:59.000 PM
>  8/12/15         2015-08-12 13:52:59-0400 [kippo.core.honeypot.HoneyPotSSHFactory] New connection: 94.102.52.174:56924 (104.167.106.44:22) [session: 711230]
   12:52:59.000 PM
```

Figure 3: Threat Intel Index Search



Security Industry News

RSS Feeds

i	_time	title	desc
>	12/2/16 11:50:57.000 AM	Implantable Cardiac Defibrillators Easily Hacked: Researchers	The communication protocol used by some of the latest generation of Implantable Cardioverter Defibrillators (ICDs) is weak enough to allow even attackers without advanced knowledge to reverse-engineer it and exploit vulnerabilities such as denial of service (DoS), security researchers have discovered. read more
>	12/2/16 11:19:52.000 AM	50 Million Potentially Impacted by AirDroid Vulnerabilities	Vulnerabilities in the Android remote management tool AirDroid potentially impact over 50 million devices, security researchers at Zimperium zLabs warn. read more
>	12/2/16 11:06:40.000 AM	Eight Vulnerabilities Found in Moxa NPort Devices	Security researchers have discovered a total of eight vulnerabilities in NPort serial device servers produced by Taiwan-based industrial automation solutions provider Moxa, ICS-CERT reported on Thursday. read more
>	12/2/16 10:44:40.000 AM	'Avalanche' botnet takes a tumble after Europol cyber-bust	Security researchers have found a new bug that allows bypassing the Activation Lock feature.
>	12/2/16 7:27:33.000 AM	Google Launches OSS-Fuzz Open Source Fuzzing Service	Just two months after Microsoft announced its Project Springfield code fuzzing service, Google has launched the beta of its own OSS-Fuzz. The purpose in both cases is to help developers locate the bugs that eventually lead to breaches. But the services, like the two organizations, are very different: one is paid for while the other is free; one is proprietary while the other is open source. read more

Figure 4: RSS Security Industry News

OPTIV

1125 17th Street Suite 1700
Denver, CO 80202

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 10,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has