Optiv Threat Intel

Splunk App

Author: Derek Arnold

Version Number: 2.80

Date: 2.12.2016

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 reaching out to, or being attacked from, known attackers. 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, URLs and domains.
- Email alerting feature.
- Easy setup screen.
- IP search feature that displays threat list activity.
- Domain 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.

Prerequisites

- Splunk 6.3.x
- Linux or Windows Operating System
- If there is a distributed environment, install the app on the search tier only.
- 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.
- Launch the app and click **Continue** to go through the setup screen. If desired, set the email alerting settings and index settings. Click **Save** when finished.
- After install, please allow 4 hours for summary indexing to finish before the splash page populates fully.

Upgrade Instructions

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

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

or on Windows:

```
c:\Program Files\Splunk\etc\apps\optiv_threat_intel
```

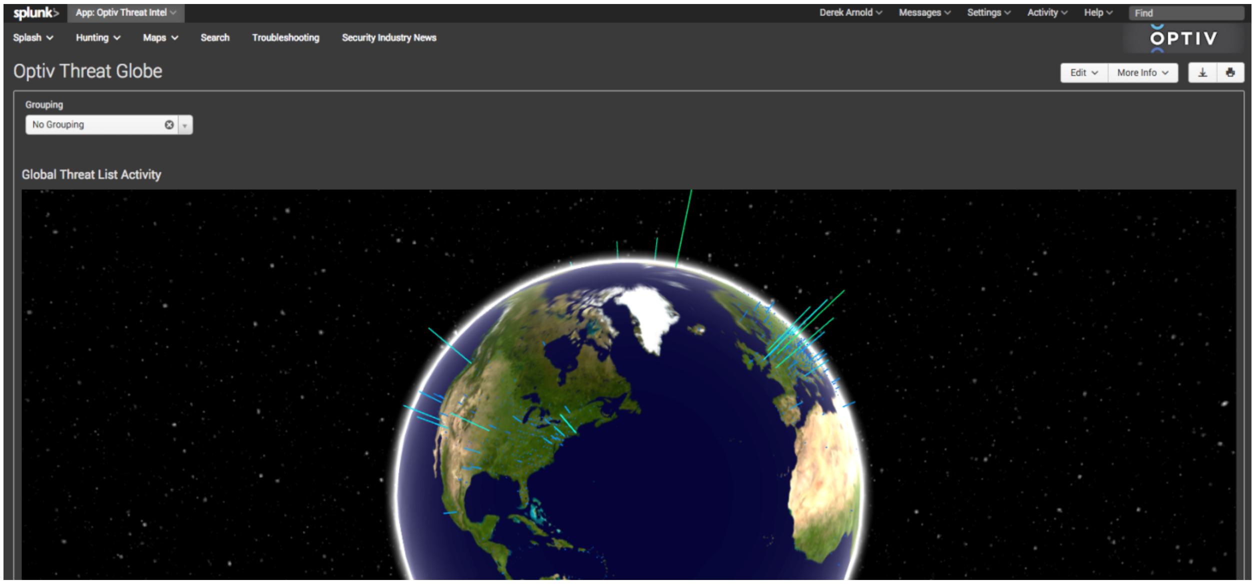
- Start Splunk
- Install using the steps shown in the Install section.
- After the app is uploaded and installed, restart Splunk.

Support

Support is provided as a best effort basis. For best results post on Splunk Answers and email the contact provided.

License

Screenshots

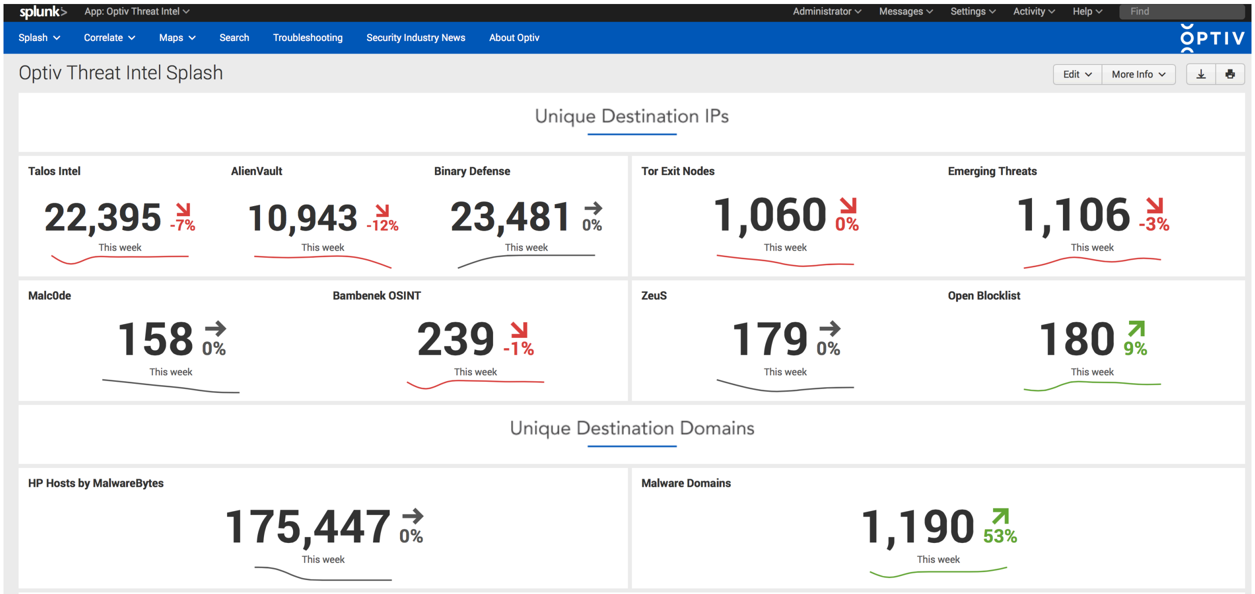


Optiv Threat Globe

Grouping: No Grouping

Global Threat List Activity

Figure 1: Optiv Threat Globe



Optiv Threat Intel Splash

Unique Destination IPs

Talos Intel: 22,395 -7% This week

AlienVault: 10,943 -12% This week

Binary Defense: 23,481 0% This week

Tor Exit Nodes: 1,060 0% This week

Emerging Threats: 1,106 -3% This week

Malc0de: 158 0% This week

Bambenek OSINT: 239 -1% This week

ZeuS: 179 0% This week

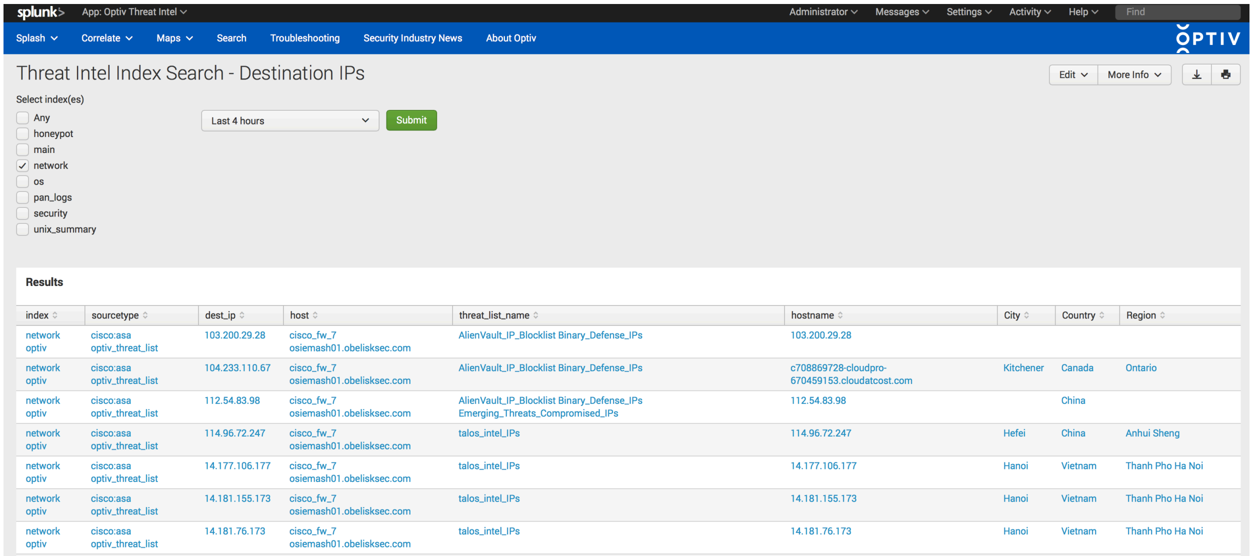
Open Blocklist: 180 9% This week

Unique Destination Domains

HP Hosts by MalwareBytes: 175,447 0% This week

Malware Domains: 1,190 53% This week

Figure 2: Optiv Threat Intel Splash



Threat Intel Index Search - Destination IPs

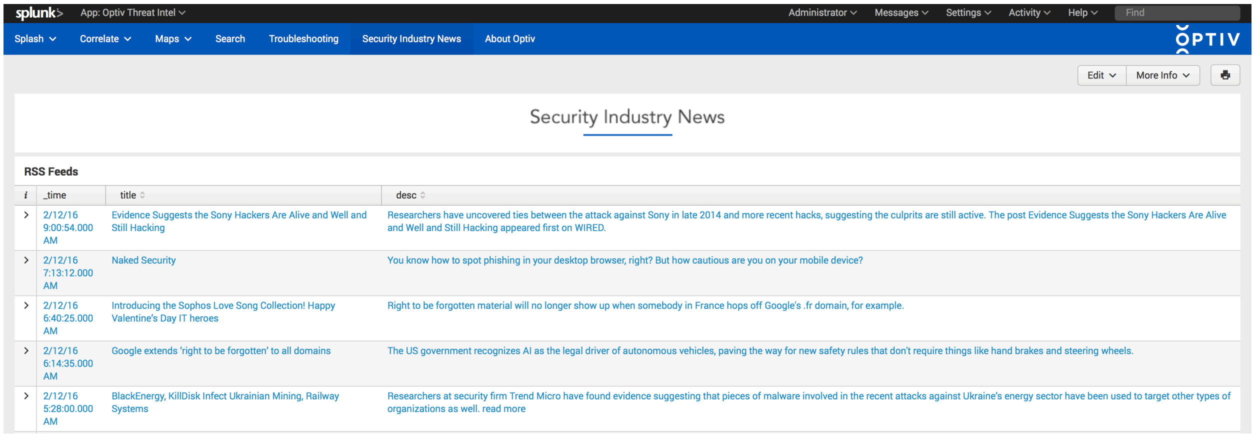
Select index(es)

□ Any
□ honeypot
□ main
☑ network
□ os
□ pan_logs
□ security
□ unix_summary

Results

index	sourcetype	dest_ip	host	threat_list_name	hostname	City	Country	Region
network optiv	cisco:asa optiv_threat_list	103.200.29.28	cisco_fw_7 osiemash01.obelisksec.com	AlienVault_IP_Blocklist Binary_Defense_IPs	103.200.29.28			
network optiv	cisco:asa optiv_threat_list	104.233.110.67	cisco_fw_7 osiemash01.obelisksec.com	AlienVault_IP_Blocklist Binary_Defense_IPs	c708869728-cloudpro-670459153.cloudatcost.com	Kitchener	Canada	Ontario
network optiv	cisco:asa optiv_threat_list	112.54.83.98	cisco_fw_7 osiemash01.obelisksec.com	AlienVault_IP_Blocklist Binary_Defense_IPs Emerging_Threats_Compromised_IPs	112.54.83.98		China	
network optiv	cisco:asa optiv_threat_list	114.96.72.247	cisco_fw_7 osiemash01.obelisksec.com	talos_intel_IPs	114.96.72.247	Hefei	China	Anhui Sheng
network optiv	cisco:asa optiv_threat_list	14.177.106.177	cisco_fw_7 osiemash01.obelisksec.com	talos_intel_IPs	14.177.106.177	Hanoi	Vietnam	Thanh Pho Ha Noi
network optiv	cisco:asa optiv_threat_list	14.181.155.173	cisco_fw_7 osiemash01.obelisksec.com	talos_intel_IPs	14.181.155.173	Hanoi	Vietnam	Thanh Pho Ha Noi
network optiv	cisco:asa optiv_threat_list	14.181.76.173	cisco_fw_7 osiemash01.obelisksec.com	talos_intel_IPs	14.181.76.173	Hanoi	Vietnam	Thanh Pho Ha Noi

Figure 3: Threat Intel Index Search



Security Industry News

RSS Feeds

i	_time	title	desc
>	2/12/16 9:00:54.000 AM	Evidence Suggests the Sony Hackers Are Alive and Well and Still Hacking	Researchers have uncovered ties between the attack against Sony in late 2014 and more recent hacks, suggesting the culprits are still active. The post Evidence Suggests the Sony Hackers Are Alive and Well and Still Hacking appeared first on WIRED.
>	2/12/16 7:13:12.000 AM	Naked Security	You know how to spot phishing in your desktop browser, right? But how cautious are you on your mobile device?
>	2/12/16 6:40:25.000 AM	Introducing the Sophos Love Song Collection! Happy Valentine's Day IT heroes	Right to be forgotten material will no longer show up when somebody in France hops off Google's .fr domain, for example.
>	2/12/16 6:14:35.000 AM	Google extends 'right to be forgotten' to all domains	The US government recognizes AI as the legal driver of autonomous vehicles, paving the way for new safety rules that don't require things like hand brakes and steering wheels.
>	2/12/16 5:28:00.000 AM	BlackEnergy, KillDisk Infect Ukrainian Mining, Railway Systems	Researchers at security firm Trend Micro have found evidence suggesting that pieces of malware involved in the recent attacks against Ukraine's energy sector have been used to target other types of organizations as well. read more

Figure 4: RSS Security Industry News