Enterprise Security Biology

Dissecting the Threat Intelligence Framework

John Stoner | Staff Security Architect | US Public Sector and then some

September 2017

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Whoami

- Splunker for 2.5 years
- MSSP, SIEM and Threat Intel for 13 years
- Other stuff for a bit longer
- Found on Splunk blogs talking about ES and Threat Intel
- Do some work with UBA as well

Agenda

- A Quick Word About Frameworks
- Collection
- Extraction
- Action
- Operationalizing

Enterprise Security Frameworks

Threat Intelligence

Incident Management

Asset & Identity

Risk

Adaptive Response

Our Goal Today?

- Better understand how Splunk processes threat indicators in Enterprise Security
- Better insight = Better Troubleshooting

Why Dissection?

dis·sect

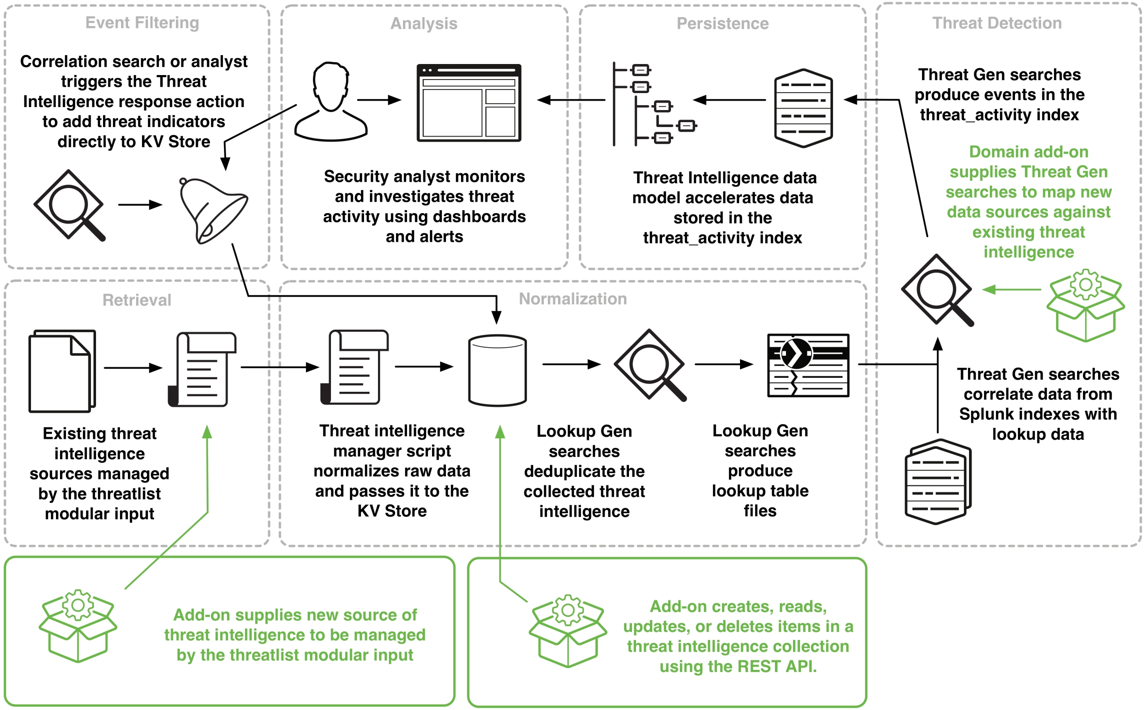
/dəˈsekt,dīˈsekt/

verb

- methodically cut up (a body, part, or plant) in order to study its internal parts
  - synonyms: anatomize, cut up/open, dismember, vivisect
- analyze (something) in minute detail
  - synonyms: analyze, examine, study, scrutinize, pore over, investigate, go over with a fine-tooth comb

Threat Intelligence Framework

http://dev.splunk.com/view/enterprise-security/SP-CAAAFBC



Event Filtering

Correlation search or analyst triggers the Threat Intelligence response action to add threat indicators directly to KV Store

Analysis

Security analyst monitors and investigates threat activity using dashboards and alerts

Persistence

Threat Intelligence data model accelerates data stored in the threat_activity index

Threat Detection

Threat Gen searches produce events in the threat_activity index

Domain add-on supplies Threat Gen searches to map new data sources against existing threat intelligence

Threat Gen searches correlate data from Splunk indexes with lookup data

Retrieval

Existing threat intelligence sources managed by the threatlist modular input

Normalization

Threat intelligence manager script normalizes raw data and passes it to the KV Store

Lookup Gen searches deduplicate the collected threat intelligence

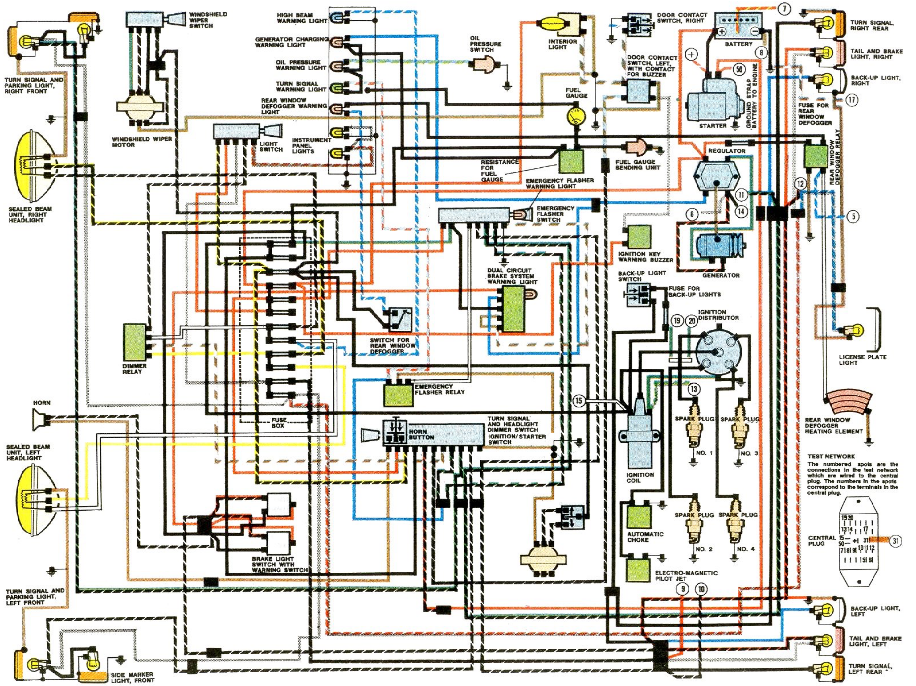
Lookup Gen searches produce lookup table files

Add-on supplies new source of threat intelligence to be managed by the threatlist modular input

Add-on creates, reads, updates, or deletes items in a threat intelligence collection using the REST API.

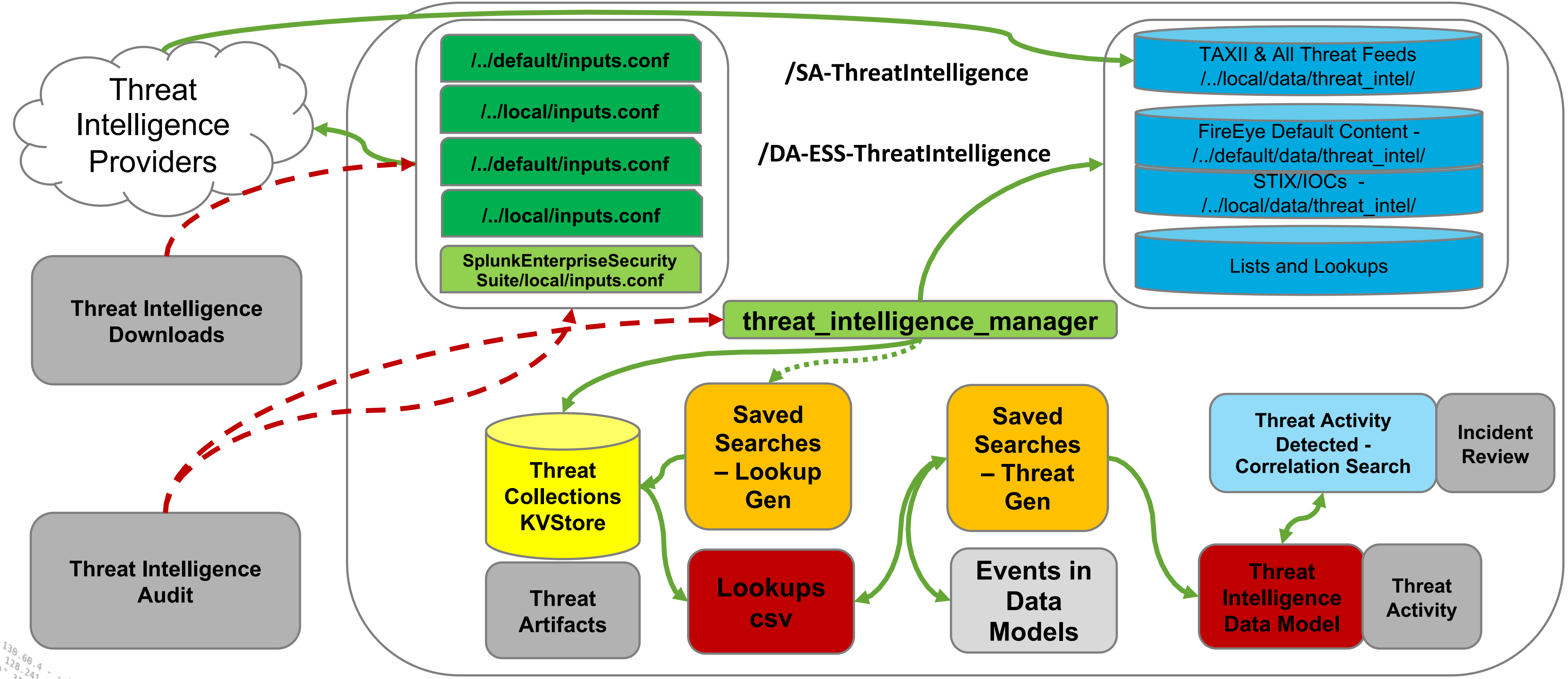
Why This Presentation...

1972 BEETLE AND SUPER BEETLE


WINDSHIELD WIPER SWITCH
HIGH BEAM WARNING LIGHT
GENERATOR CHARGING WARNING LIGHT
OIL PRESSURE WARNING LIGHT
TURN SIGNAL WARNING LIGHT
REAR WINDOW DEFOGGER WARNING LIGHT
OIL PRESSURE SWITCH
INTERIOR LIGHT
DOOR CONTACT SWITCH, RIGHT
BATTERY
7
8
TURN SIGNAL, RIGHT REAR
TAIL AND BRAKE LIGHT, RIGHT
BACK-UP LIGHT, RIGHT
FUSE FOR REAR WINDOW DEFOGGER
17
DOOR CONTACT SWITCH, LEFT, WITH CONTACT FOR BUZZER
FUEL GAUGE
50
STARTER
GROUND STRAP BATTERY TO ENGINE
TURN SIGNAL AND PARKING LIGHT, RIGHT FRONT
WINDSHIELD WIPER MOTOR
LIGHT SWITCH
INSTRUMENT PANEL LIGHTS
RESISTANCE FOR FUEL GAUGE
EMERGENCY FLASHER WARNING LIGHT
FUEL GAUGE SENDING UNIT
REGULATOR
REAR WINDOW DEFOGGER RELAY
12
11
14
6
5
SEALED BEAM UNIT, RIGHT HEADLIGHT
EMERGENCY FLASHER SWITCH
IGNITION KEY WARNING BUZZER
GENERATOR
BACK-UP LIGHT SWITCH
FUSE FOR BACK-UP LIGHTS
DUAL CIRCUIT BRAKE SYSTEM WARNING LIGHT
IGNITION DISTRIBUTOR
19
20
SWITCH FOR REAR WINDOW DEFOGGER
DIMMER RELAY
LICENSE PLATE LIGHT
EMERGENCY FLASHER RELAY
13
15
HORN
FUSE BOX
HORN BUTTON
TURN SIGNAL AND HEADLIGHT DIMMER SWITCH IGNITION/STARTER SWITCH
SPARK PLUG NO. 1
SPARK PLUG NO. 3
REAR WINDOW DEFOGGER HEATING ELEMENT
SEALED BEAM UNIT, LEFT HEADLIGHT
IGNITION COIL
CENTRAL PLUG
31
AUTOMATIC CHOKE
SPARK PLUG NO. 2
SPARK PLUG NO. 4
ELECTRO-MAGNETIC PILOT JET
9
10
BRAKE LIGHT SWITCH WITH WARNING SWITCH
TURN SIGNAL AND PARKING LIGHT, LEFT FRONT
SIDE MARKER LIGHT, FRONT
BACK-UP LIGHT, LEFT
TAIL AND BRAKE LIGHT, LEFT
TURN SIGNAL, LEFT REAR

TEST NETWORK
The numbered spots are the connections in the test network which are wired to the central plug. The numbers in the spots correspond to the terminals in the central plug.

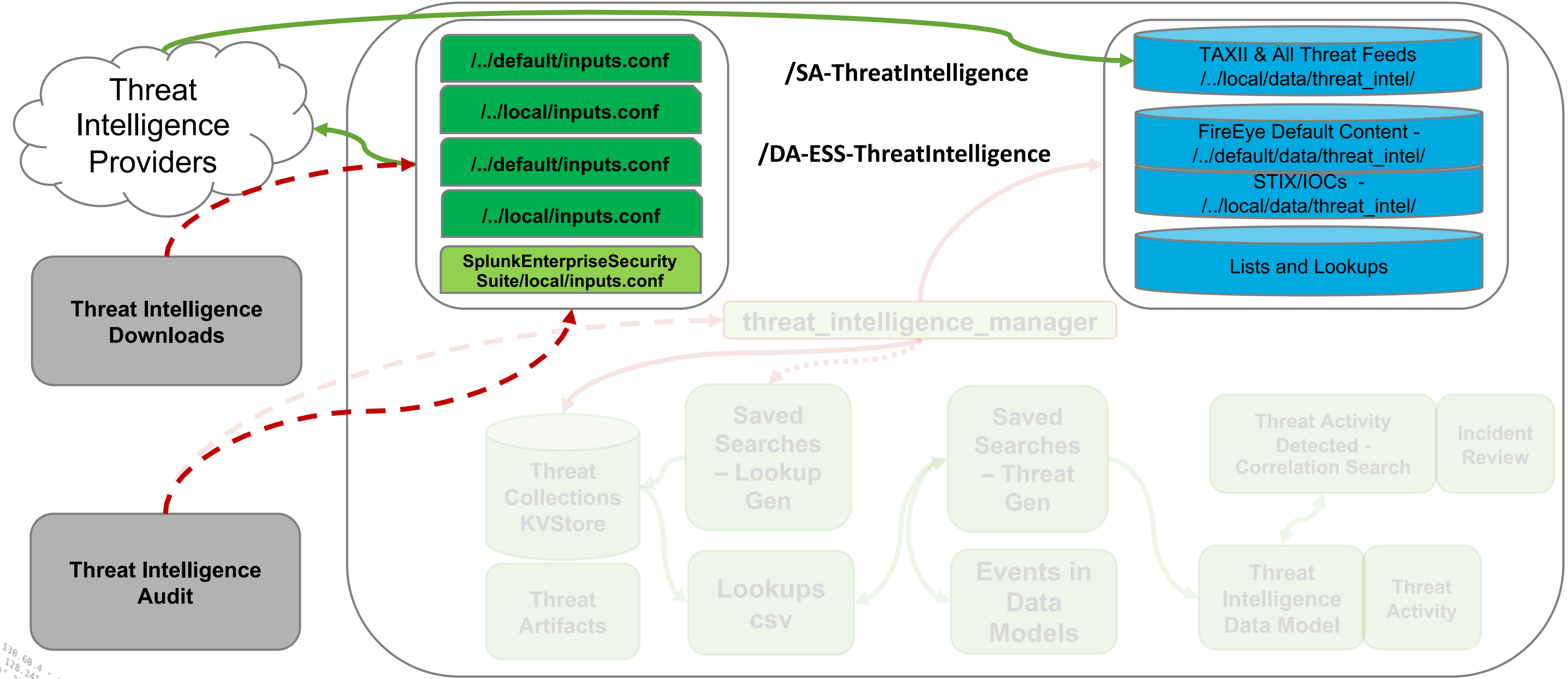
Threat Intel Framework Data Flow


Threat Intelligence Providers
/../default/inputs.conf
/../local/inputs.conf
/../default/inputs.conf
/../local/inputs.conf
SplunkEnterpriseSecuritySuite/local/inputs.conf
/SA-ThreatIntelligence
/DA-ESS-ThreatIntelligence
TAXII & All Threat Feeds
/../local/data/threat_intel/
FireEye Default Content -
/../default/data/threat_intel/
STIX/IOCs -
/../local/data/threat_intel/
Lists and Lookups
Threat Intelligence Downloads
threat_intelligence_manager
Threat Collections KVStore
Saved Searches – Lookup Gen
Saved Searches – Threat Gen
Threat Activity Detected - Correlation Search
Incident Review
Threat Intelligence Audit
Threat Artifacts
Lookups csv
Events in Data Models
Threat Intelligence Data Model
Threat Activity

splunk> .conf2017

Collection

Collection



Threat Intelligence Providers

Threat Intelligence Downloads

Threat Intelligence Audit

/../default/inputs.conf

/../local/inputs.conf

/../default/inputs.conf

/../local/inputs.conf

SplunkEnterpriseSecuritySuite/local/inputs.conf

/SA-ThreatIntelligence

/DA-ESS-ThreatIntelligence

TAXII & All Threat Feeds /../local/data/threat_intel/

FireEye Default Content - /../default/data/threat_intel/

STIX/IOCs - /../local/data/threat_intel/

Lists and Lookups

threat_intelligence_manager

Threat Collections KVStore

Threat Artifacts

Saved Searches – Lookup Gen

Lookups csv

Saved Searches – Threat Gen

Events in Data Models

Threat Activity Detected - Correlation Search

Incident Review

Threat Intelligence Data Model

Threat Activity

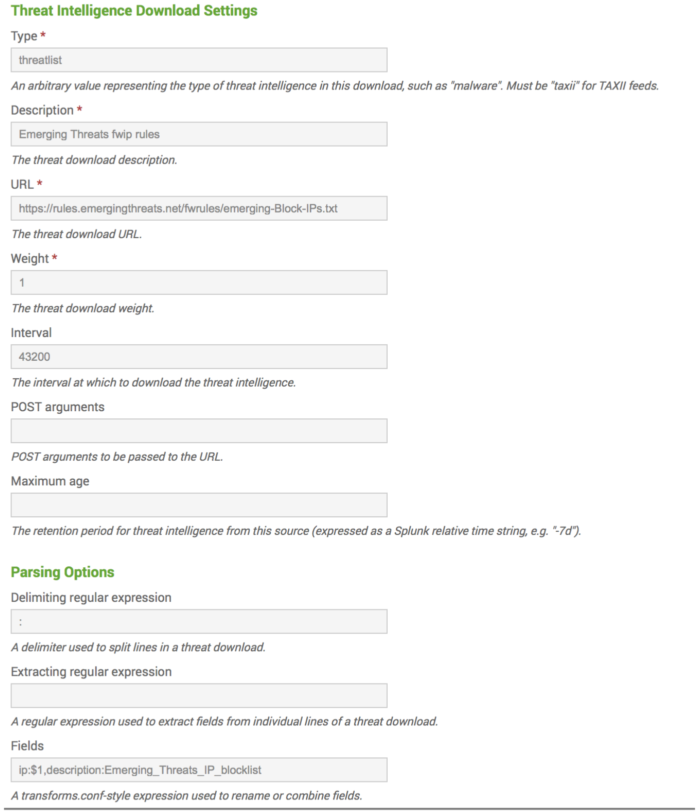
Collection

Defined by inputs.conf

- DA-ESS-ThreatIntelligence
  - default
    - Modular Input for Threat Intelligence Manager – More on that later
    - Threat Downloads
      - TAXII Feed
      - Local Lookups
  - local – Overrides the default configs
- SA-ThreatIntelligence
  - default – Commercial Threat Lists
    - Including Alexa, ICAAN Top Level Domains, Mozilla
      - Not merged into threat artifacts
  - local – Overrides the default configs
- If new threat downloads added via ES UI
  - Input will be in SplunkEnterpriseSecuritySuite directory

Threat Intel Downloads

- Found In Splunk
  - Setting -> Data Inputs
- Or ES
  - Configure -> Data Enrichment -> Threat Intelligence Downloads
- Make sure the name has no spaces in it
- Weight – Used with risk calculations
- Max Age – Provides aging of the data
  - Need to enable related saved search
- Fields is not starred as a required field but critical to get data ingested



Threat Intelligence Download Settings

Type *

threatlist

An arbitrary value representing the type of threat intelligence in this download, such as "malware". Must be "taxii" for TAXII feeds.

Description *

Emerging Threats fwip rules

The threat download description.

URL *

https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

The threat download URL.

Weight *

1

The threat download weight.

Interval

43200

The interval at which to download the threat intelligence.

POST arguments

POST arguments to be passed to the URL.

Maximum age

The retention period for threat intelligence from this source (expressed as a Splunk relative time string, e.g. "-7d").

Parsing Options

Delimiting regular expression

:

A delimiter used to split lines in a threat download.

Extracting regular expression

A regular expression used to extract fields from individual lines of a threat download.

Fields

ip:$1,description:Emerging_Threats_IP_blocklist

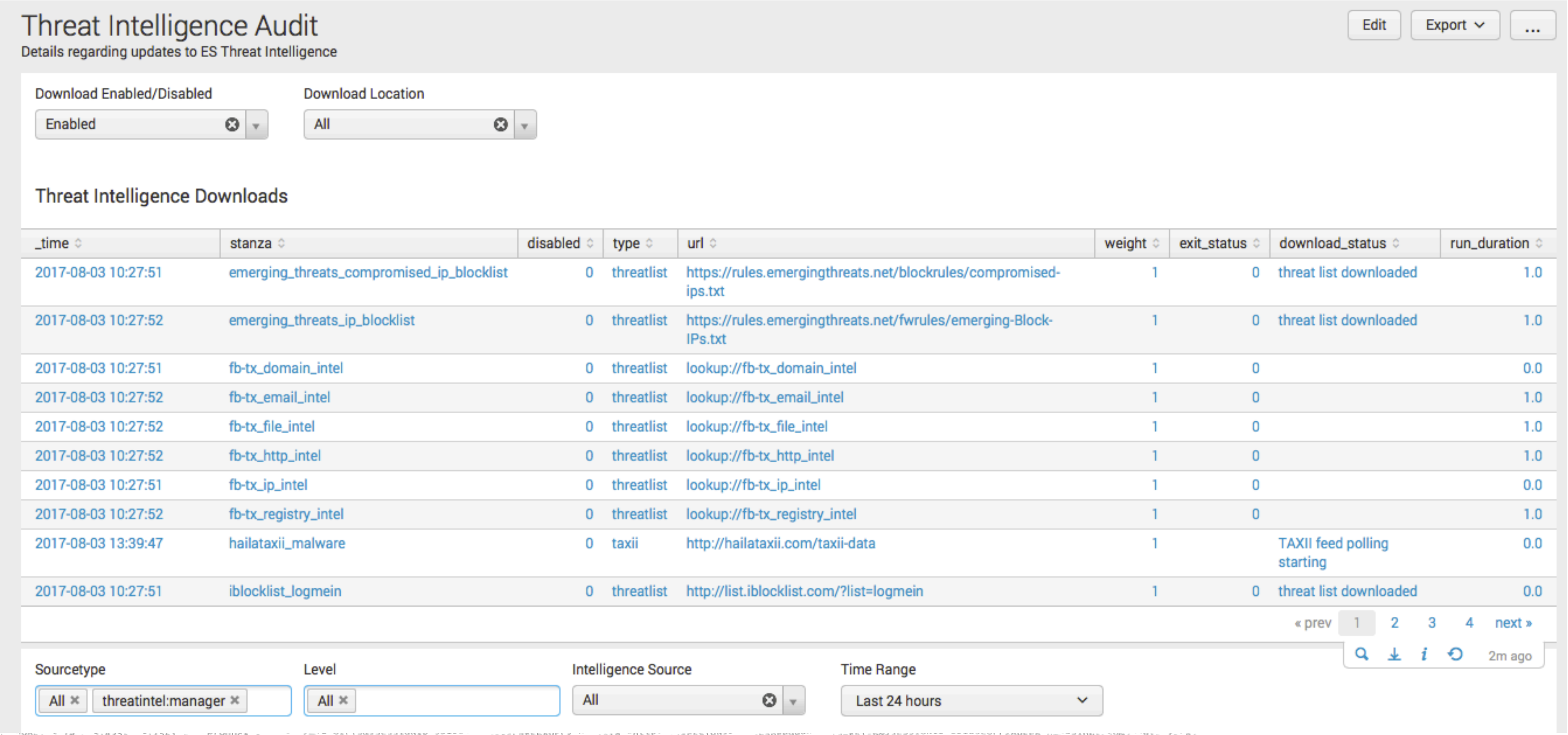
A transforms.conf-style expression used to rename or combine fields.

Default Data Downloads

Threat Provider	Threat Source	Source site
Alexa Internet*	Top 1 Million Sites	http://s3.amazonaws.com/alexa-static/
Emerging Threats	compromised IPs blocklist	http://rules.emergingthreats.net/blockrules
	fwip rules	http://rules.emergingthreats.net/fwrules
Hail a TAXII.com	Malware domain host list	http://hailataxii.com
I-Blocklist	Logmein, Piratebay, Proxy, Rapidshare, Spyware, Tor, Web attacker	http://list.iblocklist.com
IANA*	ICANN Top-level Domains List	http://data.iana.org
Malware Domains	Malware Domain Blocklist	http://mirror1.malwaredomains.com
Mozilla*	Mozilla Public Suffix List	https://publicsuffix.org
Phishtank	Phishtank Database	http://data.phishtank.com
SANS	SANS blocklist	http://isc.sans.edu
abuse.ch	Palevo C&C IP Blocklist	https://palevotracker.abuse.ch
abuse.ch	ZeuS blocklist (standard & bad IPs only)	https://zeustracker.abuse.ch

Threat Intel Download Audit

Did Threat Data Get Downloaded?



Threat Intelligence Audit

Details regarding updates to ES Threat Intelligence

Download Enabled/Disabled: Enabled

Download Location: All

Threat Intelligence Downloads

_time	stanza	disabled	type	url	weight	exit_status	download_status	run_duration
2017-08-03 10:27:51	emerging_threats_compromised_ip_blocklist	0	threatlist	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	1	0	threat list downloaded	1.0
2017-08-03 10:27:52	emerging_threats_ip_blocklist	0	threatlist	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	1	0	threat list downloaded	1.0
2017-08-03 10:27:51	fb-tx_domain_intel	0	threatlist	lookup://fb-tx_domain_intel	1	0		0.0
2017-08-03 10:27:52	fb-tx_email_intel	0	threatlist	lookup://fb-tx_email_intel	1	0		1.0
2017-08-03 10:27:52	fb-tx_file_intel	0	threatlist	lookup://fb-tx_file_intel	1	0		1.0
2017-08-03 10:27:52	fb-tx_http_intel	0	threatlist	lookup://fb-tx_http_intel	1	0		1.0
2017-08-03 10:27:51	fb-tx_ip_intel	0	threatlist	lookup://fb-tx_ip_intel	1	0		0.0
2017-08-03 10:27:52	fb-tx_registry_intel	0	threatlist	lookup://fb-tx_registry_intel	1	0		1.0
2017-08-03 13:39:47	hailataxii_malware	0	taxii	http://hailataxii.com/taxii-data	1		TAXII feed polling starting	0.0
2017-08-03 10:27:51	iblocklist_logmein	0	threatlist	http://list.iblocklist.com/?list=logmein	1	0	threat list downloaded	0.0

Sourcetype: All ×, threatintel:manager ×

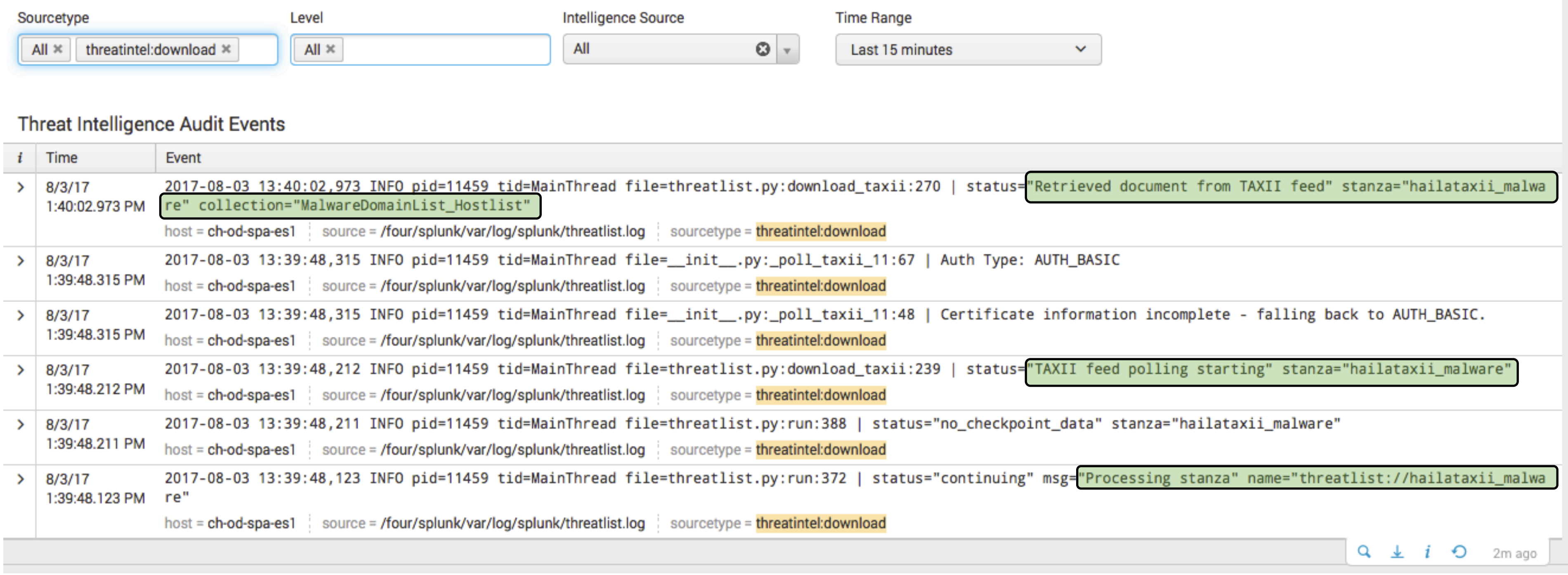
Level: All ×

Intelligence Source: All

Time Range: Last 24 hours

Threat Indicator Download

TAXII Example



Sourcetype: All × threatintel:download ×

Level: All ×

Intelligence Source: All

Time Range: Last 15 minutes

Threat Intelligence Audit Events

i	Time	Event

>	8/3/17 1:40:02.973 PM	`2017-08-03 13:40:02,973 INFO pid=11459 tid=MainThread file=threatlist.py:download_taxii:270 | status="Retrieved document from TAXII feed" stanza="hailataxii_malware" collection="MalwareDomainList_Hostlist"`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

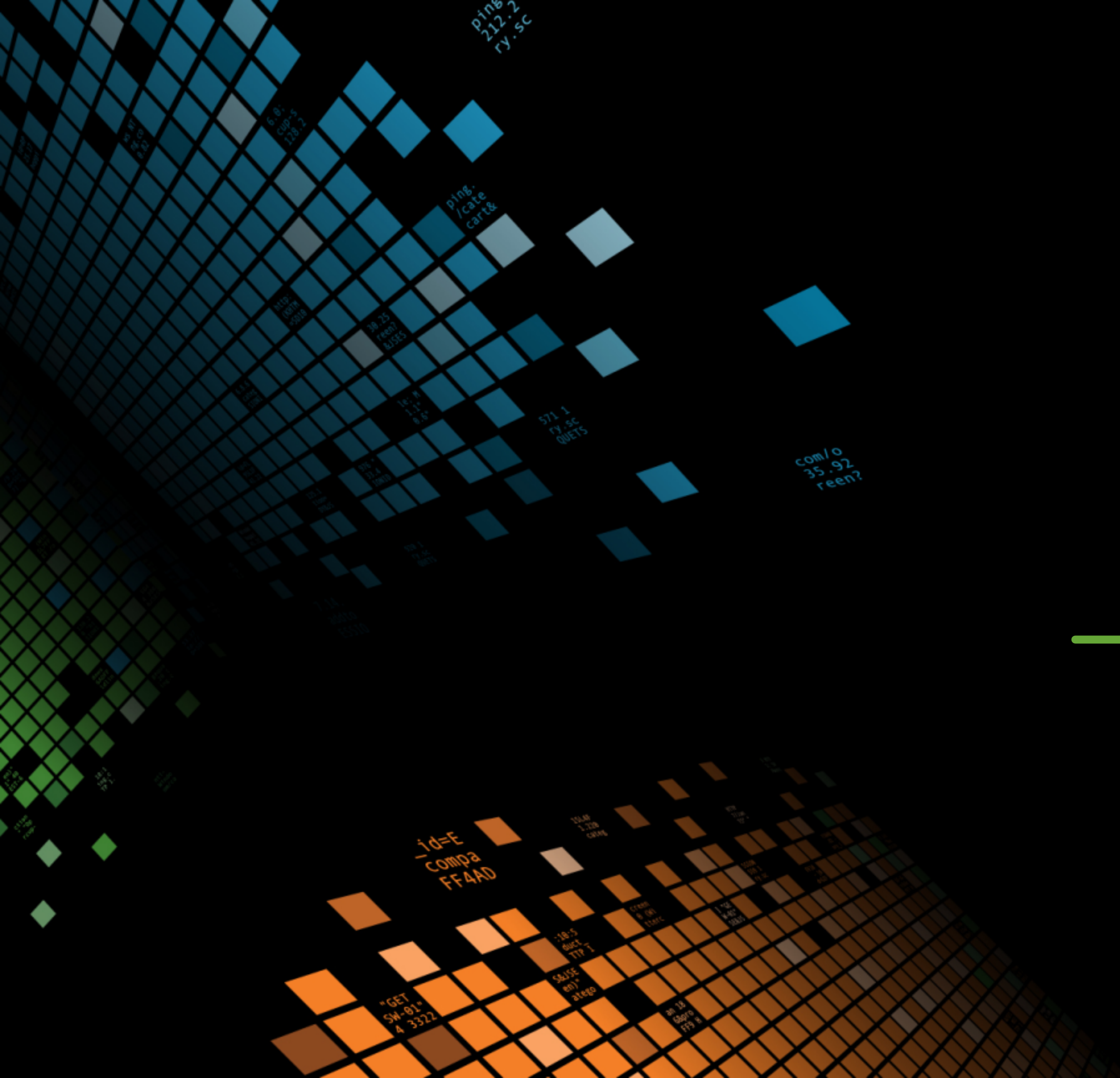
>	8/3/17 1:39:48.315 PM	`2017-08-03 13:39:48,315 INFO pid=11459 tid=MainThread file=__init__.py:_poll_taxii_11:67 | Auth Type: AUTH_BASIC`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

>	8/3/17 1:39:48.315 PM	`2017-08-03 13:39:48,315 INFO pid=11459 tid=MainThread file=__init__.py:_poll_taxii_11:48 | Certificate information incomplete - falling back to AUTH_BASIC.`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

>	8/3/17 1:39:48.212 PM	`2017-08-03 13:39:48,212 INFO pid=11459 tid=MainThread file=threatlist.py:download_taxii:239 | status="TAXII feed polling starting" stanza="hailataxii_malware"`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

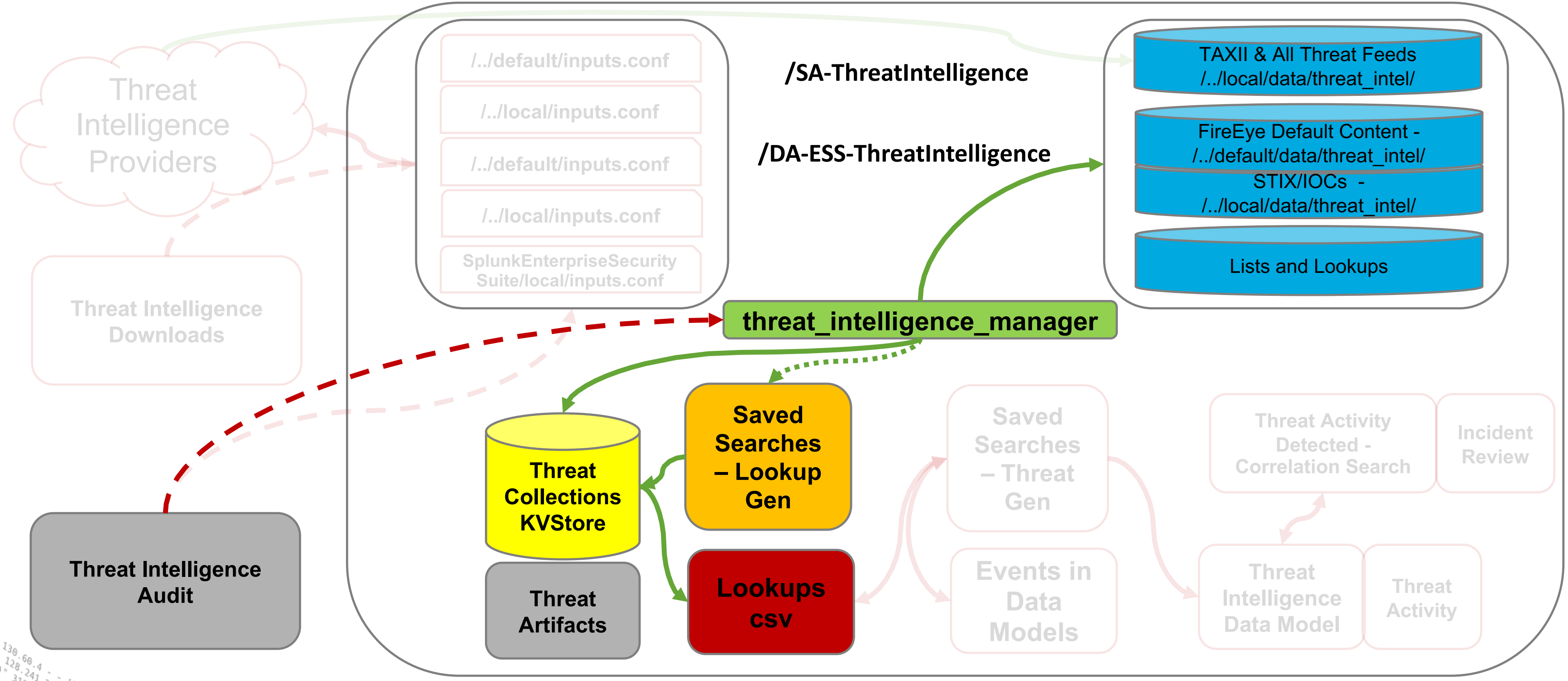
>	8/3/17 1:39:48.211 PM	`2017-08-03 13:39:48,211 INFO pid=11459 tid=MainThread file=threatlist.py:run:388 | status="no_checkpoint_data" stanza="hailataxii_malware"`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download

>	8/3/17 1:39:48.123 PM	`2017-08-03 13:39:48,123 INFO pid=11459 tid=MainThread file=threatlist.py:run:372 | status="continuing" msg="Processing stanza" name="threatlist://hailataxii_malware"`
		host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threatlist.log sourcetype = threatintel:download


ping
212.2
ry.sc
ping.
/cate
cart&
571 1
ry.sc
QUETS
com/o
35.92
reen?
_id=E
compa
FF4AD
"GET
SW-01"
4 3322

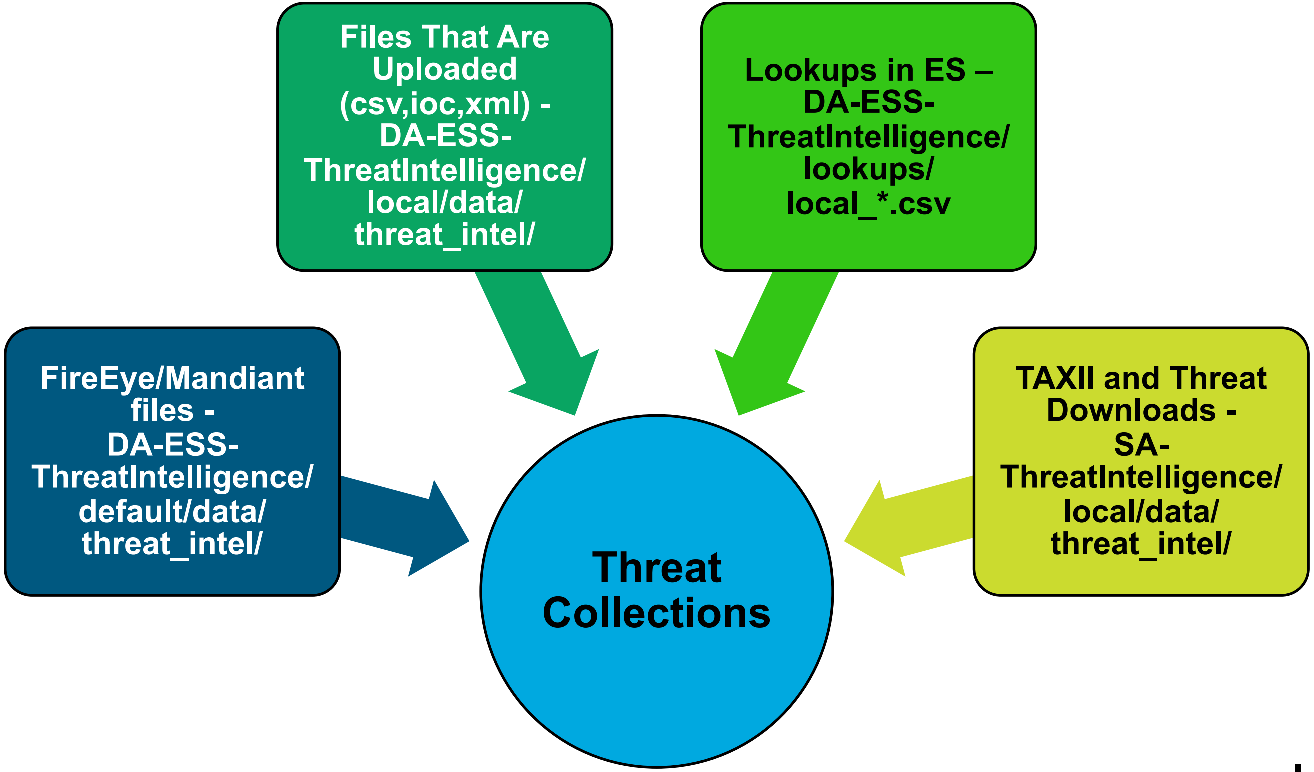
Extraction

Extraction


Threat Intelligence Providers
Threat Intelligence Downloads
Threat Intelligence Audit
/../default/inputs.conf
/../local/inputs.conf
/../default/inputs.conf
/../local/inputs.conf
SplunkEnterpriseSecurity Suite/local/inputs.conf
/SA-ThreatIntelligence
/DA-ESS-ThreatIntelligence
TAXII & All Threat Feeds /../local/data/threat_intel/
FireEye Default Content - /../default/data/threat_intel/
STIX/IOCs - /../local/data/threat_intel/
Lists and Lookups
threat_intelligence_manager
Threat Collections KVStore
Threat Artifacts
Saved Searches – Lookup Gen
Lookups csv
Saved Searches – Threat Gen
Events in Data Models
Threat Activity Detected - Correlation Search
Incident Review
Threat Intelligence Data Model
Threat Activity

splunk> .conf2017

Indicator Extraction



Files That Are Uploaded (csv,ioc,xml) - DA-ESS-ThreatIntelligence/ local/data/ threat_intel/

Lookups in ES – DA-ESS-ThreatIntelligence/ lookups/ local_*.csv

FireEye/Mandiant files - DA-ESS-ThreatIntelligence/ default/data/ threat_intel/

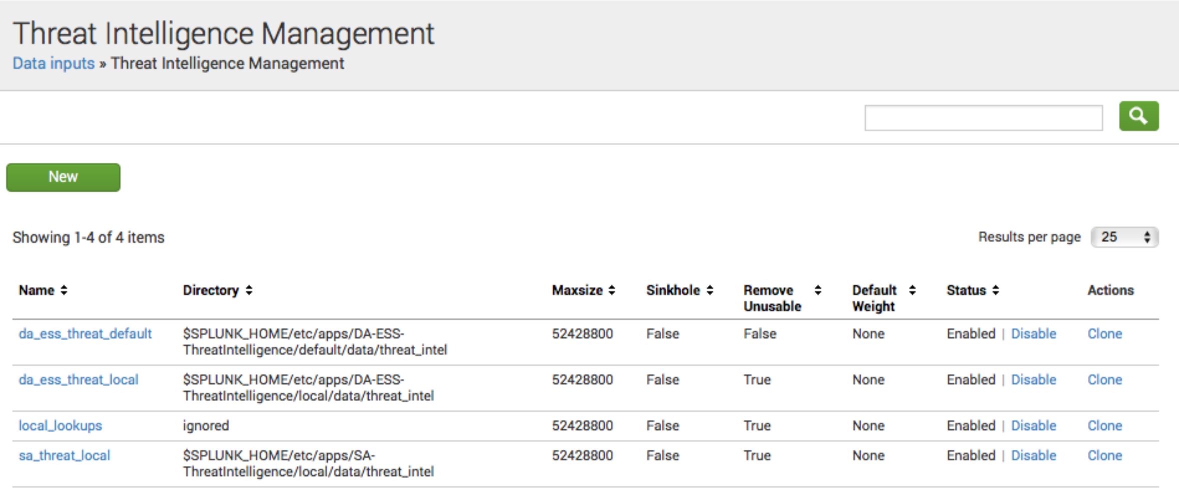
TAXII and Threat Downloads - SA-ThreatIntelligence/ local/data/ threat_intel/

Threat Collections

Threat Intelligence Management

Modular Input

- Settings -> Data Inputs -> Threat Intelligence Management Found
- In ES: Configure -> Data Enrichment -> Threat Intelligence Management
- Runs every minute by default
- Looks at data sets and then take actions
  - Parses new data if found
  - Sinkhole - delete file after processing
  - Remove Unusable – delete file after processing if it does not contain threat intelligence



Threat Intelligence Management

Data inputs » Threat Intelligence Management

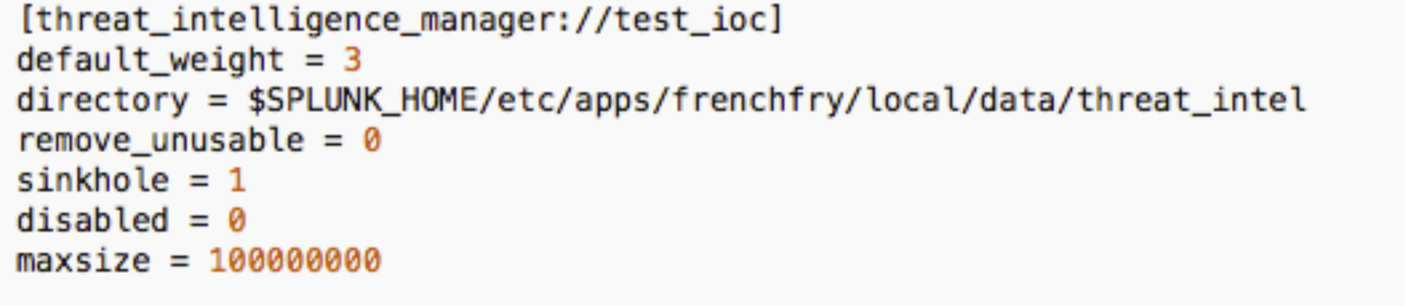
Showing 1-4 of 4 items

Results per page 25

Name	Directory	Maxsize	Sinkhole	Remove Unusable	Default Weight	Status	Actions
da_ess_threat_default	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel	52428800	False	False	None	Enabled | Disable	Clone
da_ess_threat_local	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel	52428800	False	True	None	Enabled | Disable	Clone
local_lookups	ignored	52428800	False	True	None	Enabled | Disable	Clone
sa_threat_local	$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel	52428800	False	True	None	Enabled | Disable	Clone

threat_intelligence_manager

- Found in /DA-ESS-ThreatIntelligence/bin/
- Runs threat_intelligence_manager.py
  - Parses and writes data, triggers lookup generation searches to run
- If set up via the UI, SplunkEnterpriseSecuritySuite /local/inputs.conf

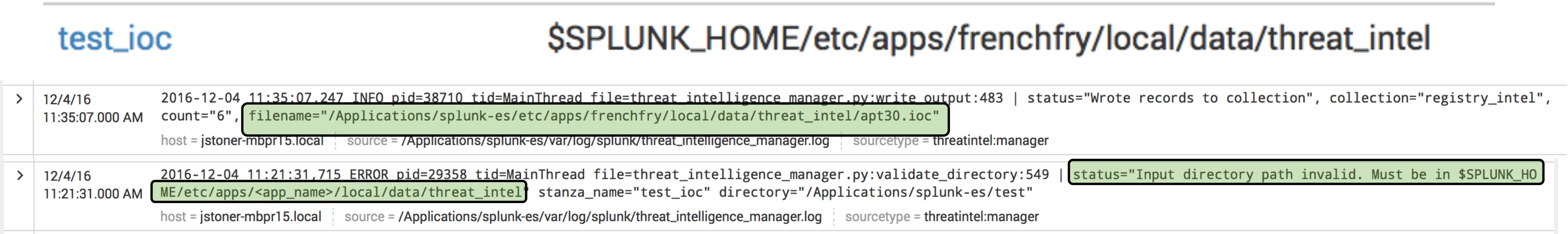


```
[threat_intelligence_manager://test_ioc]
default_weight = 3
directory = $SPLUNK_HOME/etc/apps/frenchfry/local/data/threat_intel
remove_unusable = 0
sinkhole = 1
disabled = 0
maxsize = 100000000
```

Adding Files To Threat Collections

OpenIOC and STIX

- OpenIOC files need to be .ioc
- STIX files need to be .xml
- Ad-hoc file modular input looks for files in
  - $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel folder
- User defined apps must adhere to strict directory structures
  - $SPLUNK_HOME/etc/apps/$app$/local/data/threat_intel



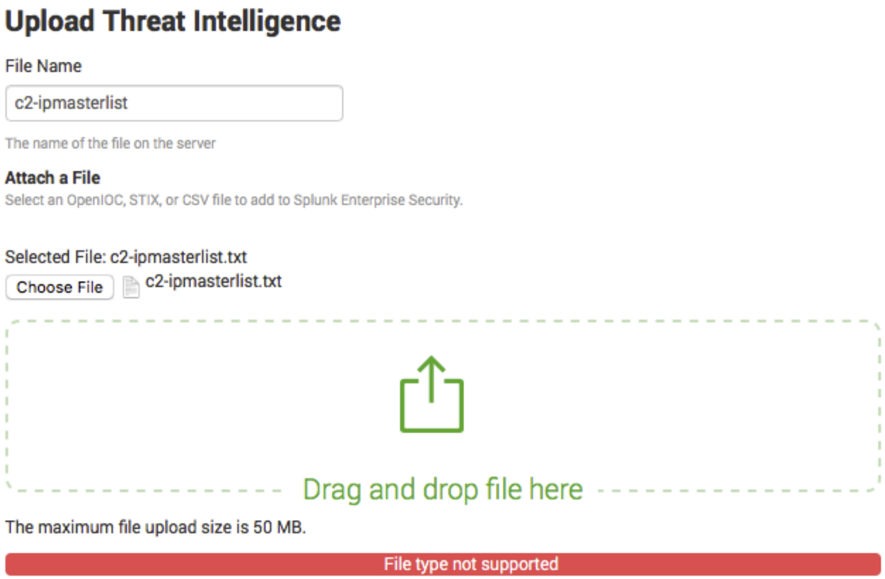
test_ioc $SPLUNK_HOME/etc/apps/frenchfry/local/data/threat_intel

```
> 12/4/16                2016-12-04 11:35:07.247 INFO pid=38710 tid=MainThread file=threat_intelligence_manager.py:write_output:483 | status="Wrote records to collection", collection="registry_intel",
  11:35:07.000 AM        count="6", filename="/Applications/splunk-es/etc/apps/frenchfry/local/data/threat_intel/apt30.ioc"
                         host = jstoner-mbpr15.local | source = /Applications/splunk-es/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 12/4/16                2016-12-04 11:21:31,715 ERROR pid=29358 tid=MainThread file=threat_intelligence_manager.py:validate_directory:549 | status="Input directory path invalid. Must be in $SPLUNK_HO
  11:21:31.000 AM        ME/etc/apps/<app_name>/local/data/threat_intel" stanza_name="test_ioc" directory="/Applications/splunk-es/test"
                         host = jstoner-mbpr15.local | source = /Applications/splunk-es/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
```

Adding Files To Threat Collections

CSV

- File Extensions Matter



Upload Threat Intelligence

File Name

c2-ipmasterlist

The name of the file on the server

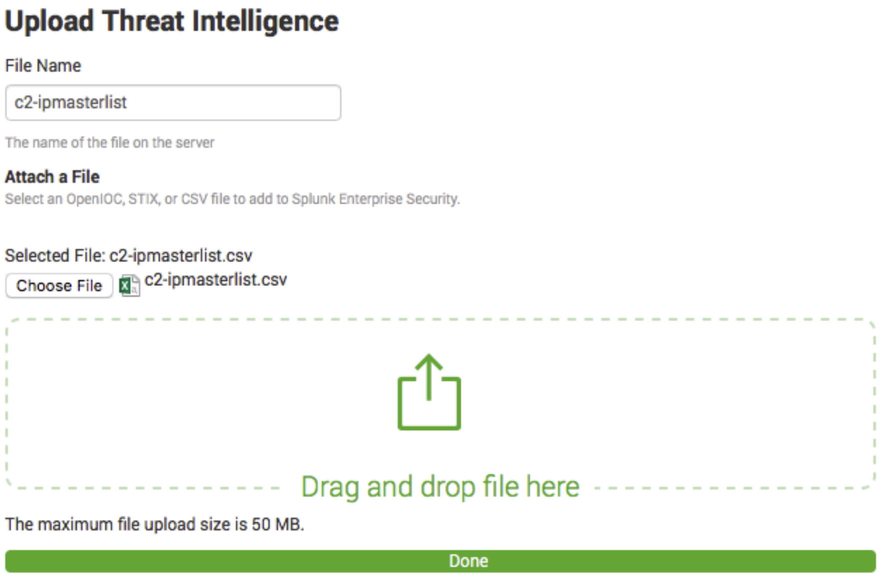
Attach a File

Select an OpenIOC, STIX, or CSV file to add to Splunk Enterprise Security.

Selected File: c2-ipmasterlist.txt

The maximum file upload size is 50 MB.

File type not supported



Upload Threat Intelligence

File Name

c2-ipmasterlist

The name of the file on the server

Attach a File

Select an OpenIOC, STIX, or CSV file to add to Splunk Enterprise Security.

Selected File: c2-ipmasterlist.csv

The maximum file upload size is 50 MB.

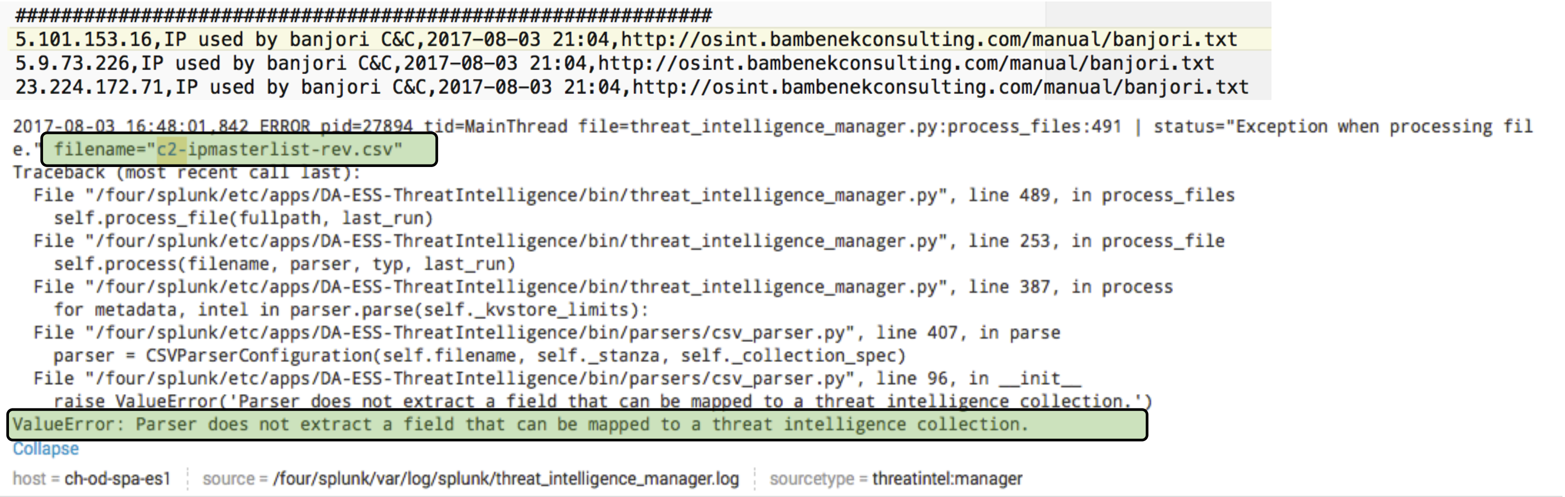
Done

Adding Files To Threat Collections

So Do File Formats

- Headers need to mirror local csv file formats
  - $SPLUNK_HOME/etc/apps/DA-ESS-ThreatInteligence/lookups/local_*.csv

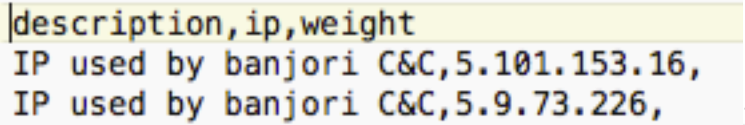
I am a sad panda.



```
##################################################################
5.101.153.16,IP used by banjori C&C,2017-08-03 21:04,http://osint.bambenekconsulting.com/manual/banjori.txt
5.9.73.226,IP used by banjori C&C,2017-08-03 21:04,http://osint.bambenekconsulting.com/manual/banjori.txt
23.224.172.71,IP used by banjori C&C,2017-08-03 21:04,http://osint.bambenekconsulting.com/manual/banjori.txt
```

```
2017-08-03 16:48:01.842 ERROR pid=27894 tid=MainThread file=threat_intelligence_manager.py:process_files:491 | status="Exception when processing fil
e." filename="c2-ipmasterlist-rev.csv"
Traceback (most recent call last):
  File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/threat_intelligence_manager.py", line 489, in process_files
    self.process_file(fullpath, last_run)
  File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/threat_intelligence_manager.py", line 253, in process_file
    self.process(filename, parser, typ, last_run)
  File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/threat_intelligence_manager.py", line 387, in process
    for metadata, intel in parser.parse(self._kvstore_limits):
  File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/parsers/csv_parser.py", line 407, in parse
    parser = CSVParserConfiguration(self.filename, self._stanza, self._collection_spec)
  File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/parsers/csv_parser.py", line 96, in __init__
    raise ValueError('Parser does not extract a field that can be mapped to a threat intelligence collection.')
ValueError: Parser does not extract a field that can be mapped to a threat intelligence collection.
```

host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

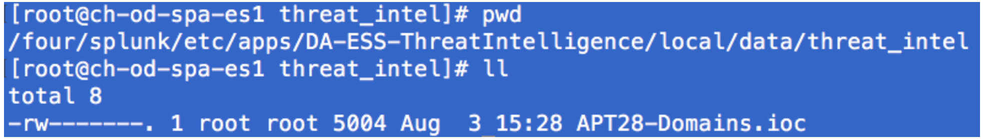


```
description,ip,weight
IP used by banjori C&C,5.101.153.16,
IP used by banjori C&C,5.9.73.226,
```

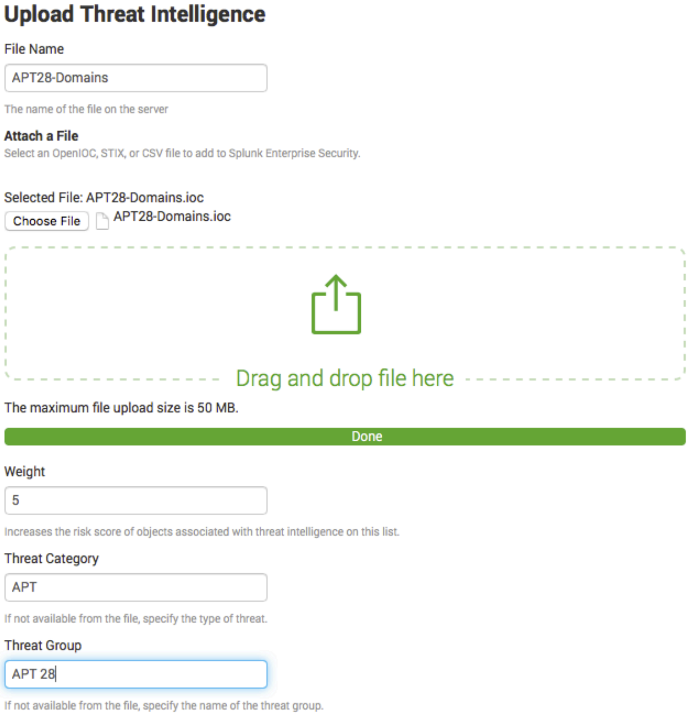
Adding Files To Threat Collections

Uploading

- Added in ES 4.6
- Removes concerns regarding placing the file correctly
- Important for cloud customers or those who don’t have CLI access
- Add a weight, category and group at ingest



```
[root@ch-od-spa-es1 threat_intel]# pwd
/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel
[root@ch-od-spa-es1 threat_intel]# ll
total 8
-rw-------. 1 root root 5004 Aug  3 15:28 APT28-Domains.ioc
```



Upload Threat Intelligence

File Name

APT28-Domains

The name of the file on the server

Attach a File

Select an OpenIOC, STIX, or CSV file to add to Splunk Enterprise Security.

Selected File: APT28-Domains.ioc

APT28-Domains.ioc

The maximum file upload size is 50 MB.

Weight

5

Increases the risk score of objects associated with threat intelligence on this list.

Threat Category

APT

If not available from the file, specify the type of threat.

Threat Group

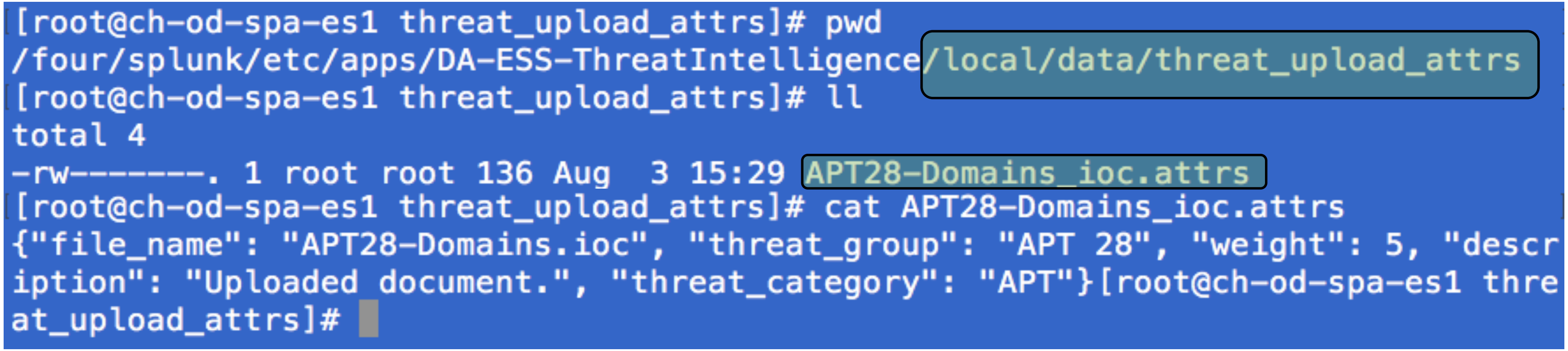
APT 28

If not available from the file, specify the name of the threat group.

splunk> .conf2017

Adding Files To Threat Collections

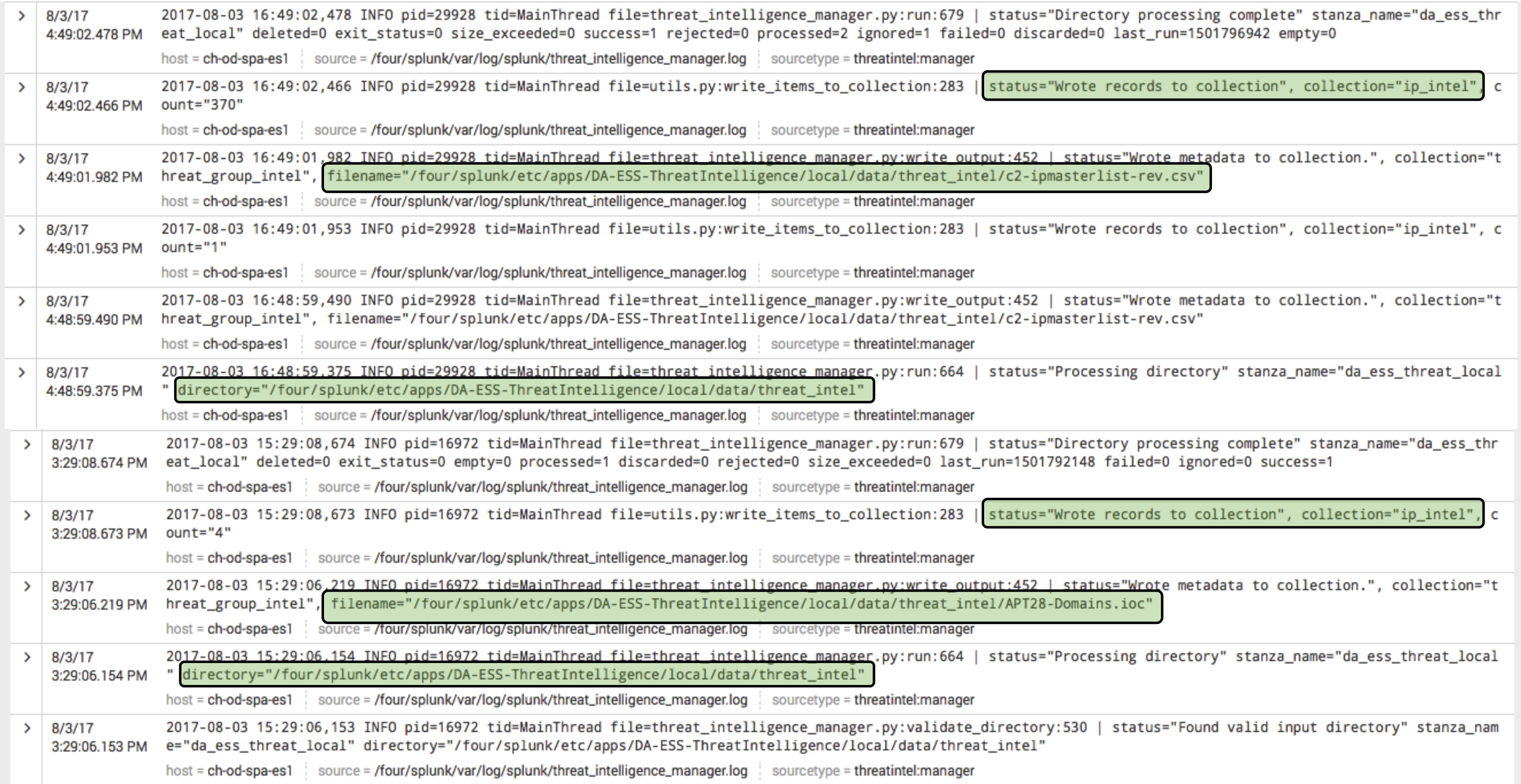
File System View



```
[root@ch-od-spa-es1 threat_upload_attrs]# pwd
/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_upload_attrs
[root@ch-od-spa-es1 threat_upload_attrs]# ll
total 4
-rw-------. 1 root root 136 Aug  3 15:29 APT28-Domains_ioc.attrs
[root@ch-od-spa-es1 threat_upload_attrs]# cat APT28-Domains_ioc.attrs
{"file_name": "APT28-Domains.ioc", "threat_group": "APT 28", "weight": 5, "descr
iption": "Uploaded document.", "threat_category": "APT"}[root@ch-od-spa-es1 thre
at_upload_attrs]# 
```

Adding Files To Threat Collections

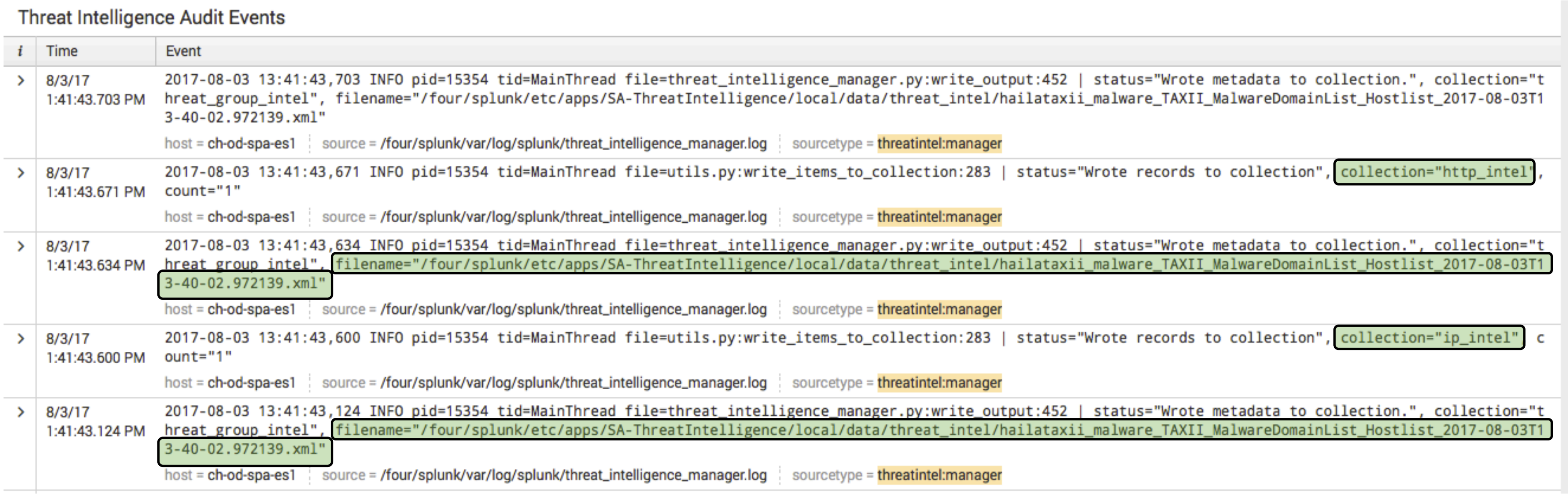
A Happy Uploader



```
> 8/3/17          2017-08-03 16:49:02,478 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="da_ess_thr
  4:49:02.478 PM  eat_local" deleted=0 exit_status=0 size_exceeded=0 success=1 rejected=0 processed=2 ignored=1 failed=0 discarded=0 last_run=1501796942 empty=0
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:49:02,466 INFO pid=29928 tid=MainThread file=utils.py:write_items_to_collection:283 | status="Wrote records to collection", collection="ip_intel", c
  4:49:02.466 PM  ount="370"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:49:01,982 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="t
  4:49:01.982 PM  hreat_group_intel", filename="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/c2-ipmasterlist-rev.csv"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:49:01,953 INFO pid=29928 tid=MainThread file=utils.py:write_items_to_collection:283 | status="Wrote records to collection", collection="ip_intel", c
  4:49:01.953 PM  ount="1"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:48:59,490 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="t
  4:48:59.490 PM  hreat_group_intel", filename="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/c2-ipmasterlist-rev.csv"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:48:59,375 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:run:664 | status="Processing directory" stanza_name="da_ess_threat_local
  4:48:59.375 PM  " directory="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 15:29:08,674 INFO pid=16972 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="da_ess_thr
  3:29:08.674 PM  eat_local" deleted=0 exit_status=0 empty=0 processed=1 discarded=0 rejected=0 size_exceeded=0 last_run=1501792148 failed=0 ignored=0 success=1
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 15:29:08,673 INFO pid=16972 tid=MainThread file=utils.py:write_items_to_collection:283 | status="Wrote records to collection", collection="ip_intel", c
  3:29:08.673 PM  ount="4"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 15:29:06,219 INFO pid=16972 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="t
  3:29:06.219 PM  hreat_group_intel", filename="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/APT28-Domains.ioc"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 15:29:06,154 INFO pid=16972 tid=MainThread file=threat_intelligence_manager.py:run:664 | status="Processing directory" stanza_name="da_ess_threat_local
  3:29:06.154 PM  " directory="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 15:29:06,153 INFO pid=16972 tid=MainThread file=threat_intelligence_manager.py:validate_directory:530 | status="Found valid input directory" stanza_nam
  3:29:06.153 PM  e="da_ess_threat_local" directory="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
```

TAXII & Threat Intel Downloads

Adding To Threat Collections



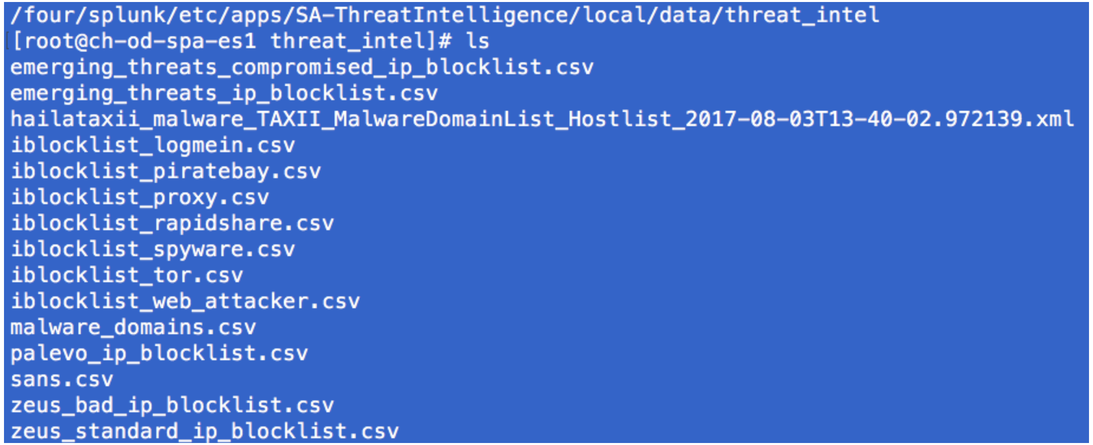
Threat Intelligence Audit Events

i	Time	Event
>	8/3/17 1:41:43.703 PM	2017-08-03 13:41:43,703 INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="threat_group_intel", filename="/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/hailataxii_malware_TAXII_MalwareDomainList_Hostlist_2017-08-03T13-40-02.972139.xml" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:41:43.671 PM	2017-08-03 13:41:43,671 INFO pid=15354 tid=MainThread file=utils.py:write_items_to_collection:283 | status="Wrote records to collection", collection="http_intel", count="1" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:41:43.634 PM	2017-08-03 13:41:43,634 INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="threat_group_intel", filename="/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/hailataxii_malware_TAXII_MalwareDomainList_Hostlist_2017-08-03T13-40-02.972139.xml" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:41:43.600 PM	2017-08-03 13:41:43,600 INFO pid=15354 tid=MainThread file=utils.py:write_items_to_collection:283 | status="Wrote records to collection", collection="ip_intel", count="1" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:41:43.124 PM	2017-08-03 13:41:43,124 INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status="Wrote metadata to collection.", collection="threat_group_intel", filename="/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/hailataxii_malware_TAXII_MalwareDomainList_Hostlist_2017-08-03T13-40-02.972139.xml" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager

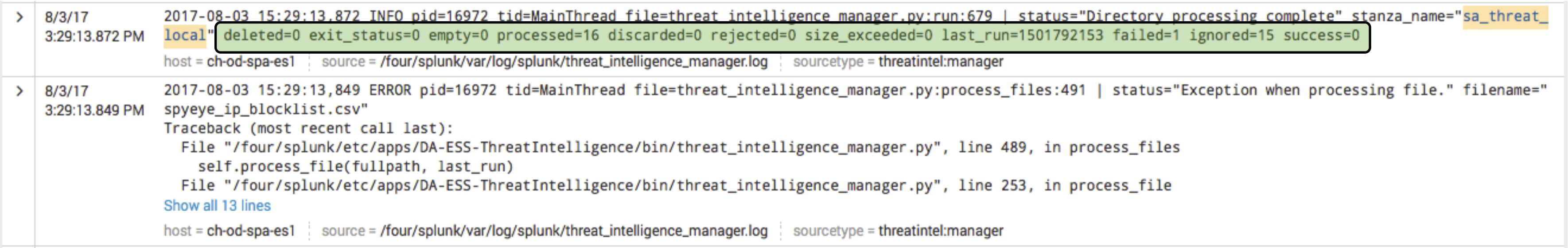
TAXII & Threat Intel Downloads

Audit Trail Provides Great Insight

- 15 csv files already downloaded had no new data
- 1 csv had an error in it



```
/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel
[root@ch-od-spa-es1 threat_intel]# ls
emerging_threats_compromised_ip_blocklist.csv
emerging_threats_ip_blocklist.csv
hailataxii_malware_TAXII_MalwareDomainList_Hostlist_2017-08-03T13-40-02.972139.xml
iblocklist_logmein.csv
iblocklist_piratebay.csv
iblocklist_proxy.csv
iblocklist_rapidshare.csv
iblocklist_spyware.csv
iblocklist_tor.csv
iblocklist_web_attacker.csv
malware_domains.csv
palevo_ip_blocklist.csv
sans.csv
zeus_bad_ip_blocklist.csv
zeus_standard_ip_blocklist.csv
```

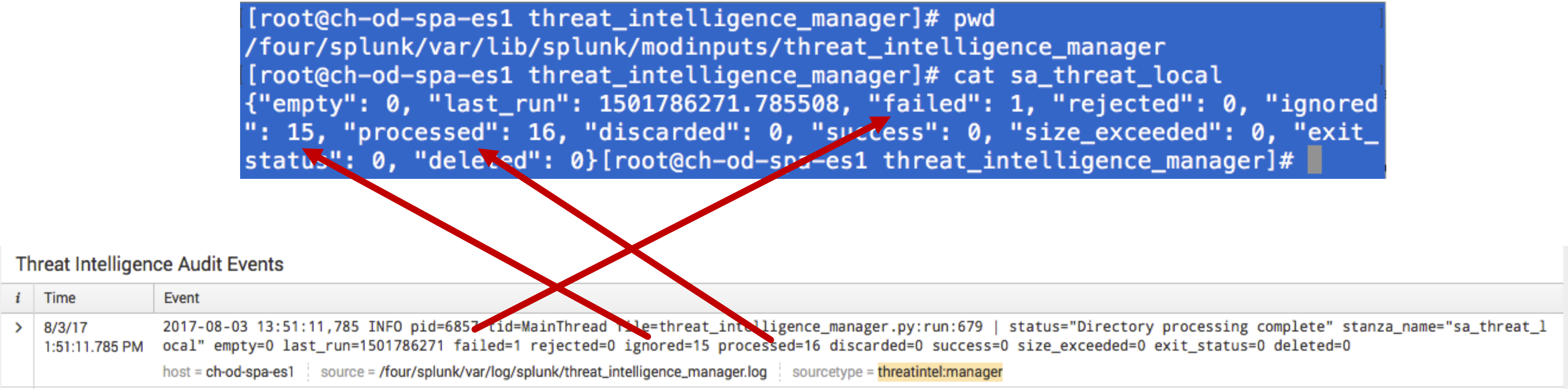


```
>  8/3/17           2017-08-03 15:29:13.872 INFO pid=16972 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="sa_threat_
   3:29:13.872 PM   local" deleted=0 exit_status=0 empty=0 processed=16 discarded=0 rejected=0 size_exceeded=0 last_run=1501792153 failed=1 ignored=15 success=0
                    host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

>  8/3/17           2017-08-03 15:29:13,849 ERROR pid=16972 tid=MainThread file=threat_intelligence_manager.py:process_files:491 | status="Exception when processing file." filename="
   3:29:13.849 PM   spyeye_ip_blocklist.csv"
                    Traceback (most recent call last):
                      File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/threat_intelligence_manager.py", line 489, in process_files
                        self.process_file(fullpath, last_run)
                      File "/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/bin/threat_intelligence_manager.py", line 253, in process_file
                    Show all 13 lines
                    host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
```

Modular Input Logging

Audit

- View Output in Threat Intelligence Audit
  - Text files in $SPLUNK_HOME/var/lib/splunk/modinputs/threat_intelligence_manager/
  - File updated every minute



```
[root@ch-od-spa-es1 threat_intelligence_manager]# pwd
/four/splunk/var/lib/splunk/modinputs/threat_intelligence_manager
[root@ch-od-spa-es1 threat_intelligence_manager]# cat sa_threat_local
{"empty": 0, "last_run": 1501786271.785508, "failed": 1, "rejected": 0, "ignored
": 15, "processed": 16, "discarded": 0, "success": 0, "size_exceeded": 0, "exit_
status": 0, "deleted": 0}[root@ch-od-spa-es1 threat_intelligence_manager]#
```

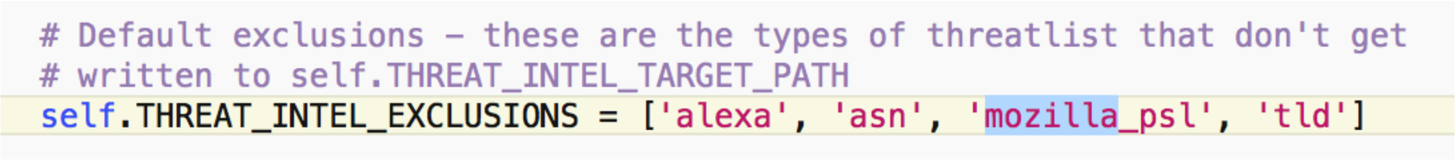
Threat Intelligence Audit Events

i	Time	Event
>	8/3/17 1:51:11.785 PM	2017-08-03 13:51:11,785 INFO pid=6857 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="sa_threat_local" empty=0 last_run=1501786271 failed=1 rejected=0 ignored=15 processed=16 discarded=0 success=0 size_exceeded=0 exit_status=0 deleted=0 host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager

Supporting Data

Alexa, ICANN, Mozilla

- Imported via the same mechanisms described
  - Stored in a different spot
    - $SPLUNK_HOME/var/lib/splunk/modinputs/threatlist/
- Excluded from the described processes
  - Threatlist.py

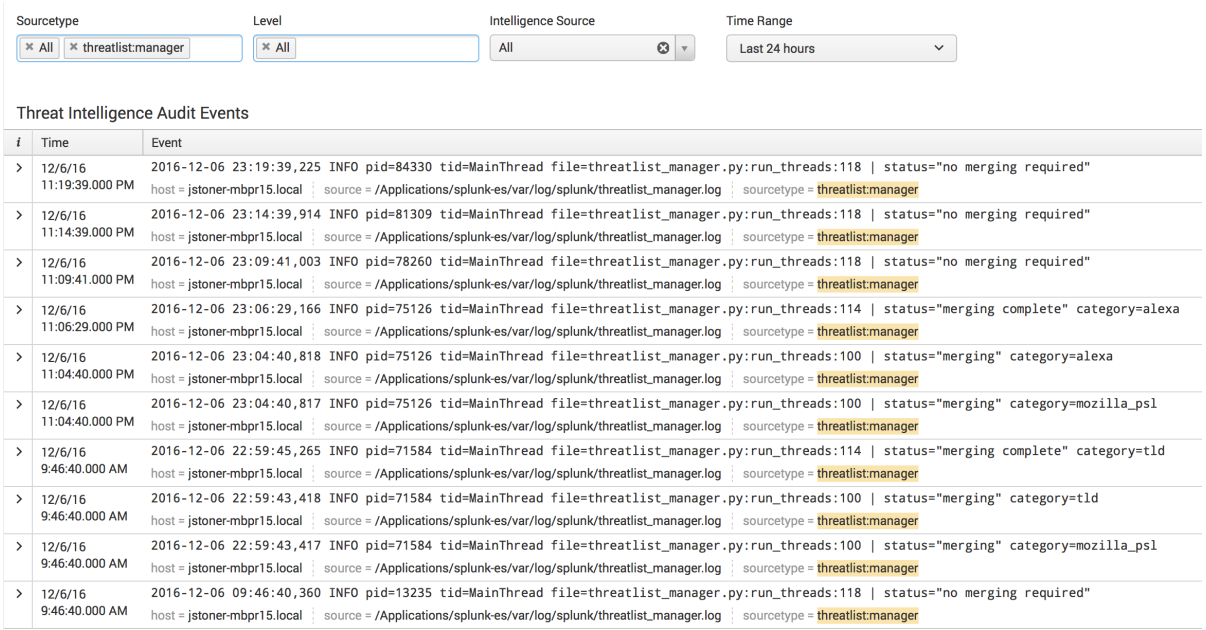


```
# Default exclusions - these are the types of threatlist that don't get
# written to self.THREAT_INTEL_TARGET_PATH
self.THREAT_INTEL_EXCLUSIONS = ['alexa', 'asn', 'mozilla_psl', 'tld']
```

- Separate Process

Previously - threatlist_manager

- SA-ThreatIntelligence
- Runs threatlist_manager.py
  - Merges Alexa, ICANN, Mozilla lists into lookups



Sourcetype: × All × threatlist:manager

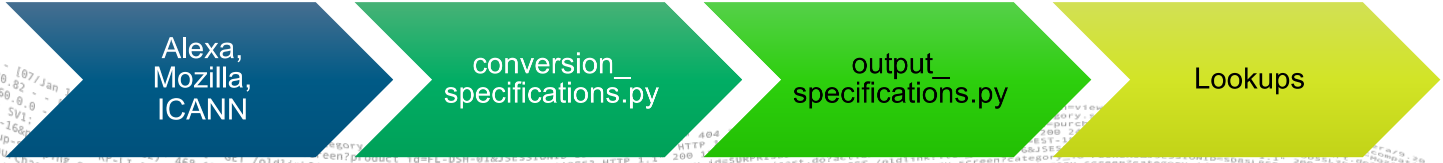
Level: × All

Intelligence Source: All

Time Range: Last 24 hours

Threat Intelligence Audit Events

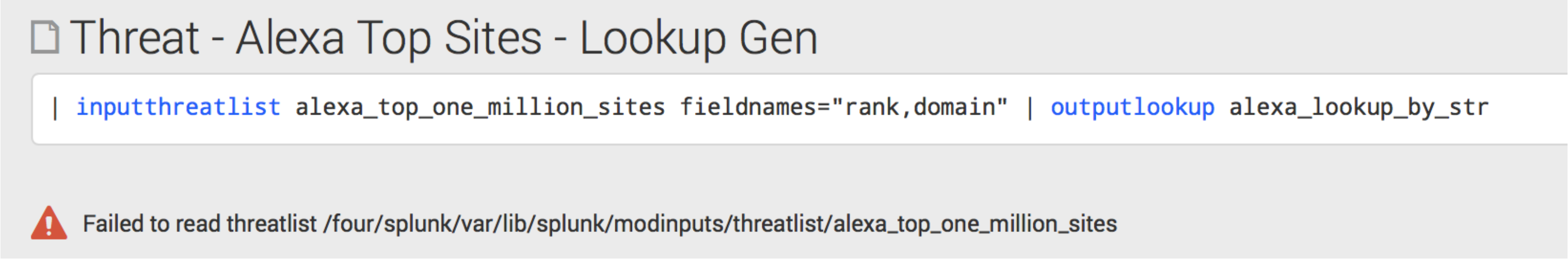
i	Time	Event
>	12/6/16 11:19:39.000 PM	2016-12-06 23:19:39,225 INFO pid=84330 tid=MainThread file=threatlist_manager.py:run_threads:118 | status="no merging required" host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 11:14:39.000 PM	2016-12-06 23:14:39,914 INFO pid=81309 tid=MainThread file=threatlist_manager.py:run_threads:118 | status="no merging required" host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 11:09:41.000 PM	2016-12-06 23:09:41,003 INFO pid=78260 tid=MainThread file=threatlist_manager.py:run_threads:118 | status="no merging required" host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 11:06:29.000 PM	2016-12-06 23:06:29,166 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:114 | status="merging complete" category=alexa host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 11:04:40.000 PM	2016-12-06 23:04:40,818 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:100 | status="merging" category=alexa host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 11:04:40.000 PM	2016-12-06 23:04:40,817 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:100 | status="merging" category=mozilla_psl host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 9:46:40.000 AM	2016-12-06 22:59:45,265 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:114 | status="merging complete" category=tld host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 9:46:40.000 AM	2016-12-06 22:59:43,418 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:100 | status="merging" category=tld host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 9:46:40.000 AM	2016-12-06 22:59:43,417 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:100 | status="merging" category=mozilla_psl host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager
>	12/6/16 9:46:40.000 AM	2016-12-06 09:46:40,360 INFO pid=13235 tid=MainThread file=threatlist_manager.py:run_threads:118 | status="no merging required" host = jstoner-mbpr15.local source = /Applications/splunk-es/var/log/splunk/threatlist_manager.log sourcetype = threatlist:manager



Now – New Process

Alexa, ICANN, Mozilla

- Handled via Saved Searches
  - inputthreatlist command
  - Looks in a very specific location (same as where we downloaded that data)
  - outputlookup command to write to lookup
  - Scheduled like any other splunk search



Threat - Alexa Top Sites - Lookup Gen

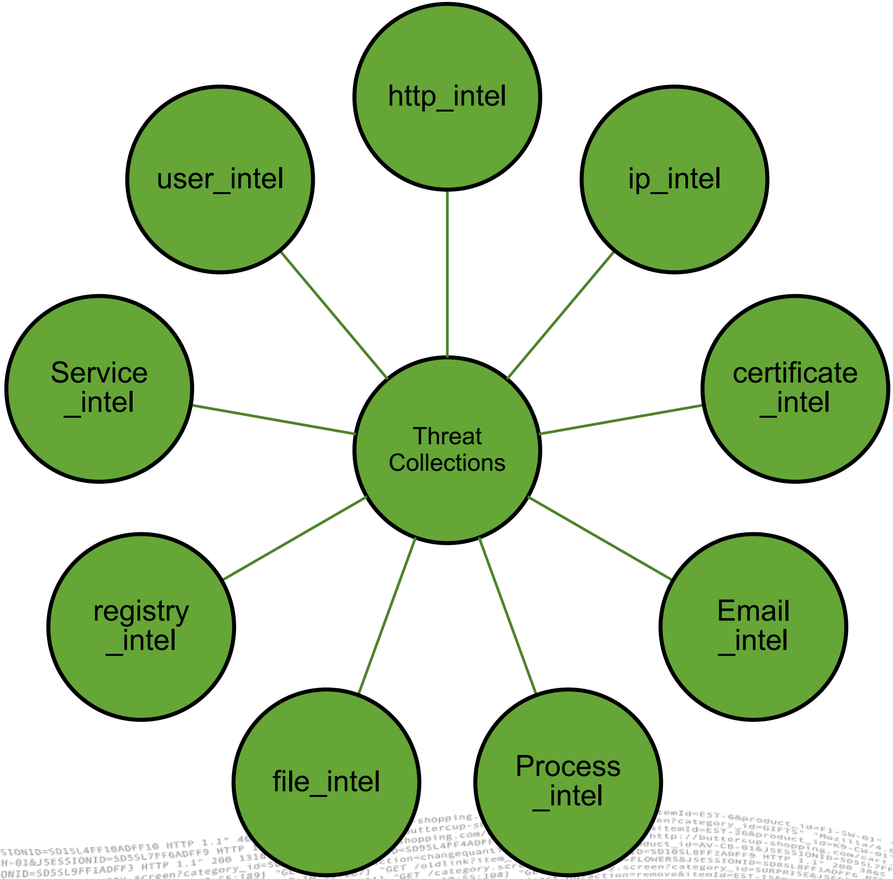
```
| inputthreatlist alexa_top_one_million_sites fieldnames="rank,domain" | outputlookup alexa_lookup_by_str
```

Failed to read threatlist /four/splunk/var/lib/splunk/modinputs/threatlist/alexa_top_one_million_sites

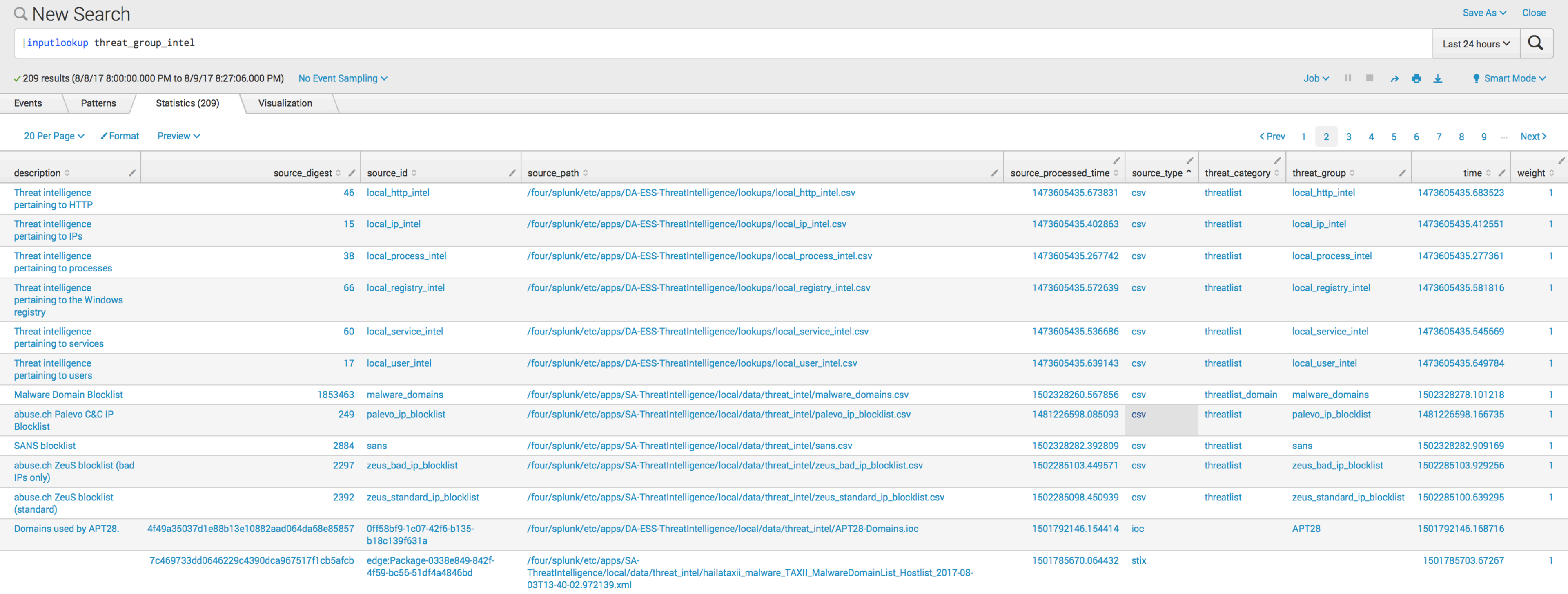
Threat Collections

Stored in KVStore

- Accessible via |inputlookup or through Threat Artifacts dashboard



threat_group_intel



```
|inputlookup threat_group_intel
```

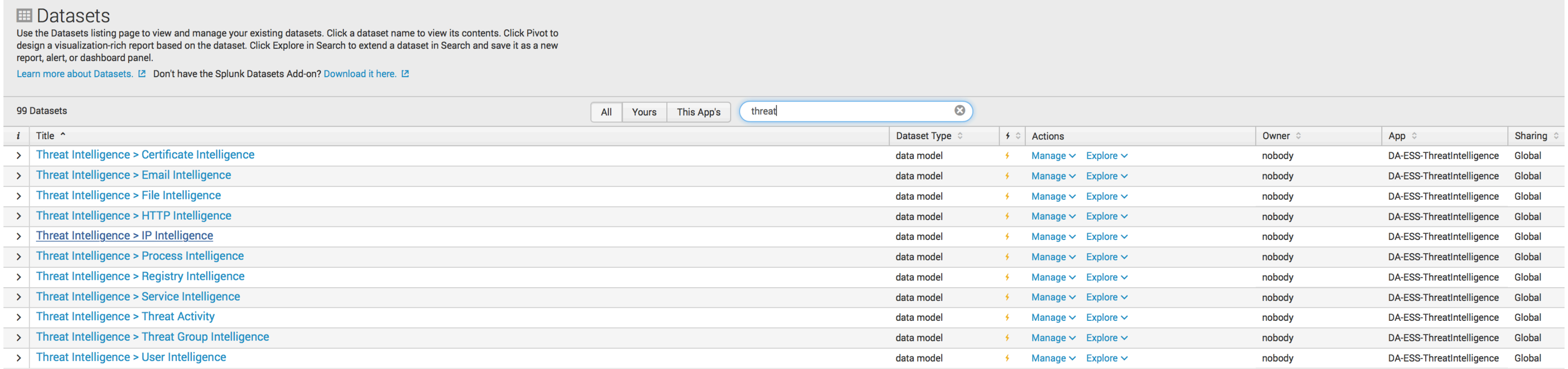
✓ 209 results (8/8/17 8:00:00.000 PM to 8/9/17 8:27:06.000 PM) No Event Sampling

description	source_digest	source_id	source_path	source_processed_time	source_type	threat_category	threat_group	time	weight
Threat intelligence pertaining to HTTP	46	local_http_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_http_intel.csv	1473605435.673831	csv	threatlist	local_http_intel	1473605435.683523	1
Threat intelligence pertaining to IPs	15	local_ip_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_ip_intel.csv	1473605435.402863	csv	threatlist	local_ip_intel	1473605435.412551	1
Threat intelligence pertaining to processes	38	local_process_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_process_intel.csv	1473605435.267742	csv	threatlist	local_process_intel	1473605435.277361	1
Threat intelligence pertaining to the Windows registry	66	local_registry_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_registry_intel.csv	1473605435.572639	csv	threatlist	local_registry_intel	1473605435.581816	1
Threat intelligence pertaining to services	60	local_service_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_service_intel.csv	1473605435.536686	csv	threatlist	local_service_intel	1473605435.545669	1
Threat intelligence pertaining to users	17	local_user_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_user_intel.csv	1473605435.639143	csv	threatlist	local_user_intel	1473605435.649784	1
Malware Domain Blocklist	1853463	malware_domains	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	1502328260.567856	csv	threatlist_domain	malware_domains	1502328278.101218	1
abuse.ch Palevo C&C IP Blocklist	249	palevo_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/palevo_ip_blocklist.csv	1481226598.085093	csv	threatlist	palevo_ip_blocklist	1481226598.166735	1
SANS blocklist	2884	sans	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/sans.csv	1502328282.392809	csv	threatlist	sans	1502328282.909169	1
abuse.ch ZeuS blocklist (bad IPs only)	2297	zeus_bad_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/zeus_bad_ip_blocklist.csv	1502285103.449571	csv	threatlist	zeus_bad_ip_blocklist	1502285103.929256	1
abuse.ch ZeuS blocklist (standard)	2392	zeus_standard_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/zeus_standard_ip_blocklist.csv	1502285098.450939	csv	threatlist	zeus_standard_ip_blocklist	1502285100.639295	1
Domains used by APT28.	4f49a35037d1e88b13e10882aad064da68e85857	0ff58bf9-1c07-42f6-b135-b18c139f631a	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/APT28-Domains.ioc	1501792146.154414	ioc		APT28	1501792146.168716	
	7c469733dd0646229c4390dca967517f1cb5afcb	edge:Package-0338e849-842f-4f59-bc56-51df4a4846bd	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/hailataxii_malware_TAXII_MalwareDomainList_Hostlist_2017-08-03T13-40-02.972139.xml	1501785670.064432	stix			1501785703.67267	1

splunk> .conf2017

Datasets and Datamodels

- Base search is based on lookup *_intel – i.e. Process Intelligence
  - Exception: IP Intelligence
    - ip_intel lookup + ip location



Datasets

Use the Datasets listing page to view and manage your existing datasets. Click a dataset name to view its contents. Click Pivot to design a visualization-rich report based on the dataset. Click Explore in Search to extend a dataset in Search and save it as a new report, alert, or dashboard panel.

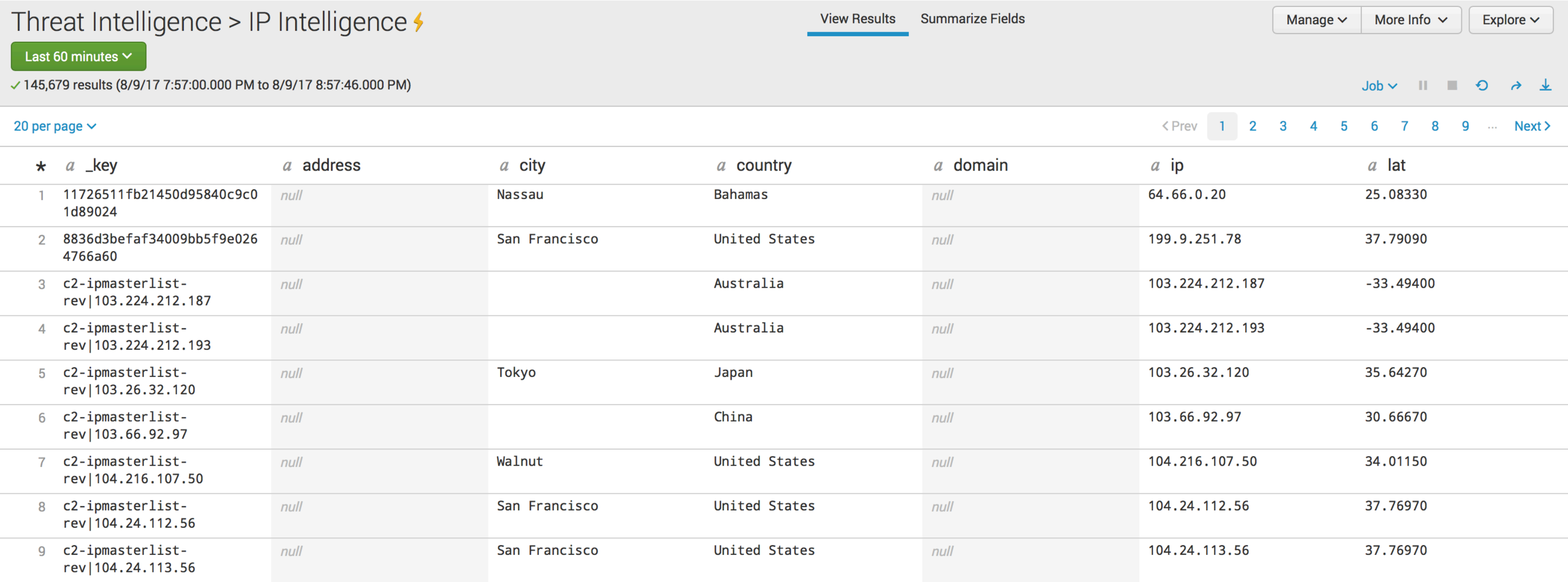
Learn more about Datasets. Don't have the Splunk Datasets Add-on? Download it here.

99 Datasets

i	Title	Dataset Type	⚡	Actions	Owner	App	Sharing
>	Threat Intelligence > Certificate Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Email Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > File Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > HTTP Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > IP Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Process Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Registry Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Service Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Threat Activity	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > Threat Group Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global
>	Threat Intelligence > User Intelligence	data model	⚡	Manage Explore	nobody	DA-ESS-ThreatIntelligence	Global

Datasets and Datamodels

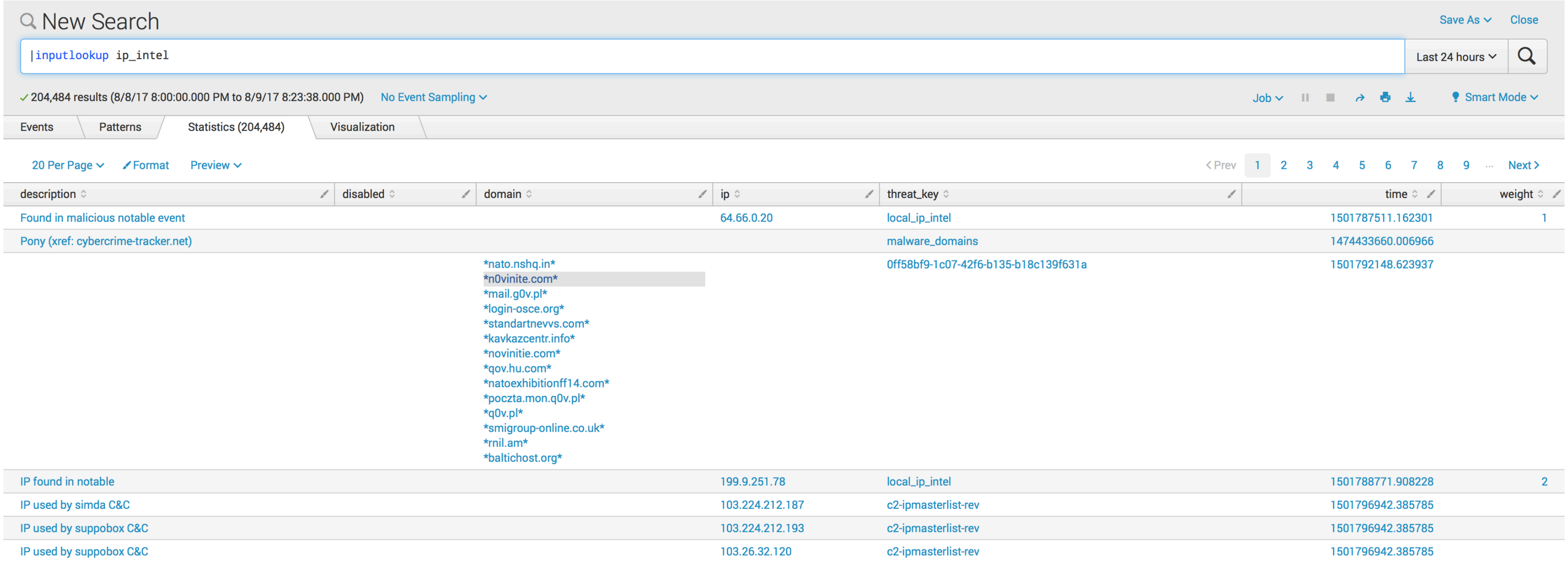
- Just the list of artifacts, nothing actionable



✓ 145,679 results (8/9/17 7:57:00.000 PM to 8/9/17 8:57:46.000 PM)

★	a _key	a address	a city	a country	a domain	a ip	a lat
1	11726511fb21450d95840c9c01d89024	null	Nassau	Bahamas	null	64.66.0.20	25.08330
2	8836d3befaf34009bb5f9e0264766a60	null	San Francisco	United States	null	199.9.251.78	37.79090
3	c2-ipmasterlist-rev|103.224.212.187	null		Australia	null	103.224.212.187	-33.49400
4	c2-ipmasterlist-rev|103.224.212.193	null		Australia	null	103.224.212.193	-33.49400
5	c2-ipmasterlist-rev|103.26.32.120	null	Tokyo	Japan	null	103.26.32.120	35.64270
6	c2-ipmasterlist-rev|103.66.92.97	null		China	null	103.66.92.97	30.66670
7	c2-ipmasterlist-rev|104.216.107.50	null	Walnut	United States	null	104.216.107.50	34.01150
8	c2-ipmasterlist-rev|104.24.112.56	null	San Francisco	United States	null	104.24.112.56	37.76970
9	c2-ipmasterlist-rev|104.24.113.56	null	San Francisco	United States	null	104.24.113.56	37.76970

ip_intel

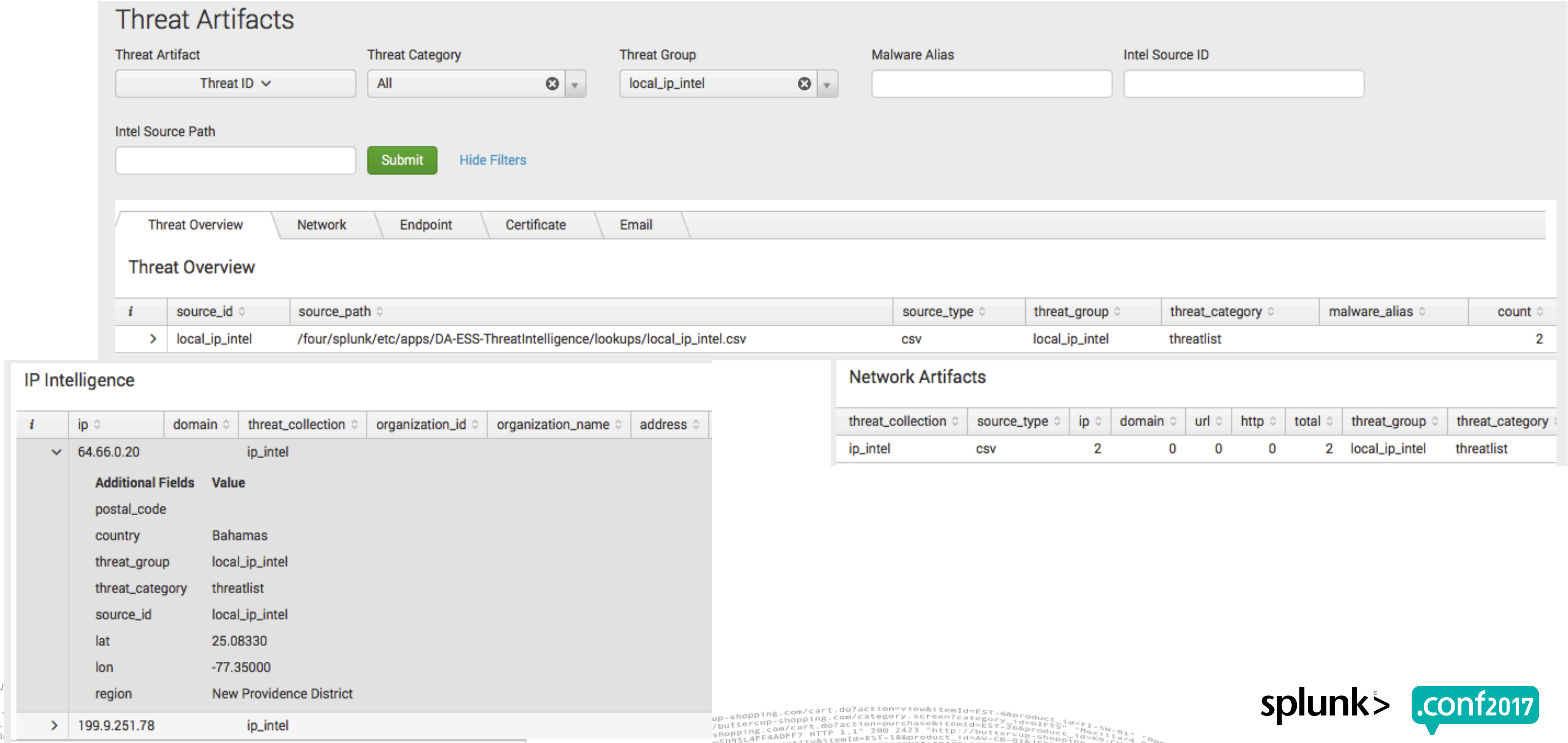


```
|inputlookup ip_intel
```

✓ 204,484 results (8/8/17 8:00:00.000 PM to 8/9/17 8:23:38.000 PM)

description	disabled	domain	ip	threat_key	time	weight
Found in malicious notable event			64.66.0.20	local_ip_intel	1501787511.162301	1
Pony (xref: cybercrime-tracker.net)				malware_domains	1474433660.006966	
		nato.nshq.in *n0vinite.com* *mail.g0v.pl* *login-osce.org* *standartnevvs.com* *kavkazcentr.info* *novinitie.com* *qov.hu.com* *natoexhibitionff14.com* *poczta.mon.q0v.pl* *q0v.pl* *smigroup-online.co.uk* *rnil.am* *baltichost.org*		0ff58bf9-1c07-42f6-b135-b18c139f631a	1501792148.623937	
IP found in notable			199.9.251.78	local_ip_intel	1501788771.908228	2
IP used by simda C&C			103.224.212.187	c2-ipmasterlist-rev	1501796942.385785	
IP used by suppobox C&C			103.224.212.193	c2-ipmasterlist-rev	1501796942.385785	
IP used by suppobox C&C			103.26.32.120	c2-ipmasterlist-rev	1501796942.385785	

Threat Artifacts Dashboard



Threat Artifacts

Threat Artifact: Threat ID

Threat Category: All

Threat Group: local_ip_intel

Malware Alias:

Intel Source ID:

Intel Source Path:

Threat Overview

i	source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
>	local_ip_intel	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/lookups/local_ip_intel.csv	csv	local_ip_intel	threatlist		2

IP Intelligence

i	ip	domain	threat_collection	organization_id	organization_name	address
⌄	64.66.0.20		ip_intel			
>	199.9.251.78		ip_intel			

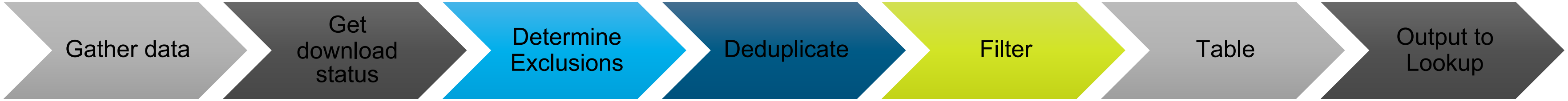
Additional Fields	Value
postal_code	
country	Bahamas
threat_group	local_ip_intel
threat_category	threatlist
source_id	local_ip_intel
lat	25.08330
lon	-77.35000
region	New Providence District

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category
ip_intel	csv	2	0	0	0	2	local_ip_intel	threatlist

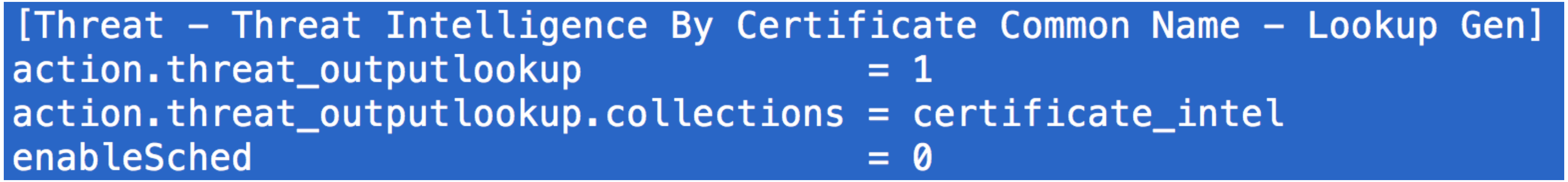
Lookup Generation Process

- | `process_intel` | `threatintel_outputlookup_wildcard(process)`



- Output files are file based not found in KVStore

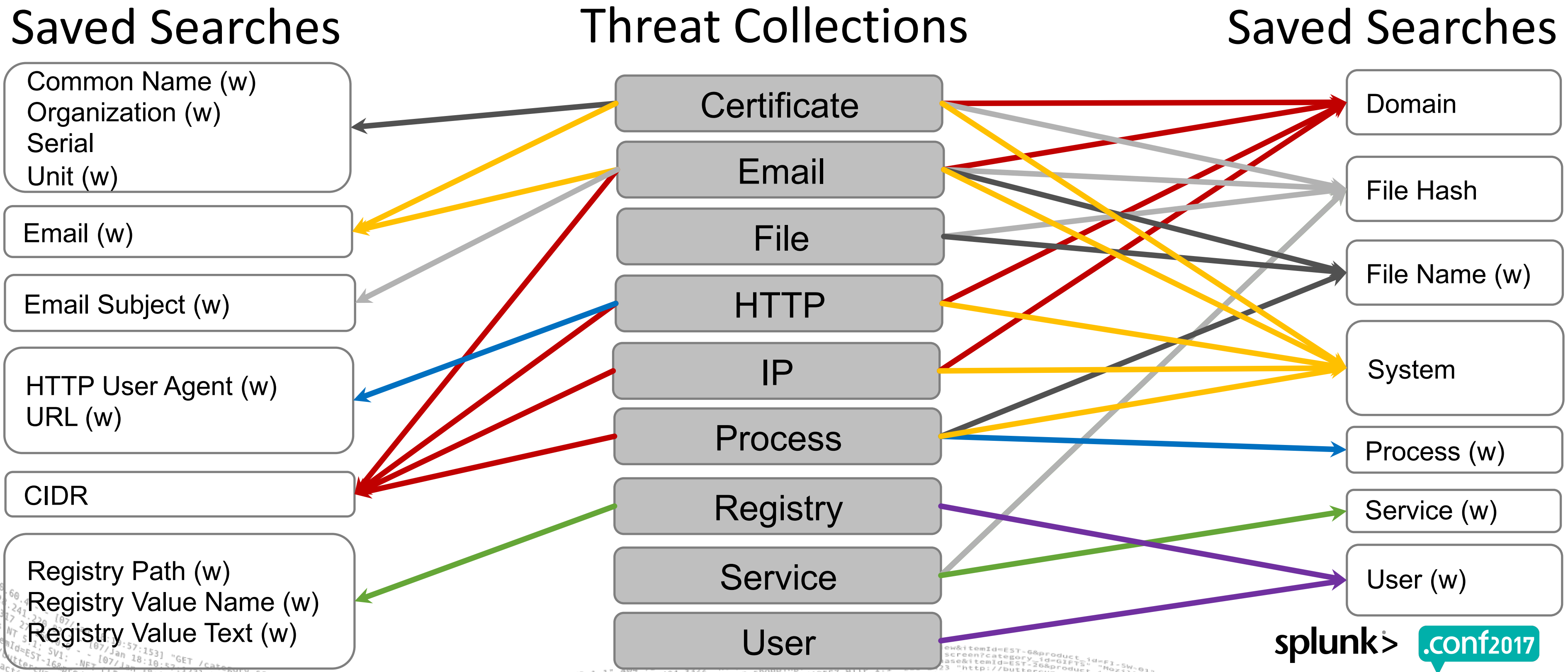
  $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/lookups/
  threatintel_by_process_wildcard.csv



```
[Threat - Threat Intelligence By Certificate Common Name - Lookup Gen]
action.threat_outputlookup             = 1
action.threat_outputlookup.collections = certificate_intel
enableSched                            = 0
```

Lookup Generating Searches

Threat - Threat Intelligence By <insert> - Lookup Gen



Saved Searches

Common Name (w)
Organization (w)
Serial
Unit (w)

Email (w)

Email Subject (w)

HTTP User Agent (w)
URL (w)

CIDR

Registry Path (w)
Registry Value Name (w)
Registry Value Text (w)

Threat Collections

Certificate

Email

File

HTTP

IP

Process

Registry

Service

User

Saved Searches

Domain

File Hash

File Name (w)

System

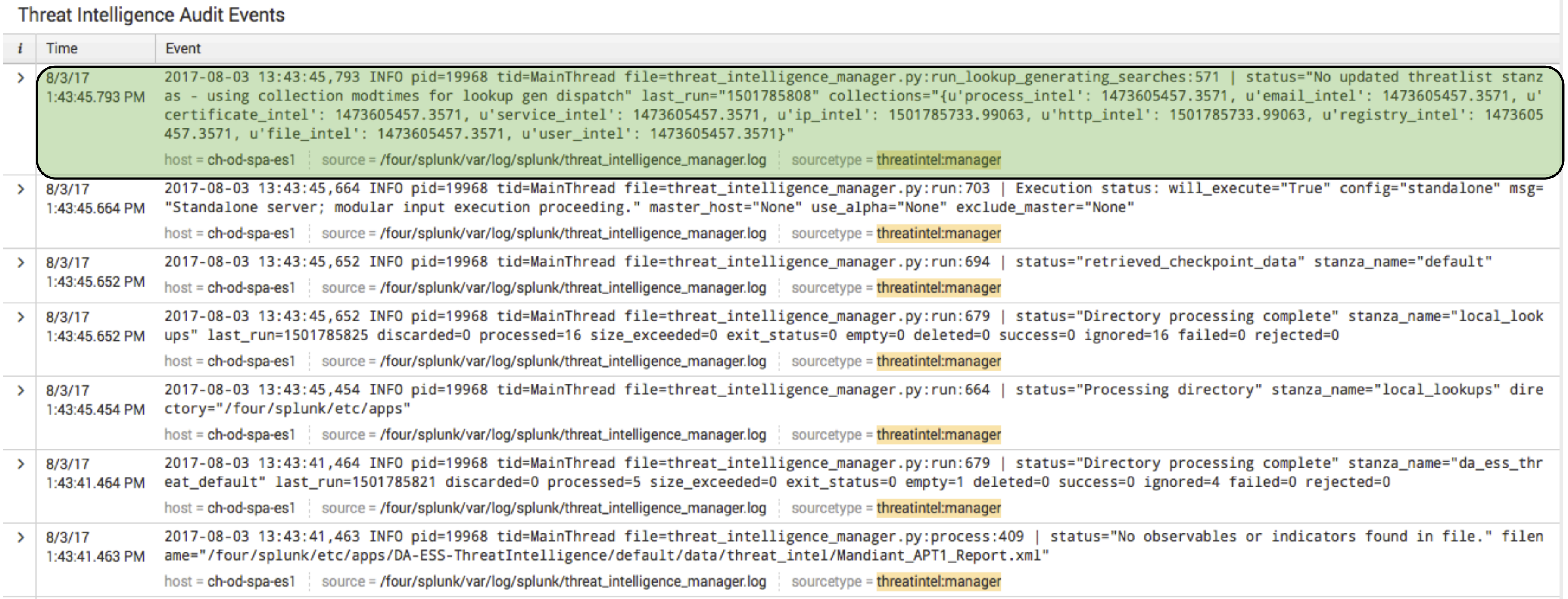
Process (w)

Service (w)

User (w)

When Nothing New Is Coming In

Audit

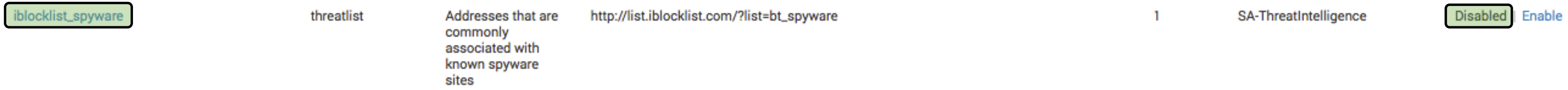


Threat Intelligence Audit Events

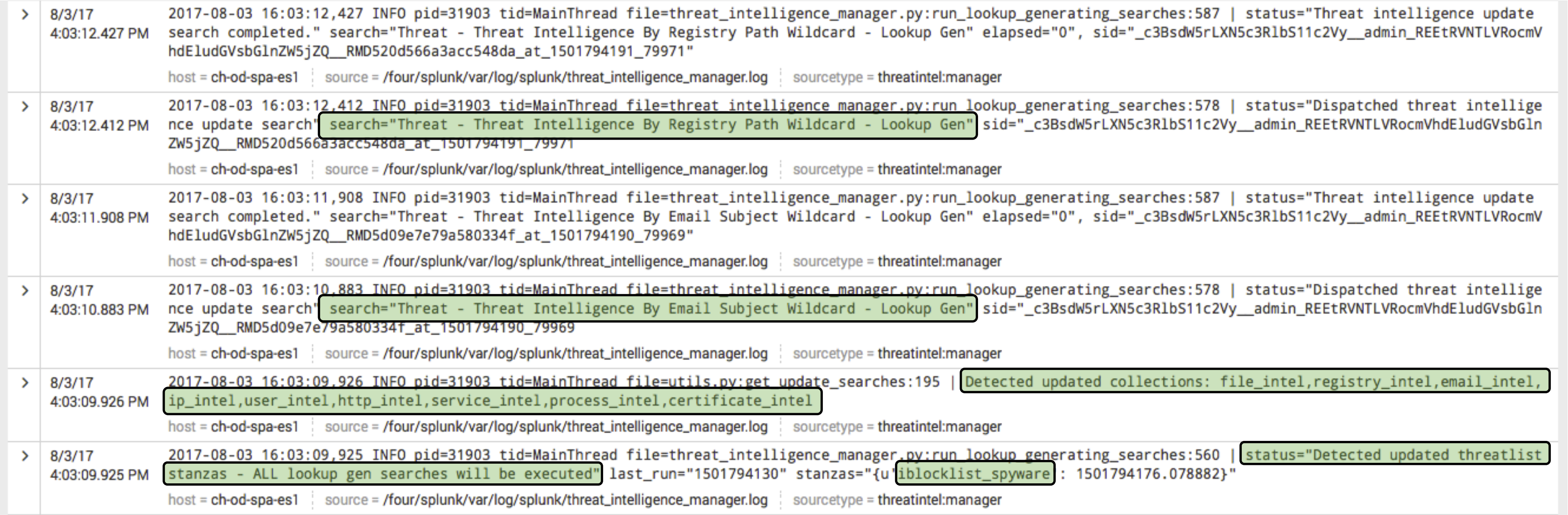
i	Time	Event
>	8/3/17 1:43:45.793 PM	2017-08-03 13:43:45,793 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:571 | status="No updated threatlist stanzas - using collection modtimes for lookup gen dispatch" last_run="1501785808" collections="{u'process_intel': 1473605457.3571, u'email_intel': 1473605457.3571, u'certificate_intel': 1473605457.3571, u'service_intel': 1473605457.3571, u'ip_intel': 1501785733.99063, u'http_intel': 1501785733.99063, u'registry_intel': 1473605457.3571, u'file_intel': 1473605457.3571, u'user_intel': 1473605457.3571}" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:45.664 PM	2017-08-03 13:43:45,664 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:703 | Execution status: will_execute="True" config="standalone" msg="Standalone server; modular input execution proceeding." master_host="None" use_alpha="None" exclude_master="None" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:45.652 PM	2017-08-03 13:43:45,652 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:694 | status="retrieved_checkpoint_data" stanza_name="default" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:45.652 PM	2017-08-03 13:43:45,652 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="local_lookups" last_run=1501785825 discarded=0 processed=16 size_exceeded=0 exit_status=0 empty=0 deleted=0 success=0 ignored=16 failed=0 rejected=0 host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:45.454 PM	2017-08-03 13:43:45,454 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:664 | status="Processing directory" stanza_name="local_lookups" directory="/four/splunk/etc/apps" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:41.464 PM	2017-08-03 13:43:41,464 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:679 | status="Directory processing complete" stanza_name="da_ess_threat_default" last_run=1501785821 discarded=0 processed=5 size_exceeded=0 exit_status=0 empty=1 deleted=0 success=0 ignored=4 failed=0 rejected=0 host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
>	8/3/17 1:43:41.463 PM	2017-08-03 13:43:41,463 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:process:409 | status="No observables or indicators found in file." filename="/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Mandiant_APT1_Report.xml" host = ch-od-spa-es1 source = /four/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager

Disabled Threat Intel Download Feed

Lookup Generation Gets Recomputed



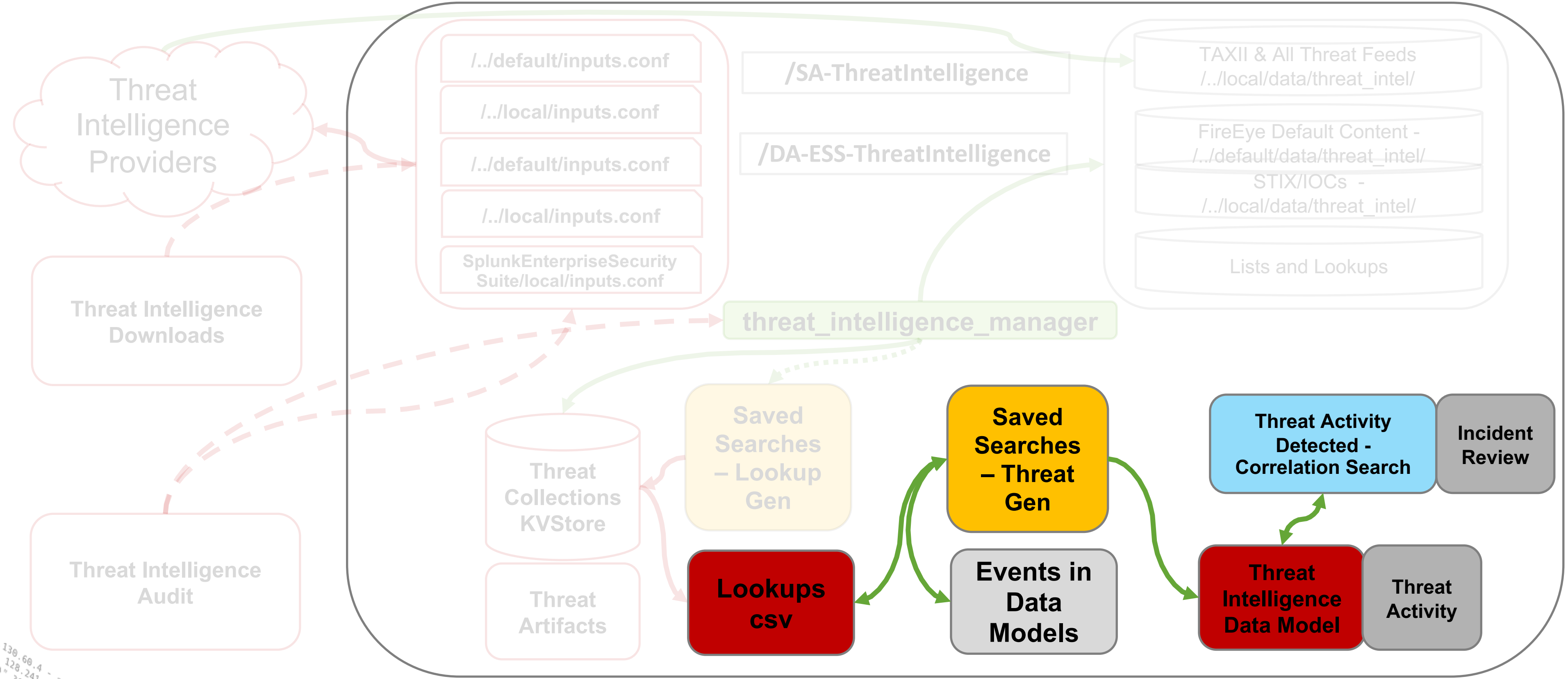
iblocklist_spyware	threatlist	Addresses that are commonly associated with known spyware sites	http://list.iblocklist.com/?list=bt_spyware	1	SA-ThreatIntelligence	Disabled Enable



```
> 8/3/17          2017-08-03 16:03:12,427 INFO pid=31903 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:587 | status="Threat intelligence update
  4:03:12.427 PM  search completed." search="Threat - Threat Intelligence By Registry Path Wildcard - Lookup Gen" elapsed="0", sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmV
                  hdEludGVsbGlnZW5jZQ__RMD520d566a3acc548da_at_1501794191_79971"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:03:12,412 INFO pid=31903 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:578 | status="Dispatched threat intellige
  4:03:12.412 PM  nce update search" search="Threat - Threat Intelligence By Registry Path Wildcard - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmVhdEludGVsbGln
                  ZW5jZQ__RMD520d566a3acc548da_at_1501794191_79971"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:03:11,908 INFO pid=31903 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:587 | status="Threat intelligence update
  4:03:11.908 PM  search completed." search="Threat - Threat Intelligence By Email Subject Wildcard - Lookup Gen" elapsed="0", sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmV
                  hdEludGVsbGlnZW5jZQ__RMD5d09e7e79a580334f_at_1501794190_79969"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:03:10,883 INFO pid=31903 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:578 | status="Dispatched threat intellige
  4:03:10.883 PM  nce update search" search="Threat - Threat Intelligence By Email Subject Wildcard - Lookup Gen" sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmVhdEludGVsbGln
                  ZW5jZQ__RMD5d09e7e79a580334f_at_1501794190_79969
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:03:09,926 INFO pid=31903 tid=MainThread file=utils.py:get_update_searches:195 | Detected updated collections: file_intel,registry_intel,email_intel,
  4:03:09.926 PM  ip_intel,user_intel,http_intel,service_intel,process_intel,certificate_intel
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

> 8/3/17          2017-08-03 16:03:09,925 INFO pid=31903 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:560 | status="Detected updated threatlist
  4:03:09.925 PM  stanzas - ALL lookup gen searches will be executed" last_run="1501794130" stanzas="{u'iblocklist_spyware': 1501794176.078882}"
                  host = ch-od-spa-es1 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
```

Action

Action



Threat Intelligence Providers

/../default/inputs.conf

/../local/inputs.conf

/../default/inputs.conf

/../local/inputs.conf

SplunkEnterpriseSecuritySuite/local/inputs.conf

/SA-ThreatIntelligence

/DA-ESS-ThreatIntelligence

TAXII & All Threat Feeds /../local/data/threat_intel/

FireEye Default Content - /../default/data/threat_intel/

STIX/IOCs - /../local/data/threat_intel/

Lists and Lookups

Threat Intelligence Downloads

threat_intelligence_manager

Threat Collections KVStore

Saved Searches – Lookup Gen

Saved Searches – Threat Gen

Threat Activity Detected - Correlation Search

Incident Review

Threat Artifacts

Lookups csv

Events in Data Models

Threat Intelligence Data Model

Threat Activity

Threat Intelligence Audit

Threat Generation Saved Searches

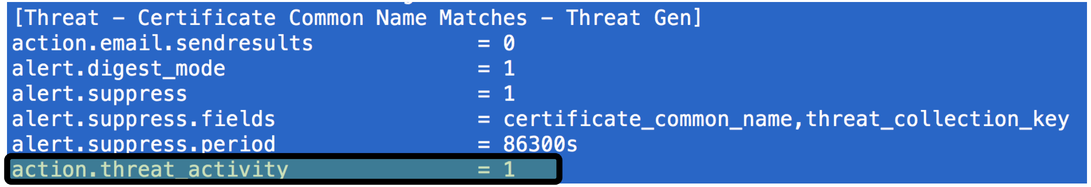
DA-ESS-ThreatIntelligence/default/savedsearches.conf

Threat Match	cron	Data Model
certificate_common_name	0,30 * * * *	Certificates
certificate_organization	5,35 * * * *	Certificates
certificate_serial	10,40 * * * *	Certificates
certificate_unit	15,45 * * * *	Certificates
email	20,50 * * * *	Certificates, Email
subject	25,55 * * * *	Email
file_hash	0,30 * * * *	Certificates, Change_Analysis, Email, Malware, Updates
file_name	5,35 * * * *	Change_Analysis, Email, Malware, Updates
http_user_agent	10,40 * * * *	Web

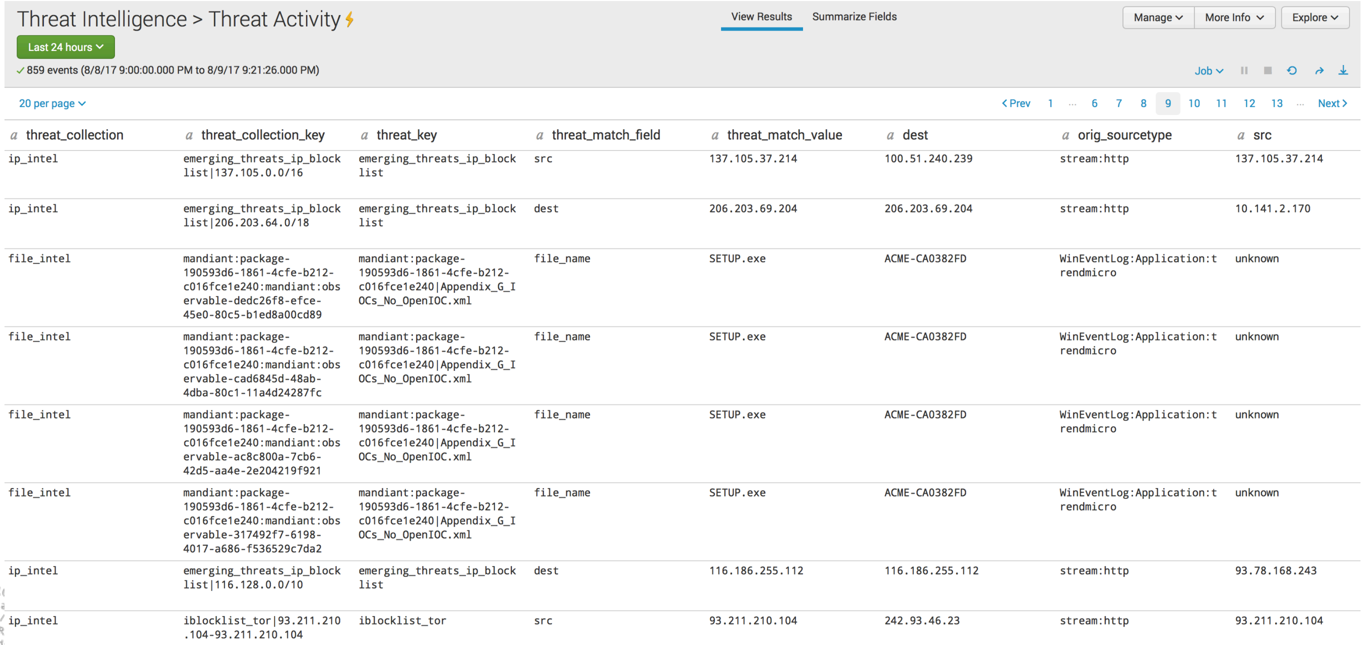
Threat Match	cron	Data Model
query	15,45 * * * *	Network_Resolution, Domain_Analysis
process	20,50 * * * *	Application_State
registry_path	25,55 * * * *	sourcetype=WinRegistry
registry_value_name	0,30 * * * *	sourcetype=WinRegistry
registry_value_text	5,35 * * * *	sourcetype=WinRegistry
service	10,40 * * * *	Application_State
src, dest	15,45 * * * *	Network_Traffic, Intrusion_Detection, Web
url	20,50 * * * *	Web
user	25,55 * * * *	Authentication, Inventory, Web

Threat Activity Data Model

- index=threat_activity
- Populated from Threat Gen saved searches



```
[Threat - Certificate Common Name Matches - Threat Gen]
action.email.sendresults                = 0
alert.digest_mode                       = 1
alert.suppress                          = 1
alert.suppress.fields                   = certificate_common_name,threat_collection_key
alert.suppress.period                   = 86300s
action.threat_activity                  = 1
```

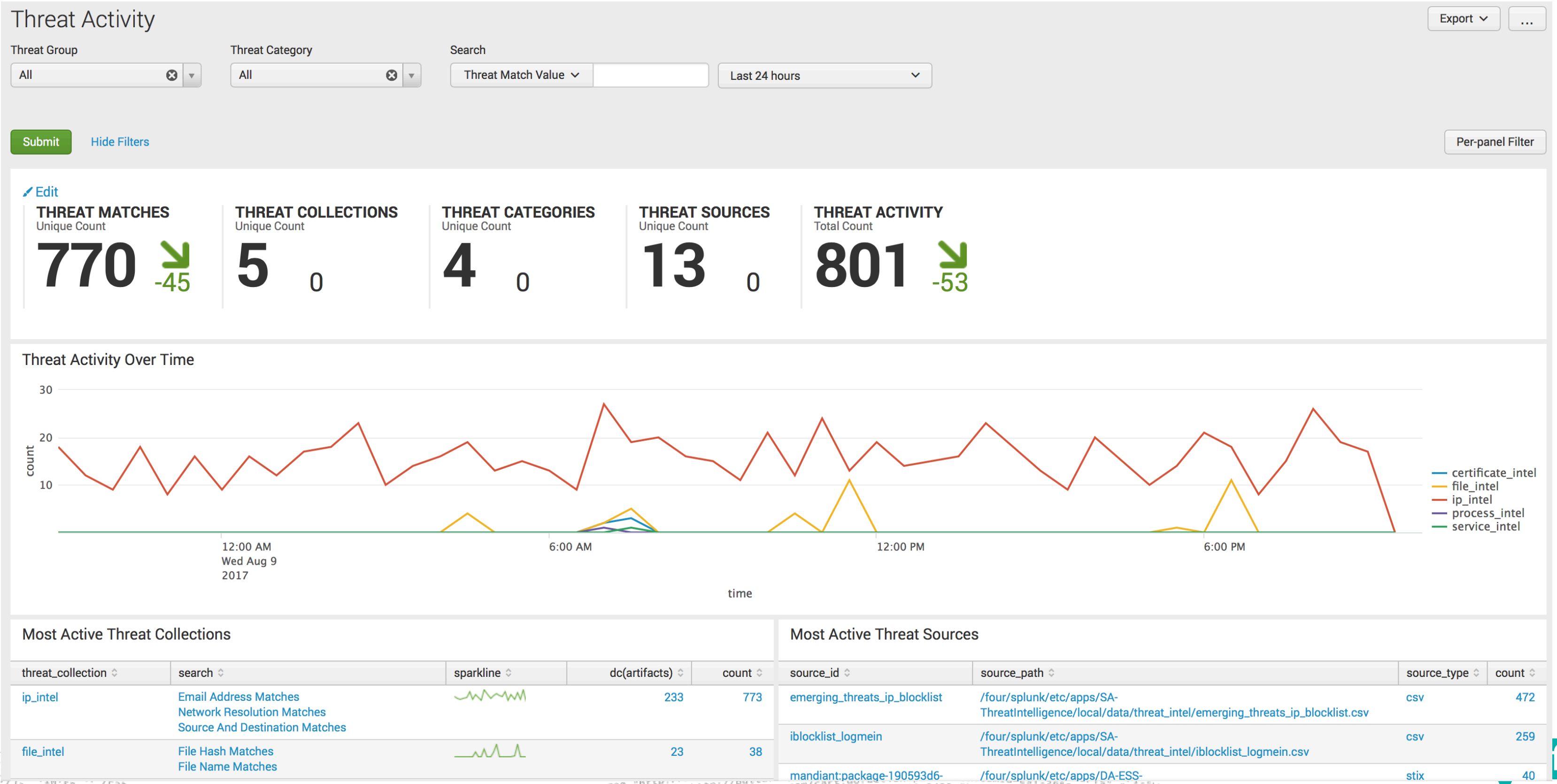


Threat Intelligence > Threat Activity
View Results
Summarize Fields
Manage
More Info
Explore
Last 24 hours
Job
20 per page
< Prev 1 ... 6 7 8 9 10 11 12 13 ... Next >

✓ 859 events (8/8/17 9:00:00.000 PM to 8/9/17 9:21:26.000 PM)

threat_collection	threat_collection_key	threat_key	threat_match_field	threat_match_value	dest	orig_sourcetype	src
ip_intel	emerging_threats_ip_blocklist|137.105.0.0/16	emerging_threats_ip_blocklist	src	137.105.37.214	100.51.240.239	stream:http	137.105.37.214
ip_intel	emerging_threats_ip_blocklist|206.203.64.0/18	emerging_threats_ip_blocklist	dest	206.203.69.204	206.203.69.204	stream:http	10.141.2.170
file_intel	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240:mandiant:observable-dedc26f8-efce-45e0-80c5-b1ed8a00cd89	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240|Appendix_G_IOCs_No_OpenIOC.xml	file_name	SETUP.exe	ACME-CA0382FD	WinEventLog:Application:trendmicro	unknown
file_intel	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240:mandiant:observable-cad6845d-48ab-4dba-80c1-11a4d24287fc	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240|Appendix_G_IOCs_No_OpenIOC.xml	file_name	SETUP.exe	ACME-CA0382FD	WinEventLog:Application:trendmicro	unknown
file_intel	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240:mandiant:observable-ac8c800a-7cb6-42d5-aa4e-2e204219f921	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240|Appendix_G_IOCs_No_OpenIOC.xml	file_name	SETUP.exe	ACME-CA0382FD	WinEventLog:Application:trendmicro	unknown
file_intel	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240:mandiant:observable-317492f7-6198-4017-a686-f536529c7da2	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240|Appendix_G_IOCs_No_OpenIOC.xml	file_name	SETUP.exe	ACME-CA0382FD	WinEventLog:Application:trendmicro	unknown
ip_intel	emerging_threats_ip_blocklist|116.128.0.0/10	emerging_threats_ip_blocklist	dest	116.186.255.112	116.186.255.112	stream:http	93.78.168.243
ip_intel	iblocklist_tor|93.211.210.104-93.211.210.104	iblocklist_tor	src	93.211.210.104	242.93.46.23	stream:http	93.211.210.104

Threat Dashboard Activity



Threat Activity

Threat Group: All

Threat Category: All

Search: Threat Match Value

Last 24 hours

THREAT MATCHES Unique Count	THREAT COLLECTIONS Unique Count	THREAT CATEGORIES Unique Count	THREAT SOURCES Unique Count	THREAT ACTIVITY Total Count
770 ↘ -45	5 0	4 0	13 0	801 ↘ -53

Threat Activity Over Time

Most Active Threat Collections

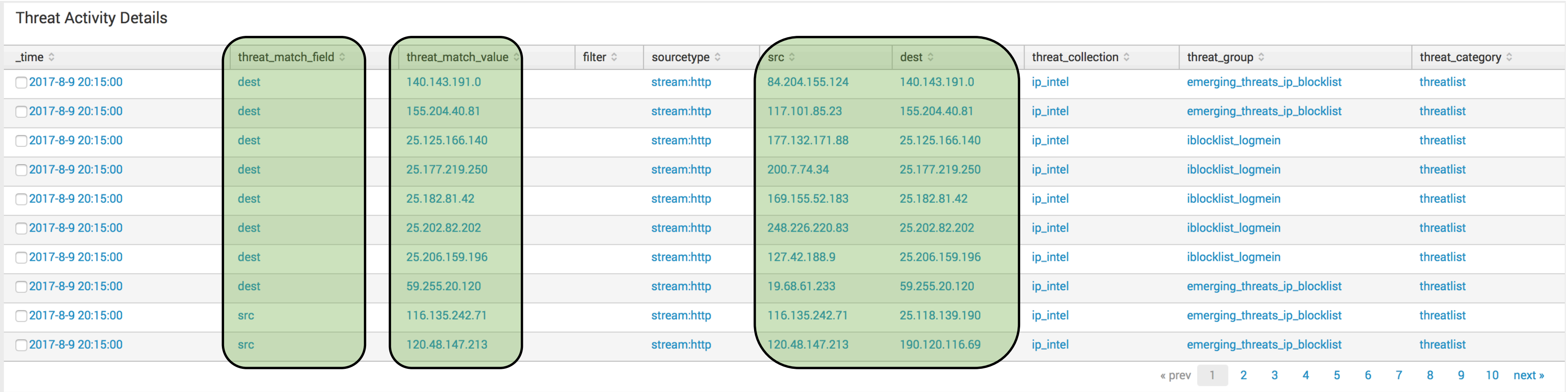
threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		233	773
file_intel	File Hash Matches File Name Matches		23	38

Most Active Threat Sources

source_id	source_path	source_type	count
emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	472
iblocklist_logmein	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	259
mandiant:package-190593d6-	/four/splunk/etc/apps/DA-ESS-	stix	40

Threat Dashboard Activity

Details

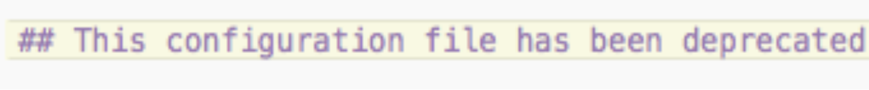


Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
□ 2017-8-9 20:15:00	dest	140.143.191.0		stream:http	84.204.155.124	140.143.191.0	ip_intel	emerging_threats_ip_blocklist	threatlist
□ 2017-8-9 20:15:00	dest	155.204.40.81		stream:http	117.101.85.23	155.204.40.81	ip_intel	emerging_threats_ip_blocklist	threatlist
□ 2017-8-9 20:15:00	dest	25.125.166.140		stream:http	177.132.171.88	25.125.166.140	ip_intel	iblocklist_logmein	threatlist
□ 2017-8-9 20:15:00	dest	25.177.219.250		stream:http	200.7.74.34	25.177.219.250	ip_intel	iblocklist_logmein	threatlist
□ 2017-8-9 20:15:00	dest	25.182.81.42		stream:http	169.155.52.183	25.182.81.42	ip_intel	iblocklist_logmein	threatlist
□ 2017-8-9 20:15:00	dest	25.202.82.202		stream:http	248.226.220.83	25.202.82.202	ip_intel	iblocklist_logmein	threatlist
□ 2017-8-9 20:15:00	dest	25.206.159.196		stream:http	127.42.188.9	25.206.159.196	ip_intel	iblocklist_logmein	threatlist
□ 2017-8-9 20:15:00	dest	59.255.20.120		stream:http	19.68.61.233	59.255.20.120	ip_intel	emerging_threats_ip_blocklist	threatlist
□ 2017-8-9 20:15:00	src	116.135.242.71		stream:http	116.135.242.71	25.118.139.190	ip_intel	emerging_threats_ip_blocklist	threatlist
□ 2017-8-9 20:15:00	src	120.48.147.213		stream:http	120.48.147.213	190.120.116.69	ip_intel	emerging_threats_ip_blocklist	threatlist

Search Correlations

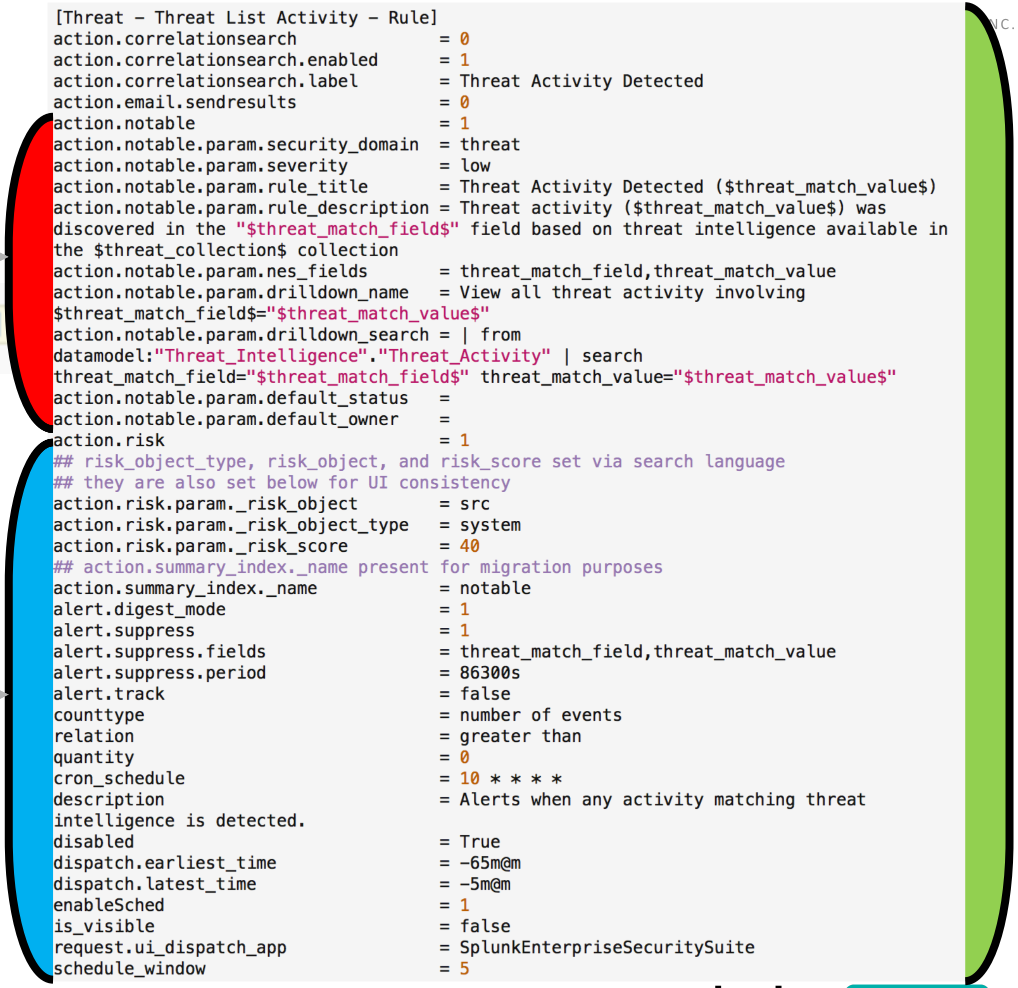
- correlationsearches.conf



```
## This configuration file has been deprecated
```

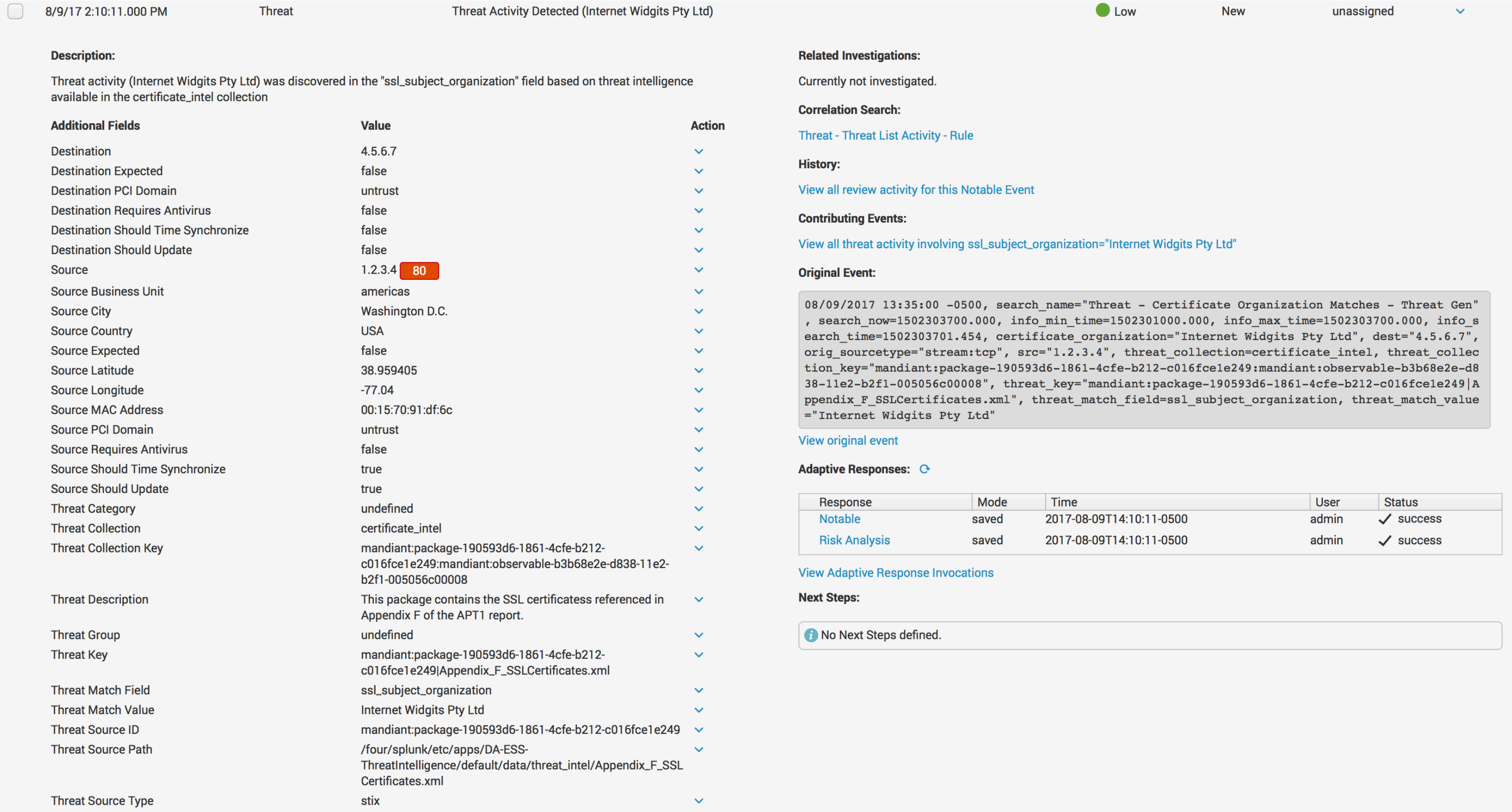
- In ES 4.6, savedsearches.conf contains all configuration values

- savedsearches.conf



```
[Threat - Threat List Activity - Rule]
action.correlationsearch                   = 0
action.correlationsearch.enabled           = 1
action.correlationsearch.label             = Threat Activity Detected
action.email.sendresults                   = 0
action.notable                             = 1
action.notable.param.security_domain       = threat
action.notable.param.severity              = low
action.notable.param.rule_title            = Threat Activity Detected ($threat_match_value$)
action.notable.param.rule_description = Threat activity ($threat_match_value$) was
discovered in the "$threat_match_field$" field based on threat intelligence available in
the $threat_collection$ collection
action.notable.param.nes_fields            = threat_match_field,threat_match_value
action.notable.param.drilldown_name        = View all threat activity involving
$threat_match_field$="$threat_match_value$"
action.notable.param.drilldown_search = | from
datamodel:"Threat_Intelligence"."Threat_Activity" | search
threat_match_field="$threat_match_field$" threat_match_value="$threat_match_value$"
action.notable.param.default_status        =
action.notable.param.default_owner         =
action.risk                                = 1
## risk_object_type, risk_object, and risk_score set via search language
## they are also set below for UI consistency
action.risk.param._risk_object             = src
action.risk.param._risk_object_type        = system
action.risk.param._risk_score              = 40
## action.summary_index._name present for migration purposes
action.summary_index._name                 = notable
alert.digest_mode                          = 1
alert.suppress                             = 1
alert.suppress.fields                      = threat_match_field,threat_match_value
alert.suppress.period                      = 86300s
alert.track                                = false
counttype                                  = number of events
relation                                   = greater than
quantity                                   = 0
cron_schedule                              = 10 * * * *
description                                = Alerts when any activity matching threat
intelligence is detected.
disabled                                   = True
dispatch.earliest_time                     = -65m@m
dispatch.latest_time                       = -5m@m
enableSched                                = 1
is_visible                                 = false
request.ui_dispatch_app                    = SplunkEnterpriseSecuritySuite
schedule_window                            = 5
```

Notable Events



☐ 8/9/17 2:10:11.000 PM | Threat | Threat Activity Detected (Internet Widgits Pty Ltd) | ● Low | New | unassigned ⌄

Description:

Threat activity (Internet Widgits Pty Ltd) was discovered in the "ssl_subject_organization" field based on threat intelligence available in the certificate_intel collection

Additional Fields	Value	Action
Destination	4.5.6.7	⌄
Destination Expected	false	⌄
Destination PCI Domain	untrust	⌄
Destination Requires Antivirus	false	⌄
Destination Should Time Synchronize	false	⌄
Destination Should Update	false	⌄
Source	1.2.3.4 80	⌄
Source Business Unit	americas	⌄
Source City	Washington D.C.	⌄
Source Country	USA	⌄
Source Expected	false	⌄
Source Latitude	38.959405	⌄
Source Longitude	-77.04	⌄
Source MAC Address	00:15:70:91:df:6c	⌄
Source PCI Domain	untrust	⌄
Source Requires Antivirus	false	⌄
Source Should Time Synchronize	true	⌄
Source Should Update	true	⌄
Threat Category	undefined	⌄
Threat Collection	certificate_intel	⌄
Threat Collection Key	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249:mandiant:observable-b3b68e2e-d838-11e2-b2f1-005056c00008	⌄
Threat Description	This package contains the SSL certificatess referenced in Appendix F of the APT1 report.	⌄
Threat Group	undefined	⌄
Threat Key	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249|Appendix_F_SSLCertificates.xml	⌄
Threat Match Field	ssl_subject_organization	⌄
Threat Match Value	Internet Widgits Pty Ltd	⌄
Threat Source ID	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249	⌄
Threat Source Path	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_SSLCertificates.xml	⌄
Threat Source Type	stix	⌄

Related Investigations:

Currently not investigated.

Correlation Search:

Threat - Threat List Activity - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View all threat activity involving ssl_subject_organization="Internet Widgits Pty Ltd"

Original Event:

```
08/09/2017 13:35:00 -0500, search_name="Threat - Certificate Organization Matches - Threat Gen"
, search_now=1502303700.000, info_min_time=1502301000.000, info_max_time=1502303700.000, info_s
earch_time=1502303701.454, certificate_organization="Internet Widgits Pty Ltd", dest="4.5.6.7",
orig_sourcetype="stream:tcp", src="1.2.3.4", threat_collection=certificate_intel, threat_collec
tion_key="mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249:mandiant:observable-b3b68e2e-d8
38-11e2-b2f1-005056c00008", threat_key="mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249|A
ppendix_F_SSLCertificates.xml", threat_match_field=ssl_subject_organization, threat_match_value
="Internet Widgits Pty Ltd"
```

View original event

Adaptive Responses: ⟳

Response	Mode	Time	User	Status
Notable	saved	2017-08-09T14:10:11-0500	admin	✓ success
Risk Analysis	saved	2017-08-09T14:10:11-0500	admin	✓ success

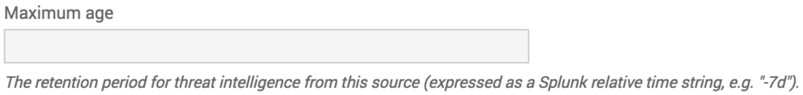
View Adaptive Response Invocations

Next Steps:

ⓘ No Next Steps defined.

Aging Out Threat Intel

- Documentation referenced this first in ES4.0
- Set of 8 Saved Searches
  - Threat - <insert threat group name> Threat Intelligence Retention - Lookup Gen
  - `filter_threatintel_collection("http_intel")`
    - inputlookup $collection$ | `filter_by_threat_age` | outputlookup $collection$ | stats count
  - Disabled by default
- Time Set in Threat Download

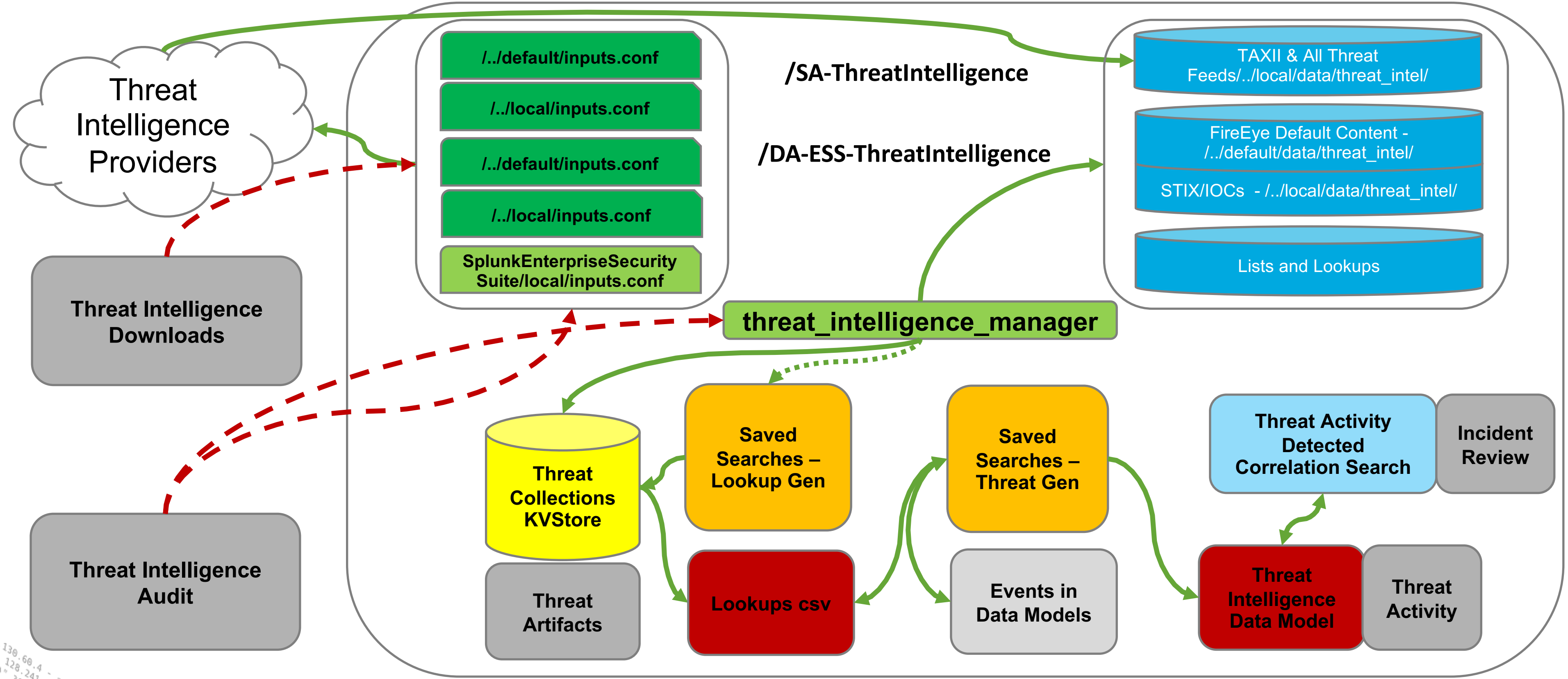


Maximum age

The retention period for threat intelligence from this source (expressed as a Splunk relative time string, e.g. "-7d").

Group	cron
Certificate	0 3 * * *
Email	5 3 * * *
File	10 3 * * *
HTTP	15 3 * * *
IP	20 3 * * *
Process	25 3 * * *
Registry	30 3 * * *
Service	35 3 * * *

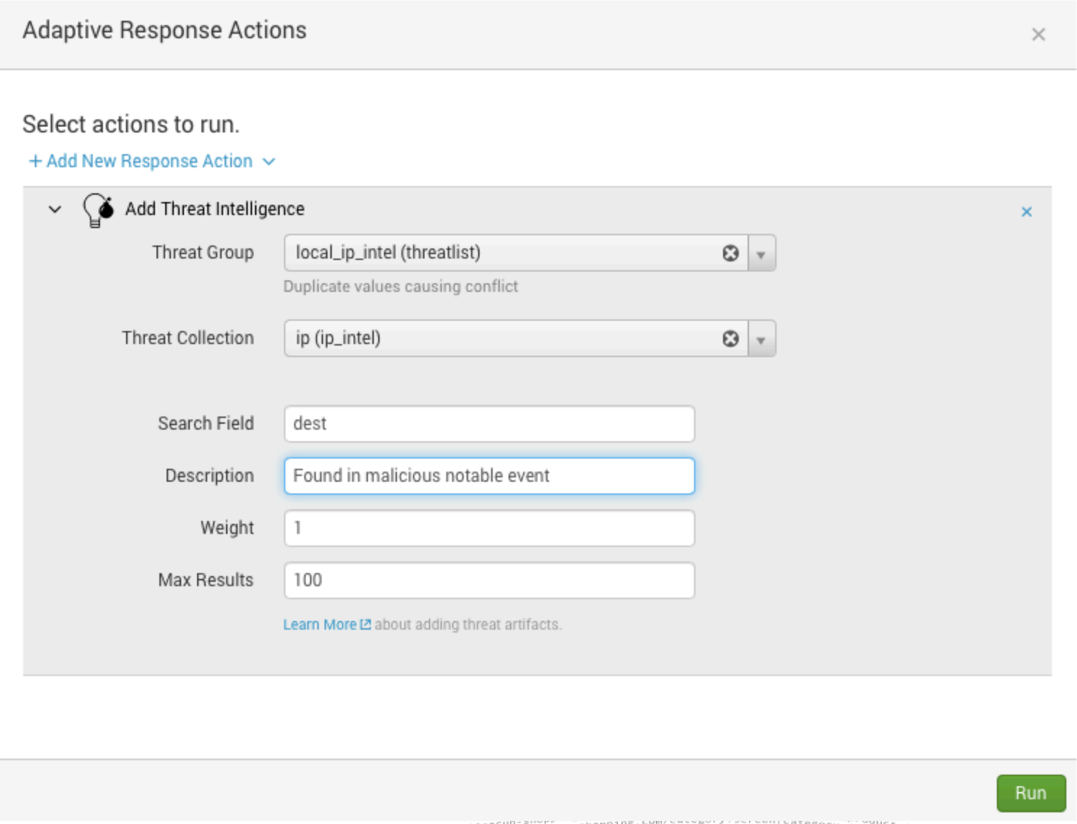
Threat Intel Framework Data Flow


Threat Intelligence Providers
/../default/inputs.conf
/../local/inputs.conf
/../default/inputs.conf
/../local/inputs.conf
SplunkEnterpriseSecuritySuite/local/inputs.conf
/SA-ThreatIntelligence
/DA-ESS-ThreatIntelligence
TAXII & All Threat Feeds/../local/data/threat_intel/
FireEye Default Content - /../default/data/threat_intel/
STIX/IOCs - /../local/data/threat_intel/
Lists and Lookups
Threat Intelligence Downloads
threat_intelligence_manager
Threat Intelligence Audit
Threat Collections KVStore
Threat Artifacts
Saved Searches – Lookup Gen
Lookups csv
Saved Searches – Threat Gen
Events in Data Models
Threat Activity Detected Correlation Search
Incident Review
Threat Intelligence Data Model
Threat Activity

Operationalizing

Operationalizing Threat Indicators

Adaptive Response



Adaptive Response Actions

Select actions to run.

Add Threat Intelligence

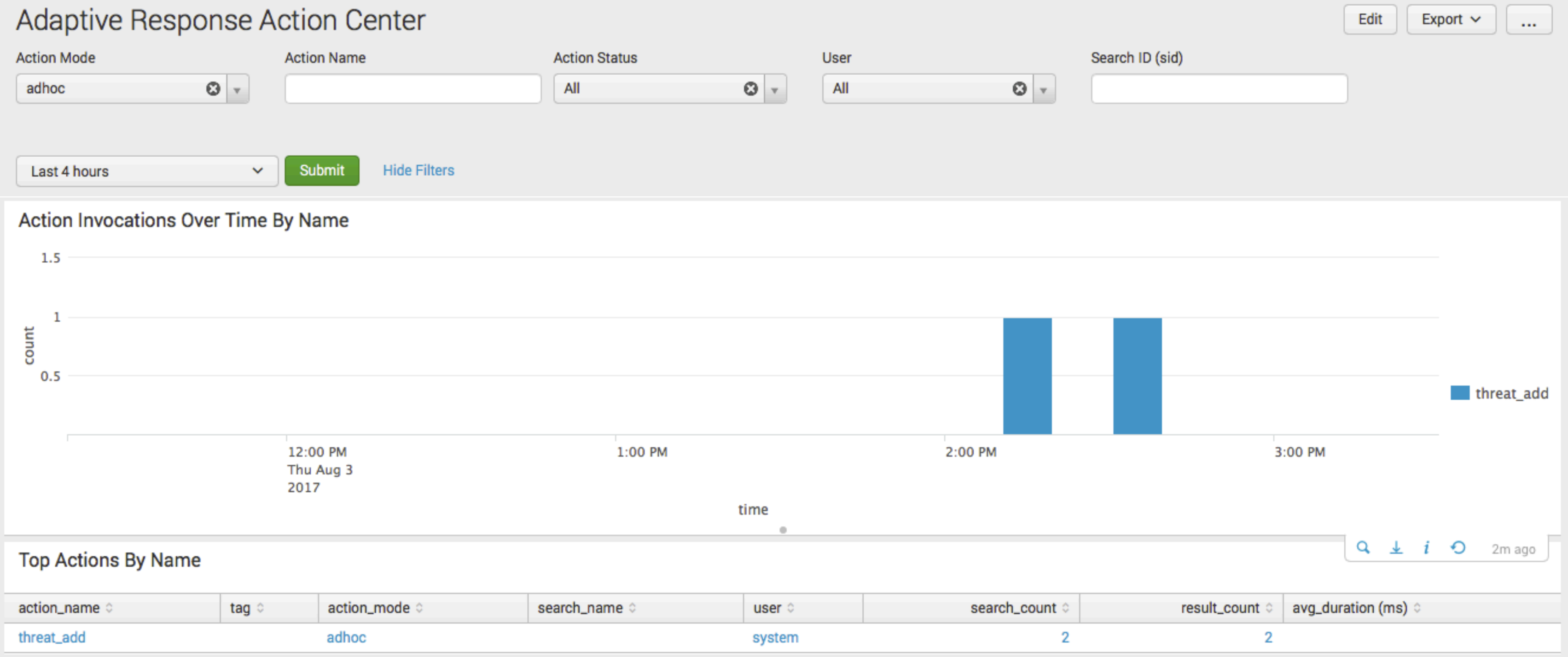
Threat Group	local_ip_intel (threatlist)
	Duplicate values causing conflict
Threat Collection	ip (ip_intel)
Search Field	dest
Description	Found in malicious notable event
Weight	1
Max Results	100

Learn More about adding threat artifacts.

splunk> .conf2017

Adaptive Response

Audit Threat Indicator Actions



Adaptive Response Action Center

Action Mode: adhoc

Action Name:

Action Status: All

User: All

Search ID (sid):

Last 4 hours

Action Invocations Over Time By Name

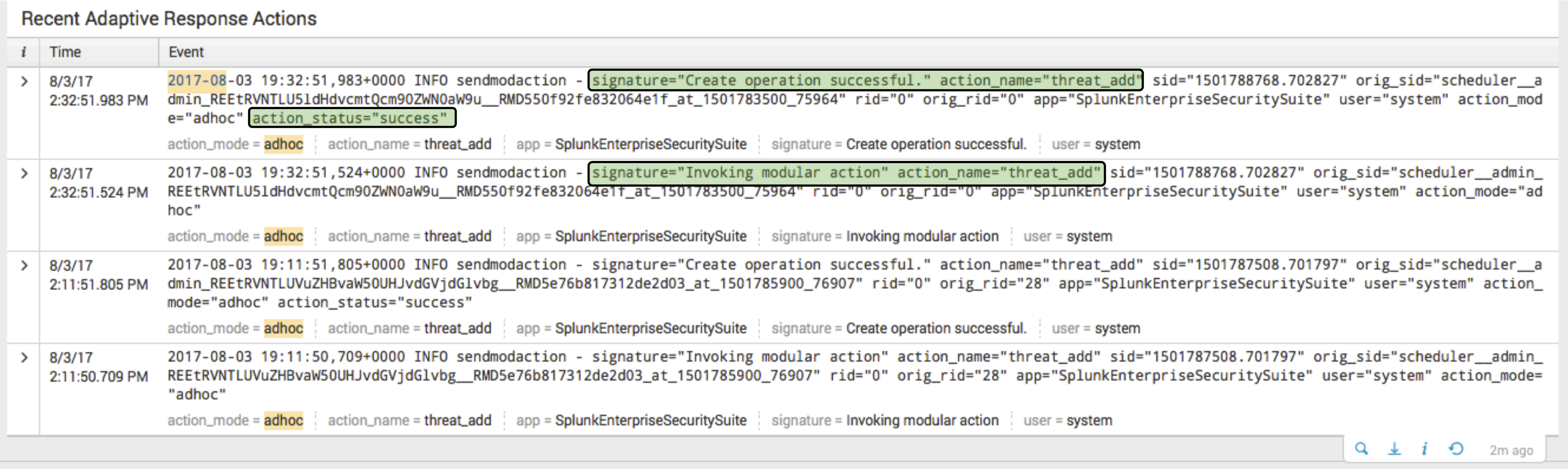
Top Actions By Name

action_name	tag	action_mode	search_name	user	search_count	result_count	avg_duration (ms)
threat_add		adhoc		system	2	2	

splunk> .conf2017

Operationalizing Threat Indicators

Adaptive Response Audit Trail



Recent Adaptive Response Actions

i	Time	Event
>	8/3/17 2:32:51.983 PM	2017-08-03 19:32:51,983+0000 INFO sendmodaction - signature="Create operation successful." action_name="threat_add" sid="1501788768.702827" orig_sid="scheduler__admin_REEtRVNTLU5ldHdvcmtQcm90ZWN0aW9u__RMD550f92fe832064e1f_at_1501783500_75964" rid="0" orig_rid="0" app="SplunkEnterpriseSecuritySuite" user="system" action_mode="adhoc" action_status="success" action_mode = adhoc action_name = threat_add app = SplunkEnterpriseSecuritySuite signature = Create operation successful. user = system
>	8/3/17 2:32:51.524 PM	2017-08-03 19:32:51,524+0000 INFO sendmodaction - signature="Invoking modular action" action_name="threat_add" sid="1501788768.702827" orig_sid="scheduler__admin_REEtRVNTLU5ldHdvcmtQcm90ZWN0aW9u__RMD550f92fe832064e1f_at_1501783500_75964" rid="0" orig_rid="0" app="SplunkEnterpriseSecuritySuite" user="system" action_mode="adhoc" action_mode = adhoc action_name = threat_add app = SplunkEnterpriseSecuritySuite signature = Invoking modular action user = system
>	8/3/17 2:11:51.805 PM	2017-08-03 19:11:51,805+0000 INFO sendmodaction - signature="Create operation successful." action_name="threat_add" sid="1501787508.701797" orig_sid="scheduler__admin_REEtRVNTLUVuZHBvaW50UHJvdGVjdGlvbg__RMD5e76b817312de2d03_at_1501785900_76907" rid="0" orig_rid="28" app="SplunkEnterpriseSecuritySuite" user="system" action_mode="adhoc" action_status="success" action_mode = adhoc action_name = threat_add app = SplunkEnterpriseSecuritySuite signature = Create operation successful. user = system
>	8/3/17 2:11:50.709 PM	2017-08-03 19:11:50,709+0000 INFO sendmodaction - signature="Invoking modular action" action_name="threat_add" sid="1501787508.701797" orig_sid="scheduler__admin_REEtRVNTLUVuZHBvaW50UHJvdGVjdGlvbg__RMD5e76b817312de2d03_at_1501785900_76907" rid="0" orig_rid="28" app="SplunkEnterpriseSecuritySuite" user="system" action_mode="adhoc" action_mode = adhoc action_name = threat_add app = SplunkEnterpriseSecuritySuite signature = Invoking modular action user = system

Threat Intel Framework via API

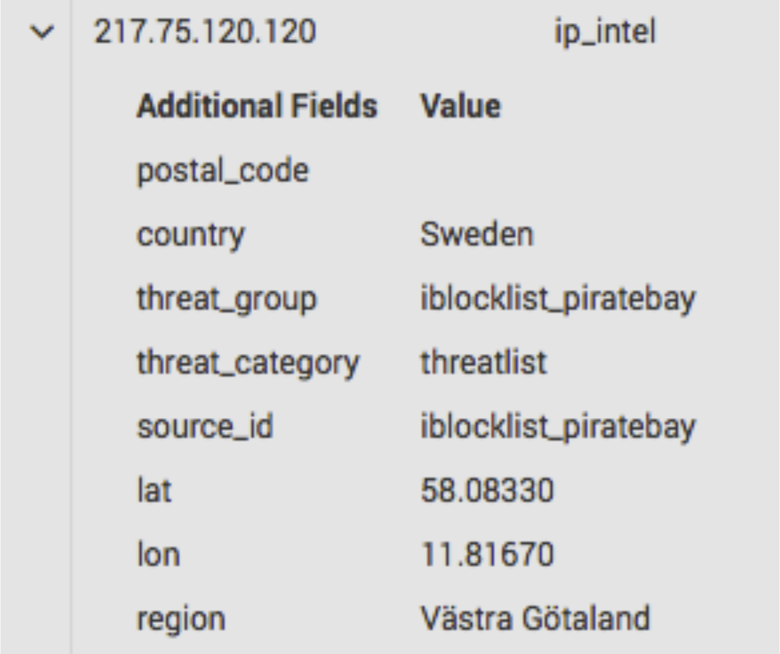
- Access - edit_threat_intel_collections capability
- Cloud URL will be slightly different
- Upload threat indicators
  - https://<host>:<mPort>/data/threat_intel/upload
- Perform CRUD operations on an existing threat intelligence collection
  - https://<host>:<mPort>/services/data/threat_intel/item/{threat_intel_collection}
- Perform read, update, and delete operations on a row of an existing threat intelligence collection
  - https://<host>:<mPort>/services/data/threat_intel/item/{threat_intel_collection}/{item_key}

https://docs.splunk.com/Documentation/ES/4.7.2/API/ThreatIntelligenceAPIreference

Marking Artifacts

Keep But Don’t Correlate

- Introduced keeping artifacts for reference – marked disabled via API

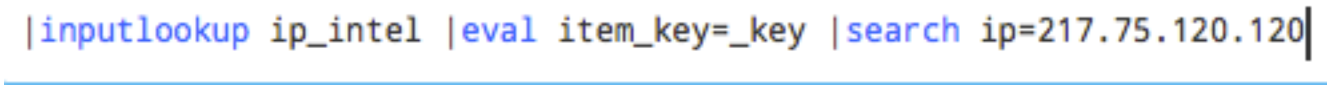


217.75.120.120 ip_intel

Additional Fields	Value
postal_code	
country	Sweden
threat_group	iblocklist_piratebay
threat_category	threatlist
source_id	iblocklist_piratebay
lat	58.08330
lon	11.81670
region	Västra Götaland

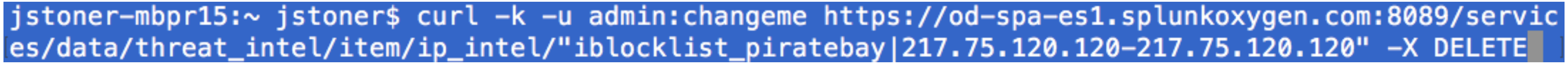
Deletion (Disable) Threat Indicators

- Important to know which indicators were at one time used
- Staleness can set in
- Don’t want to delete, but don’t want to correlate
- Mark as disabled will not remove it from kvstore
  - Will prevent it from correlating against events
  - Threat generating searches bypass t via macro

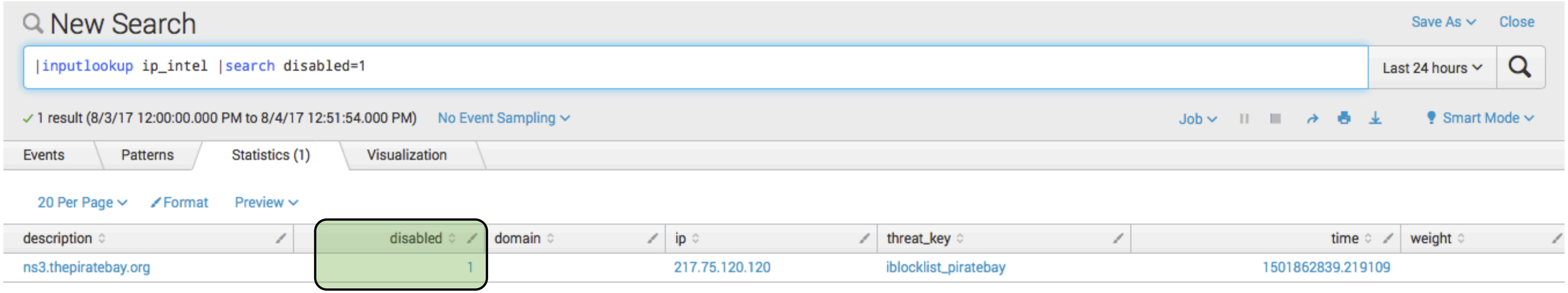


```
|inputlookup ip_intel |eval item_key=_key |search ip=217.75.120.120
```

Deletion(Disable) Threat Indicators



```
jstoner-mbpr15:~ jstoner$ curl -k -u admin:changeme https://od-spa-es1.splunkoxygen.com:8089/servic
es/data/threat_intel/item/ip_intel/"iblocklist_piratebay|217.75.120.120-217.75.120.120" -X DELETE
```

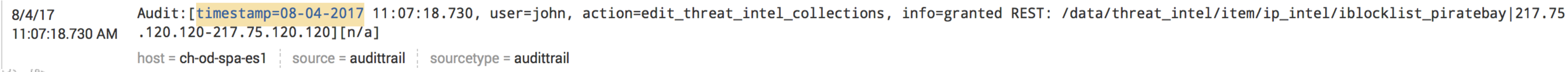


```
|inputlookup ip_intel |search disabled=1
```

✓ 1 result (8/3/17 12:00:00.000 PM to 8/4/17 12:51:54.000 PM)

description	disabled	domain	ip	threat_key	time	weight
ns3.thepiratebay.org	1		217.75.120.120	iblocklist_piratebay	1501862839.219109	

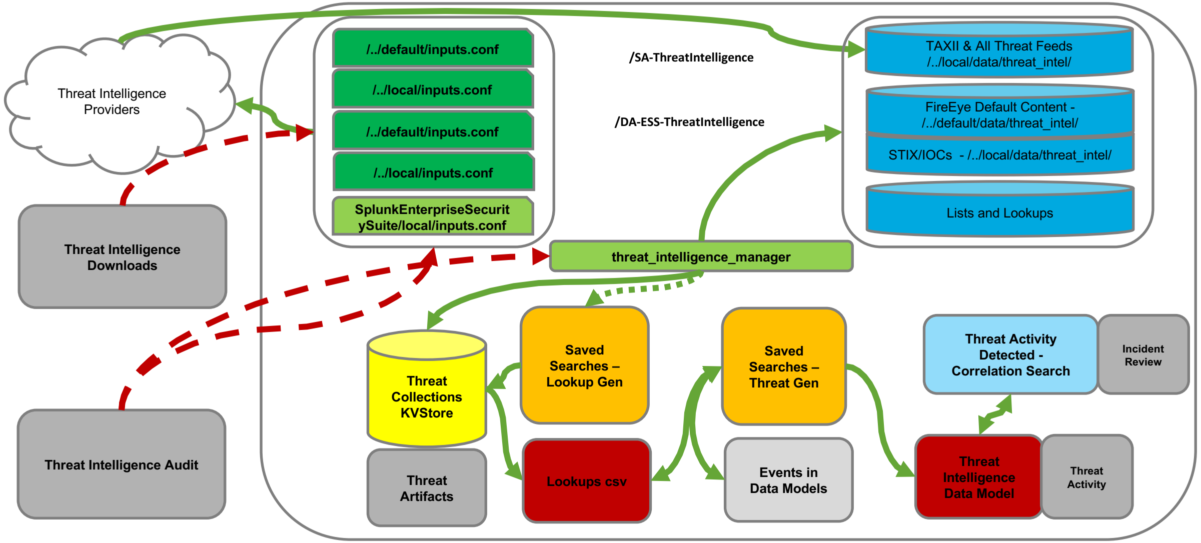
```
index=_* action=edit_threat_intel_collections
```



```
8/4/17          Audit:[timestamp=08-04-2017 11:07:18.730, user=john, action=edit_threat_intel_collections, info=granted REST: /data/threat_intel/item/ip_intel/iblocklist_piratebay|217.75
11:07:18.730 AM .120.120-217.75.120.120][n/a]
                host = ch-od-spa-es1   source = audittrail   sourcetype = audittrail
```

Summary

- Threat Intel is one of the five frameworks of ES
- Ingest from CSV, IOC, STIX, TAXII, Internet Feeds (need to format)
- Audit logs are very robust for troubleshooting
- API has been made available to work with collections


Threat Intelligence Providers
Threat Intelligence Downloads
Threat Intelligence Audit
/../default/inputs.conf
/../local/inputs.conf
/../default/inputs.conf
/../local/inputs.conf
SplunkEnterpriseSecuritySuite/local/inputs.conf
/SA-ThreatIntelligence
/DA-ESS-ThreatIntelligence
TAXII & All Threat Feeds /../local/data/threat_intel/
FireEye Default Content - /../default/data/threat_intel/
STIX/IOCs - /../local/data/threat_intel/
Lists and Lookups
threat_intelligence_manager
Threat Collections KVStore
Threat Artifacts
Saved Searches – Lookup Gen
Lookups csv
Saved Searches – Threat Gen
Events in Data Models
Threat Activity Detected - Correlation Search
Incident Review
Threat Intelligence Data Model
Threat Activity

Don't forget to **rate this session** in the .conf2017 mobile app

splunk> .conf2017

splunk>