Enterprise Security Biology
Dissecting the Threat Intelligence Framework

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

September 2017
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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
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
Better understand how Splunk processes threat indicators in Enterprise Security

Better insight = Better Troubleshooting
dis·sect

/dəˈsekt,dɪˈsekt/
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-CAAAAFBC
Why This Presentation...
Collection
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
# Default Data Downloads

<table>
<thead>
<tr>
<th>Threat Provider</th>
<th>Threat Source</th>
<th>Source site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerging Threats</td>
<td>compromised IPs blocklist</td>
<td><a href="http://rules.emergingthreats.net/blockrules">http://rules.emergingthreats.net/blockrules</a></td>
</tr>
<tr>
<td></td>
<td>fwip rules</td>
<td><a href="http://rules.emergingthreats.net/fwrules">http://rules.emergingthreats.net/fwrules</a></td>
</tr>
<tr>
<td>Hail a TAXII.com</td>
<td>Malware domain host list</td>
<td><a href="http://hailataxii.com">http://hailataxii.com</a></td>
</tr>
<tr>
<td>I-Blocklist</td>
<td>Logmein, Piratebay, Proxy, Rapidshare, Spyware, Tor, Web attacker</td>
<td><a href="http://list.iblocklist.com">http://list.iblocklist.com</a></td>
</tr>
<tr>
<td>IANA*</td>
<td>ICANN Top-level Domains List</td>
<td><a href="http://data.iana.org">http://data.iana.org</a></td>
</tr>
<tr>
<td>Malware Domains</td>
<td>Malware Domain Blocklist</td>
<td><a href="http://mirror1.malwaredomains.com">http://mirror1.malwaredomains.com</a></td>
</tr>
<tr>
<td>Mozilla*</td>
<td>Mozilla Public Suffix List</td>
<td><a href="https://publicsuffix.org">https://publicsuffix.org</a></td>
</tr>
<tr>
<td>Phishtank</td>
<td>Phishtank Database</td>
<td><a href="http://data.phishtank.com">http://data.phishtank.com</a></td>
</tr>
<tr>
<td>SANS</td>
<td>SANS blocklist</td>
<td><a href="http://isc.sans.edu">http://isc.sans.edu</a></td>
</tr>
<tr>
<td>abuse.ch</td>
<td>Palevo C&amp;C IP Blocklist</td>
<td><a href="https://palevotracker.abuse.ch">https://palevotracker.abuse.ch</a></td>
</tr>
<tr>
<td>abuse.ch</td>
<td>ZeuS blocklist (standard &amp; bad IPs only)</td>
<td><a href="https://zeustracker.abuse.ch">https://zeustracker.abuse.ch</a></td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th><em>time</em></th>
<th>stanza</th>
<th>disabled</th>
<th>type</th>
<th>url</th>
<th>weight</th>
<th>exit_status</th>
<th>download_status</th>
<th>run_duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-03 10:27:51</td>
<td>emerging_threats_compromised_ip_blocklist</td>
<td>0</td>
<td>threatlist</td>
<td><a href="https://rules.emergingthreats.net/blockrules/compromised-ip-list.txt">https://rules.emergingthreats.net/blockrules/compromised-ip-list.txt</a></td>
<td>1</td>
<td>0</td>
<td>threat list downloaded</td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:52</td>
<td>emerging_threats_ip_blocklist</td>
<td>0</td>
<td>threatlist</td>
<td><a href="https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt">https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt</a></td>
<td>1</td>
<td>0</td>
<td>threat list downloaded</td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:51</td>
<td>fb-tx_domain_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_domain_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:51</td>
<td>fb-tx_email_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_email_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:52</td>
<td>fb-tx_file_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_file_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:52</td>
<td>fb-tx_http_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_http_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:51</td>
<td>fb-tx_ip_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_ip_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:52</td>
<td>fb-tx_registry_intel</td>
<td>0</td>
<td>threatlist</td>
<td>lookup://fb-tx_registry_intel</td>
<td>1</td>
<td>0</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>2017-08-03 13:39:47</td>
<td>hailataxi_malware</td>
<td>0</td>
<td>taxii</td>
<td><a href="http://hailataxi.com/taxi-data">http://hailataxi.com/taxi-data</a></td>
<td>1</td>
<td>0</td>
<td>TAXII feed polling starting</td>
<td>0.0</td>
</tr>
<tr>
<td>2017-08-03 10:27:51</td>
<td>iblocklist_logmein</td>
<td>0</td>
<td>threatlist</td>
<td><a href="http://list.iblocklist.com/list-logmein">http://list.iblocklist.com/list-logmein</a></td>
<td>1</td>
<td>0</td>
<td>threat list downloaded</td>
<td>1.0</td>
</tr>
</tbody>
</table>
## Threat Indicator Download

### TAXII Example

### Threat Intelligence Audit Events

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Source Details</th>
</tr>
</thead>
</table>
Extraction
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 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_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

```
SPLUNK_HOME/etc/apps/frenchfry/local/data/threat_intel
```
Adding Files To Threat Collections

CSV

File Extensions Matter

Upload Threat Intelligence

File Name

c2-ipmasterlist

Drag and drop file here

File type not supported

The maximum file upload size is 50 MB.

Done

Upload Threat Intelligence

File Name

c2-ipmasterlist
c2-ipmasterlist.csv

Drag and drop file here

The maximum file upload size is 50 MB.
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
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
```
Adding Files To Threat Collections
File System View

[root@ch-od-spa-es1 threat_upload_attrs]# pwd
/local/data/threat_upload_attrs
[root@ch-od-spa-es1 threat_upload_attrs]# ll
-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, "description": "Uploaded document.", "threat_category": "APT"}
## Adding Files To Threat Collections

### A Happy Uploader

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/3/17 4:49:02.478 PM</td>
<td>17:08-03:16:49:02.478 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:run:679</td>
</tr>
<tr>
<td>8/3/17 4:49:02.466 PM</td>
<td>17:08-03:16:49:02.466 INFO pid=29928 tid=MainThread file=util.py:write_items_to_collection:283</td>
</tr>
<tr>
<td>8/3/17 4:49:01.982 PM</td>
<td>17:08-03:16:49:01.982 INFO pid=29928 tid=MainThread file=threat_intelligence_manager.py:write_output:452</td>
</tr>
<tr>
<td>8/3/17 4:49:01.953 PM</td>
<td>17:08-03:16:49:01.953 INFO pid=29928 tid=MainThread file=util.py:write_items_to_collection:283</td>
</tr>
<tr>
<td>8/3/17 4:49:01.963 PM</td>
<td>17:08-03:16:49:01.963 INFO pid=29928 tid=MainThread file=util.py:write_items_to_collection:283</td>
</tr>
<tr>
<td>8/3/17 3:29:08.674 PM</td>
<td>17:08-03:15:29:08.674 INFO pid=16672 tid=MainThread file=threat_intelligence_manager.py:run:679</td>
</tr>
<tr>
<td>8/3/17 3:29:08.673 PM</td>
<td>17:08-03:15:29:08.673 INFO pid=16672 tid=MainThread file=util.py:write_items_to_collection:283</td>
</tr>
<tr>
<td>8/3/17 3:29:05.219 PM</td>
<td>17:08-03:15:29:05.219 INFO pid=16672 tid=MainThread file=threat_intelligence_manager.py:write_output:452</td>
</tr>
<tr>
<td>8/3/17 3:29:05.154 PM</td>
<td>17:08-03:15:29:05.154 INFO pid=16672 tid=MainThread file=threat_intelligence_manager.py:run:664</td>
</tr>
<tr>
<td>8/3/17 3:29:05.153 PM</td>
<td>17:08-03:15:29:05.153 INFO pid=16672 tid=MainThread file=threat_intelligence_manager.py:validate_directory:530</td>
</tr>
</tbody>
</table>
# TAXII & Threat Intel Downloads
## Adding To Threat Collections

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 1/41:43.703 PM | INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status=&quot;wrote metadata to collection.&quot;, collection=&quot;threat_group_INTEL&quot;,

Filename=\"/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intelligence_manager/threat_intelligence_manager.xml\" |

host=chod-spa-es1, source=\"/four/splunk/var/log/splunk/threat_intelligence_manager.log\", sourcetype=\"threat intel\" |

count=\"1\" |
| 1/41:43.671 PM | info pid=15354 tid=MainThread file=utils.py:write_items_to_collection:283 | status=&quot;Wrote records to collection&quot;, collection=&quot;http_intel\n
Filename=\"/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intelligence_manager/threat_intelligence_manager.xml\" |

host=chod-spa-es1, source=\"/four/splunk/var/log/splunk/threat_intelligence_manager.log\", sourcetype=\"threat intel\" |

count=\"1\" |
| 1/41:43.634 PM | INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status=&quot;wrote metadata to collection.&quot;, collection=&quot;threat_group_INTEL&quot;,

Filename=\"/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intelligence_manager/threat_intelligence_manager.xml\" |

host=chod-spa-es1, source=\"/four/splunk/var/log/splunk/threat_intelligence_manager.log\", sourcetype=\"threat intel\" |

count=\"1\" |
| 1/41:43.600 PM | info pid=15354 tid=MainThread file=utils.py:write_items_to_collection:283 | status=&quot;Wrote records to collection&quot;, collection=&quot;ip_intel\n
Filename=\"/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intelligence_manager/threat_intelligence_manager.xml\" |

host=chod-spa-es1, source=\"/four/splunk/var/log/splunk/threat_intelligence_manager.log\", sourcetype=\"threat intel\" |

count=\"1\" |
| 1/41:43.124 PM | INFO pid=15354 tid=MainThread file=threat_intelligence_manager.py:write_output:452 | status=&quot;wrote metadata to collection.&quot;, collection=&quot;threat_group_INTEL&quot;,

Filename=\"/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intelligence_manager/threat_intelligence_manager.xml\" |

host=chod-spa-es1, source=\"/four/splunk/var/log/splunk/threat_intelligence_manager.log\", sourcetype=\"threat intel\" |

count=\"1\" |
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
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}
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/3/17 15:11:78PM</td>
<td>INFO pid=6858 tid=MainThread stanza_name=&quot;sa_threat_local&quot; 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</td>
</tr>
</tbody>
</table>

splunk>
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
SA-ThreatIntelligence

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

Previously - threatlist_manager

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Level</th>
<th>Intelligence Source</th>
<th>Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>Lookups</td>
<td>Last 24 hours</td>
</tr>
</tbody>
</table>

### Threat Intelligence Audit Events

- 12/6/16 23:19:39.225 INFO pid=84330 tid=MainThread file=threatlist_manager.py:run_threads:118 status="no merging required"
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:14:39.914 INFO pid=81309 tid=MainThread file=threatlist_manager.py:run_threads:118 status="no merging required"
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:09:41.003 INFO pid=78260 tid=MainThread file=threatlist_manager.py:run_threads:118 status="no merging required"
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:06:29.166 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:114 status="merging complete" category=alexa
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:04:40.818 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:100 status="merging" category=alexa
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:04:40.817 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:100 status="merging" category=mozilla_psl
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 23:04:40.816 INFO pid=75126 tid=MainThread file=threatlist_manager.py:run_threads:100 status="merging" category=tld
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 22:59:45.265 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:114 status="merging complete" category=alexa
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 22:59:43.418 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:100 status="merging" category=mozilla_psl
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 22:59:43.417 INFO pid=71584 tid=MainThread file=threatlist_manager.py:run_threads:100 status="merging" category=tld
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

- 12/6/16 22:59:40.360 INFO pid=13235 tid=MainThread file=threatlist_manager.py:run_threads:118 status="no merging required"
  - Host: localhost
  - Source: Applications/splunk/es/var/log/splunk/threatlist_manager.log
  - Source Type: threatlist_manager

Alexa, Mozilla, ICANN
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

```
| 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 Collections
- http_intel
- ip_intel
- user_intel
- certificate_intel
- Service_intel
- registry_intel
- Email_intel
- file_intel
- Process_intel
threat_group_intel
Datasets and Datamodels

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

- Just the list of artifacts, nothing actionable
### ip_intel

**New Search**

<table>
<thead>
<tr>
<th>description</th>
<th>disabled</th>
<th>domain</th>
<th>ip</th>
<th>threat_key</th>
<th>time</th>
<th>weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found in malicious notable event</td>
<td></td>
<td></td>
<td>64.66.0.20</td>
<td>local_ip_intel</td>
<td>1501787511.162301</td>
<td>1</td>
</tr>
</tbody>
</table>

**Pony (ref: cybercrime-tracker.net)**

<table>
<thead>
<tr>
<th><em>nato.nsh.in</em></th>
<th><em>np0ivite.com</em></th>
<th><em>mail.qiv.pl</em></th>
<th><em>login-voce.org</em></th>
<th><em>standardnews.co</em></th>
<th><em>kvlavtsenr.info</em></th>
<th><em>novivtis.com</em></th>
<th><em>gov.hu.com</em></th>
<th><em>nato88s8s8ionf14.com</em></th>
<th><em>soccra.moneqfree.pl</em></th>
<th><em>g0y.pl</em></th>
<th><em>smi8roup-online.co.uk</em></th>
<th><em>vnili.arp</em></th>
<th><em>ball1host.org</em></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>0758B64-1d07-4296-b135-b18c1396531a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP found in notable**

<table>
<thead>
<tr>
<th>ip</th>
<th>domain</th>
<th>time</th>
<th>weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.231.78</td>
<td>local_ip_intel</td>
<td>1501788771.008228</td>
<td>2</td>
</tr>
<tr>
<td>103.234.212.187</td>
<td>c2-lpmasterlist-rev</td>
<td>1501796942.385785</td>
<td></td>
</tr>
<tr>
<td>103.234.212.193</td>
<td>c2-lpmasterlist-rev</td>
<td>1501796942.385785</td>
<td></td>
</tr>
<tr>
<td>103.26.32.120</td>
<td>c2-lpmasterlist-rev</td>
<td>1501796942.385785</td>
<td></td>
</tr>
</tbody>
</table>

**IP used by simda C&C**

<table>
<thead>
<tr>
<th>ip</th>
<th>domain</th>
<th>time</th>
<th>weight</th>
</tr>
</thead>
</table>

**IP used by suppobox C&C**

<table>
<thead>
<tr>
<th>ip</th>
<th>domain</th>
<th>time</th>
<th>weight</th>
</tr>
</thead>
</table>
Threat Artifacts Dashboard

### Threat Artifacts

<table>
<thead>
<tr>
<th>Threat Artifact</th>
<th>Threat Category</th>
<th>Threat Group</th>
<th>Malware Alias</th>
<th>Intel Source ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat ID</td>
<td>All</td>
<td>local_ip_intel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Intel Source Path

Submit  Hide Filters

### Threat Overview

- **source_id:** source_path
- **source_type:** threat_group
- **threat_category:** malware_alias
- **count:**

<table>
<thead>
<tr>
<th>source_id</th>
<th>source_path</th>
<th>source_type</th>
<th>threat_group</th>
<th>threat_category</th>
<th>malware_alias</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_ip_intel</td>
<td>/four/splunk/etc/apps/DA-E59-ThreatIntelligence/lookups/local_ip_intel.csv</td>
<td>csv</td>
<td>local_ip_intel</td>
<td>threatlist</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

### IP Intelligence

- **ip:** 64.66.0.20
- **domain:** ip_intel
- **additional_fields:**
  - postal_code
  - country: Bahamas
  - threat_group: local_ip_intel
  - threat_category: threatlist
  - source_id: local_ip_intel
  - lat: 25.0833
  - lon: -77.3500
  - region: New Providence District

<table>
<thead>
<tr>
<th>ip</th>
<th>domain</th>
<th>threat_collection</th>
<th>organization_id</th>
<th>organization_name</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>64.66.0.20</td>
<td>ip_intel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Network Artifacts

- **threat_collection:** csv
- **source_type:** local_ip_intel
- **ip:** 199.9251.78
- **domain:** ip_intel

<table>
<thead>
<tr>
<th>threat_collection</th>
<th>source_type</th>
<th>ip</th>
<th>domain</th>
<th>url</th>
<th>http</th>
<th>total</th>
<th>threat_group</th>
<th>threat_category</th>
</tr>
</thead>
<tbody>
<tr>
<td>csv</td>
<td>local_ip_intel</td>
<td>199.9251.78</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lookup Generation Process

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

- Output files are file based not found in KVStore

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

```bash
[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

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/3/17 1:48:45.664 PM</td>
<td>2017-08-03 13:43:45.664 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:703</td>
</tr>
<tr>
<td>8/3/17 1:48:45.652 PM</td>
<td>2017-08-03 13:43:45.652 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:679</td>
</tr>
<tr>
<td>8/3/17 1:48:41.464 PM</td>
<td>2017-08-03 13:43:41.464 INFO pid=19968 tid=MainThread file=threat_intelligence_manager.py:run:679</td>
</tr>
</tbody>
</table>
Disabled Threat Intel Download Feed

Lookup Generation Gets Recomputed
Action
<table>
<thead>
<tr>
<th>Threat Match</th>
<th>cron</th>
<th>Data Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate_common_name</td>
<td>0,30 * * * *</td>
<td>Certificates</td>
</tr>
<tr>
<td>certificate_organization</td>
<td>5,35 * * * *</td>
<td>Certificates</td>
</tr>
<tr>
<td>certificate_serial</td>
<td>10,40 * * * *</td>
<td>Certificates</td>
</tr>
<tr>
<td>certificate_unit</td>
<td>15,45 * * * *</td>
<td>Certificates</td>
</tr>
<tr>
<td>email</td>
<td>20,50 * * * *</td>
<td>Certificates, Email</td>
</tr>
<tr>
<td>subject</td>
<td>25,55 * * * *</td>
<td>Email</td>
</tr>
<tr>
<td>file_hash</td>
<td>0,30 * * * *</td>
<td>Certificates, Change_Analysis, Email, Malware, Updates</td>
</tr>
<tr>
<td>file_name</td>
<td>5,35 * * * *</td>
<td>Change_Analysis, Email, Malware, Updates</td>
</tr>
<tr>
<td>http_user_agent</td>
<td>10,40 * * * *</td>
<td>Web</td>
</tr>
</tbody>
</table>

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

- `index=threat_activity`
- Populated from Threat Gen saved searches

```plaintext
[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
```

<table>
<thead>
<tr>
<th>Threat Intelligence &gt; Threat Activity</th>
<th>View Results</th>
<th>Summarize Fields</th>
<th>Manage</th>
<th>More Info</th>
<th>Explore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 24 hours &gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>359 events (9/8/17 9:00:00 PM to 9/8/17 9:21:26 PM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a</th>
<th>threat_collection</th>
<th>a</th>
<th>threat_collection_key</th>
<th>a</th>
<th>threat_key</th>
<th>a</th>
<th>threat_match_field</th>
<th>a</th>
<th>threat_match_value</th>
<th>a</th>
<th>dest</th>
<th>a</th>
<th>orig_source</th>
<th>a</th>
<th>src</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_intel</td>
<td>emerging_threats_ip_block</td>
<td>list:175.105.0.0/16</td>
<td>emerging_threats_ip_block</td>
<td>list</td>
<td>src</td>
<td>137.105.37.214</td>
<td>100.51.240.239</td>
<td>stream:http</td>
<td>stream:http</td>
<td>137.105.37.214</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip_intel</td>
<td>emerging_threats_ip_block</td>
<td>list:206.203.64.0/18</td>
<td>emerging_threats_ip_block</td>
<td>list</td>
<td>dest</td>
<td>206.203.69.204</td>
<td>206.203.69.204</td>
<td>stream:http</td>
<td>stream:http</td>
<td>19.141.2.170</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file_intel</td>
<td>mandiant-package: 190539dbe-1801-4cfe-b212-c01f6cefe240</td>
<td>mandiant:obj:emrable-8aee9bbfe-45eb-80c5-1b16-8a00-d89</td>
<td>file_name</td>
<td>SETUP, exe</td>
<td>ACME-CAD038P</td>
<td>WinInvent: Application: t</td>
<td>rendeccio</td>
<td>unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip_intel</td>
<td>emerging_threats_ip_block</td>
<td>list:198.128.0.0/19</td>
<td>emerging_threats_ip_block</td>
<td>list</td>
<td>dest</td>
<td>116.186.255.112</td>
<td>116.186.255.112</td>
<td>stream:http</td>
<td>stream:http</td>
<td>93.78.168.243</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Threat Dashboard Activity

Threat Activity Over Time

Most Active Threat Collections

<table>
<thead>
<tr>
<th>threat_collection</th>
<th>search</th>
<th>sparkline</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_intel</td>
<td>Email Address Matches</td>
<td></td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Network Resolution Matches</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source And Destination Matches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>file_intel</td>
<td>File Hash Matches</td>
<td></td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>File Name Matches</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Most Active Threat Sources

<table>
<thead>
<tr>
<th>source_id</th>
<th>source_path</th>
<th>source_type</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>emerging.threats_ip_blocklist</td>
<td>/usr/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv</td>
<td>csv</td>
<td>472</td>
</tr>
<tr>
<td>blacklist_logmein</td>
<td>/usr/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/blacklist_logmein.csv</td>
<td>csv</td>
<td>259</td>
</tr>
<tr>
<td>mandiant_package-19059346</td>
<td>/usr/splunk/etc/apps/04.EIPS/mandiant-package-19059346</td>
<td>stix</td>
<td>40</td>
</tr>
</tbody>
</table>
Threat Dashboard Activity
Details

<table>
<thead>
<tr>
<th><em>time</em></th>
<th>threat_match_field</th>
<th>threat_match_value</th>
<th>filter</th>
<th>sourcetype</th>
<th>src</th>
<th>dest</th>
<th>threat_collection</th>
<th>threat_group</th>
<th>threat_category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>140.143.191.0</td>
<td>stream.http</td>
<td></td>
<td>84.200.155.124</td>
<td>140.143.191.0</td>
<td>ip_intel</td>
<td>emerging_threats_ip_blocklist</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>155.204.40.81</td>
<td>stream.http</td>
<td></td>
<td>117.101.85.23</td>
<td>155.204.40.81</td>
<td>ip_intel</td>
<td>emerging_threats_ip_blocklist</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>25.125.166.140</td>
<td>stream.http</td>
<td></td>
<td>177.132.171.88</td>
<td>25.125.166.140</td>
<td>ip_intel</td>
<td>ibblocklist_logmein</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>25.177.219.250</td>
<td>stream.http</td>
<td></td>
<td>200.7.74.34</td>
<td>25.177.219.250</td>
<td>ip_intel</td>
<td>ibblocklist_logmein</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>25.182.81.42</td>
<td>stream.http</td>
<td></td>
<td>169.155.52.183</td>
<td>25.182.81.42</td>
<td>ip_intel</td>
<td>ibblocklist_logmein</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>25.206.159.196</td>
<td>stream.http</td>
<td></td>
<td>127.42.188.9</td>
<td>25.206.159.196</td>
<td>ip_intel</td>
<td>ibblocklist_logmein</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>dest</td>
<td>59.255.20.120</td>
<td>stream.http</td>
<td></td>
<td>19.68.61.233</td>
<td>59.255.20.120</td>
<td>ip_intel</td>
<td>emerging_threats_ip_blocklist</td>
<td>threatlist</td>
</tr>
<tr>
<td>2017-09-20 15:00</td>
<td>src</td>
<td>120.48.147.213</td>
<td>stream.http</td>
<td></td>
<td>120.48.147.213</td>
<td>190.120.116.69</td>
<td>ip_intel</td>
<td>emerging_threats_ip_blocklist</td>
<td>threatlist</td>
</tr>
</tbody>
</table>
## Search Correlations

- **correlationsearches.conf**
  
  ```
  ## This configuration file has been deprecated
  ```

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

- **savedsearches.conf**

```java
[Search - Search - 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 ($threat_match_values$)
action.notable.param.rule_description = Threat activity ($threat_match_values$) was discovered in the "$threat_match_field$" field based on threat intelligence available in the $threat_collections$ collection
action.notable.param.interesting_fields = threat_match_field,threat_match_value
action.notable.param.drilldown_name = View all threat activity involving
action.notable.param.drilldown_search = [ from datamodel:"Threat_Intelligence","Threat_Activity" ] | search threat_match_field="$threat_match_field$" threat_match_value="$threat_match_values$"
action.notable.param.default_status = 1
action.notable.param.default_owner = action.risk
# 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 = 86400s
alert.track = number of events
alert.relational = greater than
alert.quantity = 10
alert.description = Alerts when any activity matching threat
alert.intelligence_is_detected = True
alert.dispatch.earliest_time = -65m
alert.dispatch.latest_time = -5m
alert.enable = 1
alert.is_visible = false
request.ui.dispatch_app = SplunkEnterpriseSecuritySuite
```
Notable Events
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

<table>
<thead>
<tr>
<th>Group</th>
<th>cron</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>0 3 ***</td>
</tr>
<tr>
<td>Email</td>
<td>5 3 ***</td>
</tr>
<tr>
<td>File</td>
<td>10 3 ***</td>
</tr>
<tr>
<td>HTTP</td>
<td>15 3 ***</td>
</tr>
<tr>
<td>IP</td>
<td>20 3 ***</td>
</tr>
<tr>
<td>Process</td>
<td>25 3 ***</td>
</tr>
<tr>
<td>Registry</td>
<td>30 3 ***</td>
</tr>
<tr>
<td>Service</td>
<td>35 3 ***</td>
</tr>
</tbody>
</table>

Maximum age

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

Adaptive Response

Adaptive Response Actions

Select actions to run.

Add New Response Action

Add Threat Intelligence

Threat Group: localIp_intel (threatlist)

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

Run
Adaptive Response
Audit Threat Indicator Actions
## Operationalizing Threat Indicators

### Adaptive Response Audit Trail

<table>
<thead>
<tr>
<th>i</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>8/3/17</td>
<td>23:25:1.983 INFO sendmodaction - <strong>signature=&quot;Create operation successful.&quot; action_name=&quot;threat_add&quot;</strong> sid=1501788768.702827 orig_sid=scheduler__admin_REETvNTLUVzHbavwS0NuhVdGyjDlGbCg__RMD50f92f68b6f41f_at_1501783500_79064 rid=0 orig_rid=0 app=SplunkEnterpriseSecuritySuite user=system action_mod=&quot;adhoc&quot; action_status=&quot;success&quot; action_mode=adhoc action_name=threat_add app=SplunkEnterpriseSecuritySuite signature=Create operation successful user=system</td>
</tr>
<tr>
<td>&gt;</td>
<td>8/3/17</td>
<td>23:25:1.984 INFO sendmodaction - <strong>signature=&quot;Invoking modular action&quot; action_name=&quot;threat_add&quot;</strong> sid=1501788768.702827 orig_sid=scheduler__admin_REETvNTLUVzHbavwS0NuhVdGyjDlGbCg__RMD50f92f68b6f41f_at_1501783500_79064 rid=0 orig_rid=0 app=SplunkEnterpriseSecuritySuite user=system action_mod=&quot;adhoc&quot; action_status=&quot;success&quot; action_mode=adhoc action_name=threat_add app=SplunkEnterpriseSecuritySuite signature=Invoking modular action user=system</td>
</tr>
<tr>
<td>&gt;</td>
<td>8/3/17</td>
<td>21:15:1.805 INFO sendmodaction - <strong>signature=&quot;Create operation successful.&quot; action_name=&quot;threat_add&quot;</strong> sid=1501787508.701797 orig_sid=scheduler__admin_REETvNTLUVzHbavwS0NuhVdGyjDlGbCg__RMD50f92f68b6f41f_at_1501783500_79064 rid=0 orig_rid=28 app=SplunkEnterpriseSecuritySuite user=system action_mod=&quot;adhoc&quot; action_status=&quot;success&quot; action_mode=adhoc action_name=threat_add app=SplunkEnterpriseSecuritySuite signature=Create operation successful user=system</td>
</tr>
<tr>
<td>&gt;</td>
<td>8/3/17</td>
<td>21:15:1.806 INFO sendmodaction - <strong>signature=&quot;Invoking modular action&quot; action_name=&quot;threat_add&quot;</strong> sid=1501787508.701797 orig_sid=scheduler__admin_REETvNTLUVzHbavwS0NuhVdGyjDlGbCg__RMD50f92f68b6f41f_at_1501783500_79064 rid=0 orig_rid=28 app=SplunkEnterpriseSecuritySuite user=system action_mod=&quot;adhoc&quot; action_status=&quot;success&quot; action_mode=adhoc action_name=threat_add app=SplunkEnterpriseSecuritySuite signature=Invoking modular action user=system</td>
</tr>
</tbody>
</table>
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
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

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

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

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/217.75.120.120-217.75.120.120][n/a]
```
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.
Don't forget to rate this session in the .conf2017 mobile app