

ES Biology IV: Integrating a Threat Intelligence Platform

John Stoner

Principal Security Strategist | Splunk



Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing 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. © 2020 Splunk Inc. All rights reserved

#whoami

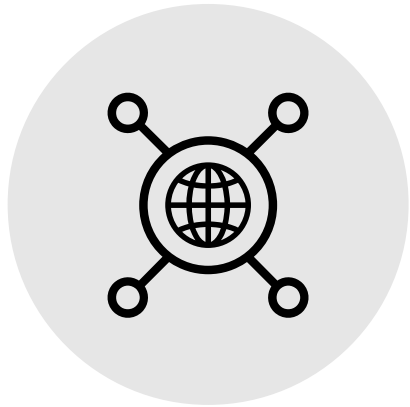
Principal Security Strategist | @stonerpsu | GCIA, GCIH, GCTI

- 20+ years kicking around databases, ISPs and cyber
- 5.5 years at Splunk
- Creator of SA-Investigator for Enterprise Security
- Co-editor and author
 - Hunting with Splunk: The Basics
 - Dear Buttercup: The Security Letters
- Assist in steering the BOTS ship
 - APT Scenario Developer
 - Workshop Development and Wrangler
- Speaker
 - SANS Summits, FIRST, DefCon PHV, BSides

Agenda

- 1. Threat Intel Framework Primer**
- 2. MISP Integration**
- 3. Adding ES To The Mix**
- 4. Links and References**

Enterprise Security Frameworks



Threat
Intelligence



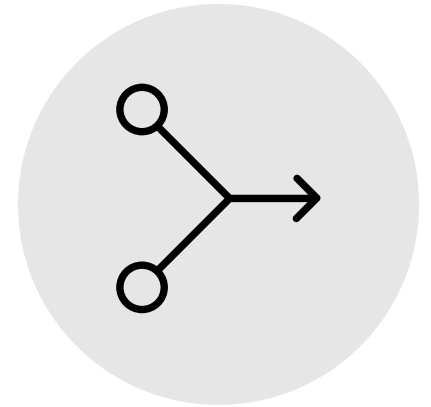
Incident
Management



Asset &
Identity



Risk

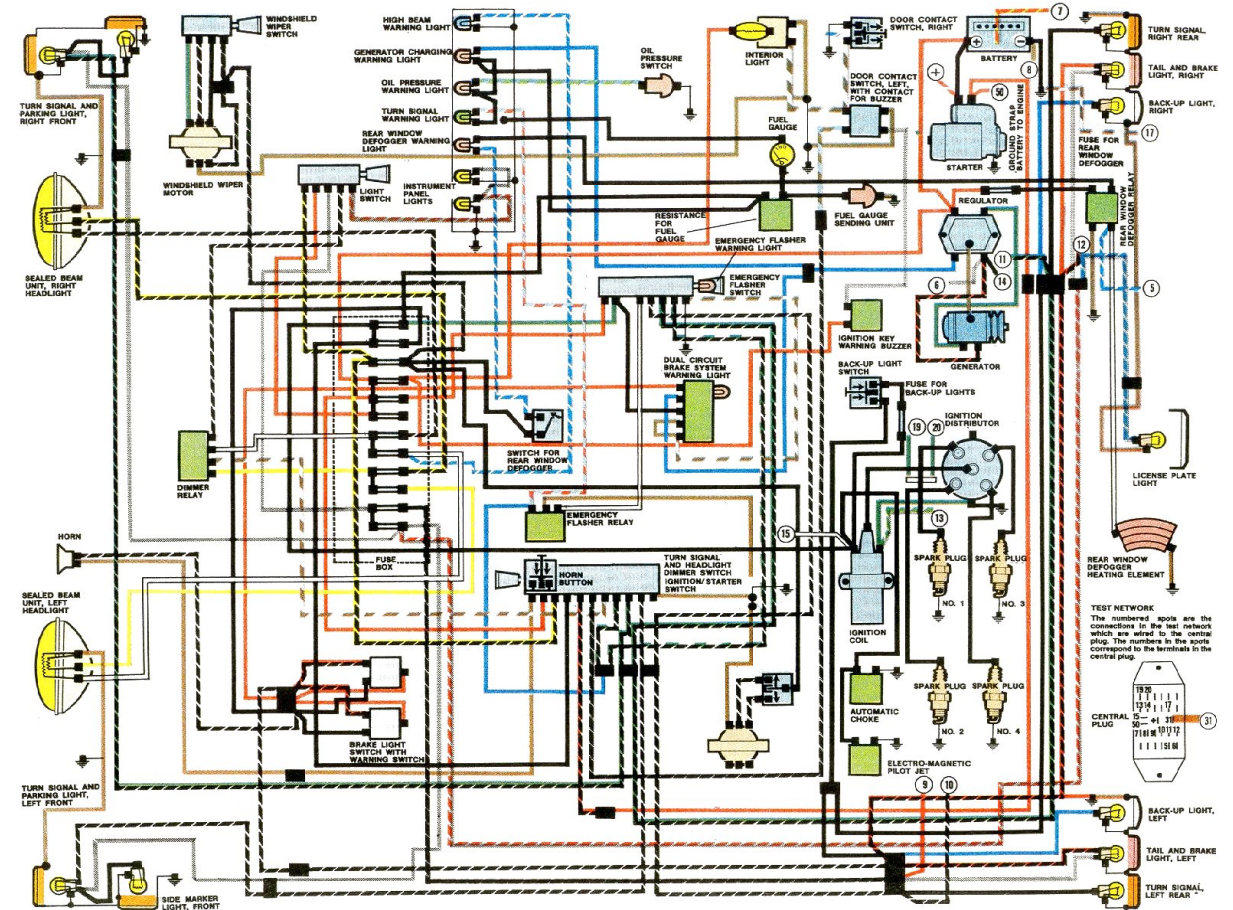


Adaptive
Response

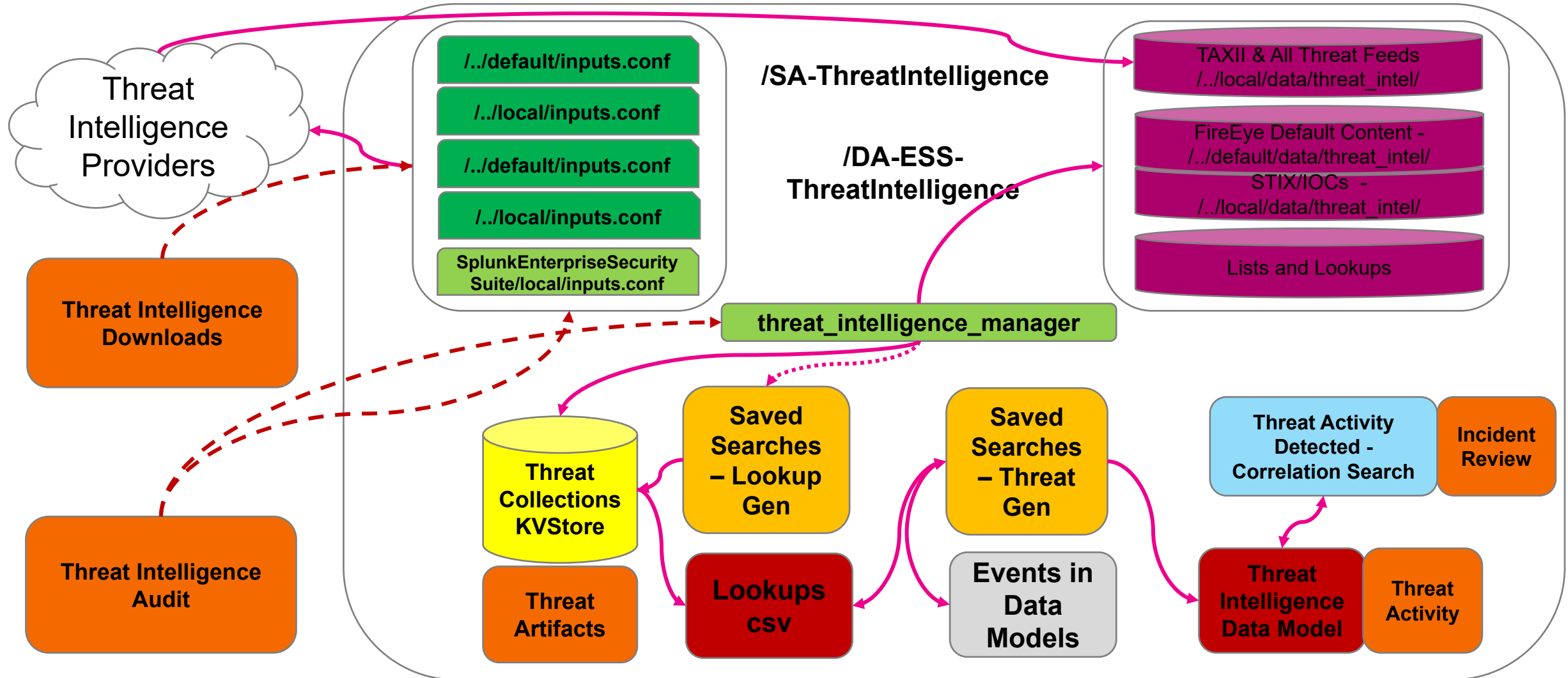
Why This Presentation...



1972 BEETLE AND SUPER BEETLE



Threat Intel Framework Data Flow



Numerous Threat Intel Platforms

Not Intended to Be an Endorsement or Survey of Them





MISP Integration



MISP42Splunk

Created to pull in MISP data via API to Splunk

Consists of

- Saved Searches
- Custom Search Commands
- Lookups (Email, File, HTTP, IP)
- Alert Actions (Create Event/Sighting in MISP)

Setup is straightforward

- API Key
- Account Name
- Index



Default Saved Search

Title	MISP_getioc_email_related_last1d_to_KV_MISP_email
Description	<input type="text" value="optional"/>
Search	<pre> mispgetioc misp_instance=MISP last=1d getuuid=t getorg=t geteventtag=t type ="email-attachment,email-src,email-src-display-name,email-subject,email-dst" where isnotnull(misp_email_attachment) or isnotnull(misp_email_src) or isnotnull(misp_email_src_display_name) or isnotnull(misp_email_subject) or isnotnull(misp_email_dst) outputlookup MISP_email append=true</pre>
Earliest time	<input type="text" value="-24h@h"/> Time specifiers: y, mon, d, h, m, s Learn More
Latest time	<input type="text" value="now"/> Time specifiers: y, mon, d, h, m, s Learn More

Custom Commands

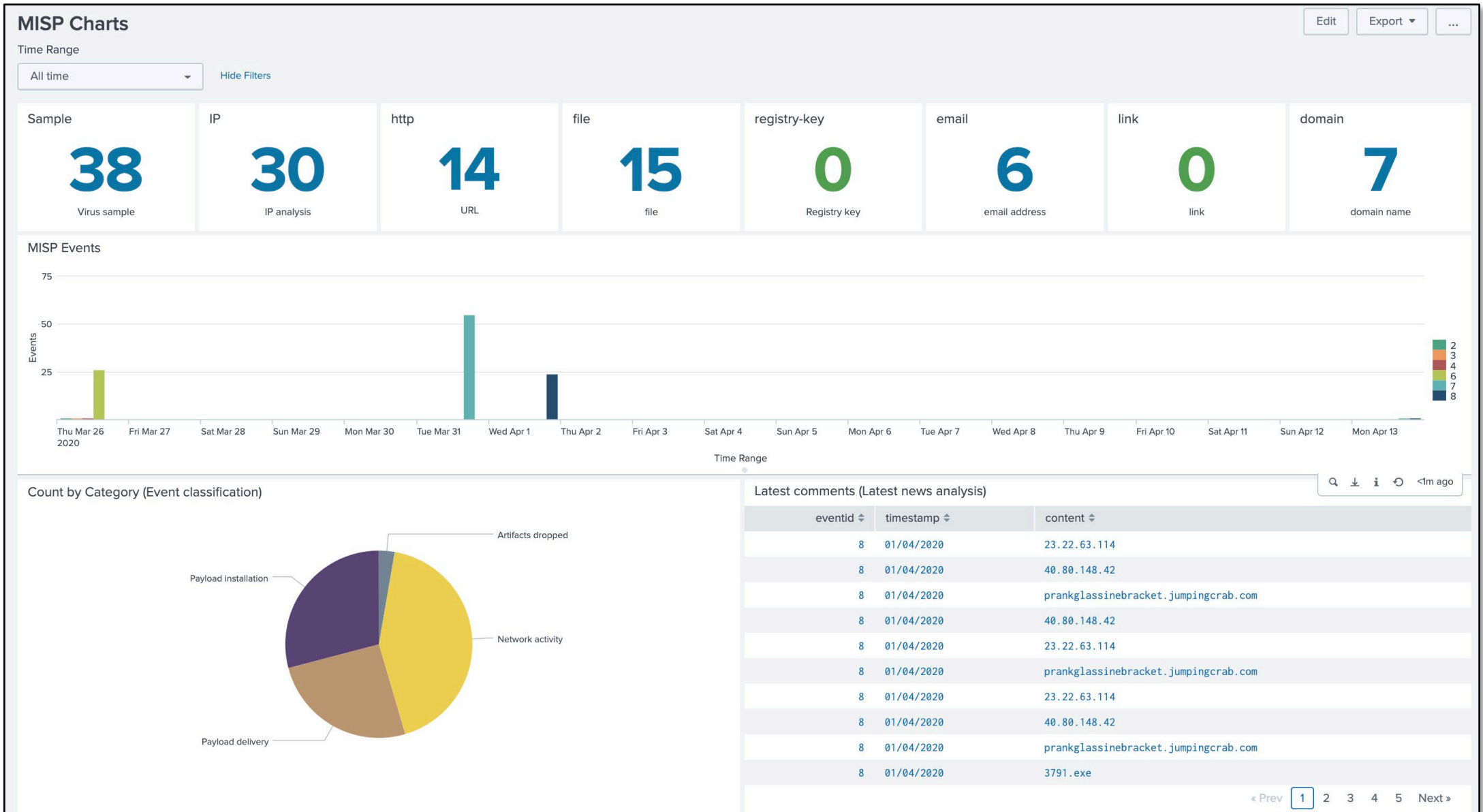
Collect / Search MISP Instance

| `mispgetioc misp_instance=MISP last=180d`

<pre> mispgetioc misp_instance=MISP last=270d getuuid=t getorg=t geteventtag=t type="email-dst,email-attachment,email-src,email-src-display-name,email-subject" limit=0 where isnotnull(misp_email_dst) or isnotnull(misp_email_attachment) or isnotnull(misp_email_src) or isnotnull(misp_email_src_display_name) or isnotnull(misp_email_subject) fields - _time, _raw, host</pre>										
<div> <div>✓ 2 results (8/24/20 1:00:00.000 PM to 8/25/20 1:40:54.000 PM) No Event Sampling ▼</div> <div> <div>Job ▼</div> <div>⏏</div> <div>⏏</div> <div>↶</div> <div>⏏</div> <div>⏏</div> <div>⏏</div> <div>⏏</div> <div>⏏</div> <div>⏏</div> <div>⏏</div> <div>Smart Mode ▼</div> </div> </div>										
<div> <div>Events (0)</div> <div>Patterns</div> <div>Statistics (2)</div> <div>Visualization</div> </div>										
<div> <div>20 Per Page ▼</div> <div>Format</div> <div>Preview ▼</div> </div>										
misp_tag	misp_comment	misp_to_ids	misp_email_dst	misp_type	misp_timestamp	misp_attribute_id	misp_category	misp_object_id	misp_attribute_uuid	misp_value
osint:source-type="block-or-filter-list"		True	sahro.bella7@post.cz	email-dst	1585673954	56	Payload delivery	0	5e8376ca-f060-49eb-8866-279fac1f26b3	sahro.bella7@post.cz
		True	trala.cosh2@post.cz	email-dst	1586812577	55	Payload delivery	0	5e83768d-3d48-4d20-8232-1ceaac1f26b3	trala.cosh2@post.cz

Customization

```
| mispgetioc misp_instance=MISP last=1d getuuid=t getorg=t geteventtag=t type  
  ="email-attachment,email-src,email-src-display-name,email-subject,email-dst"  
| where isnotnull(misp_email_attachment) or isnotnull(misp_email_src) or  
  isnotnull(misp_email_src_display_name) or isnotnull(misp_email_subject) or  
  isnotnull(misp_email_dst)  
| outputlookup MISP_email append=true | eval _time=misp_timestamp | collect index  
  =misp
```





Adding ES to the Mix



Where to Integrate?

Local Lookups

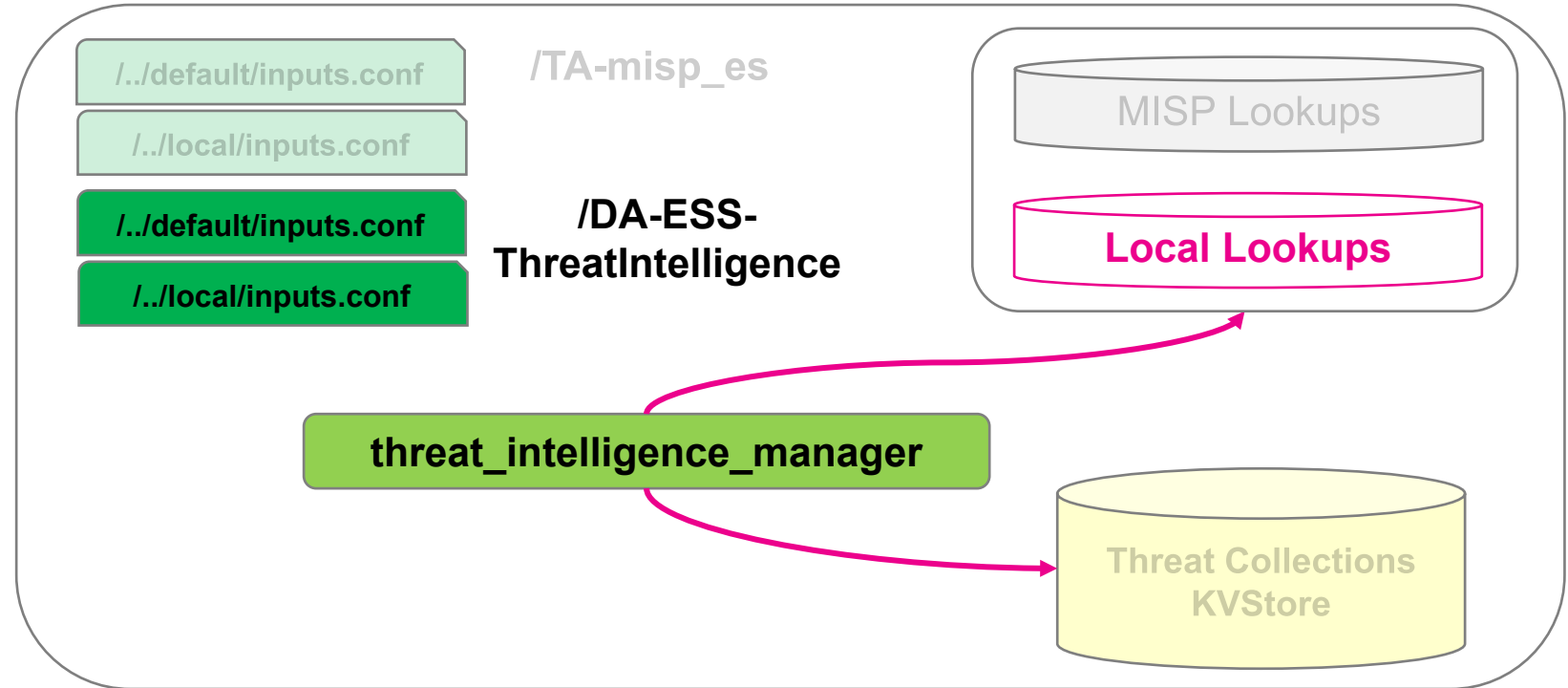
Simplest

Saved Search will output to existing csvs

Mixing truly local indicators with TIP – do things get muddled? Aging indicators out?

Everything is designed to go here unless an automated feed....

Do we want to separate indicators captured in Splunk ES from your TIP (MISP)?



Where to Integrate?

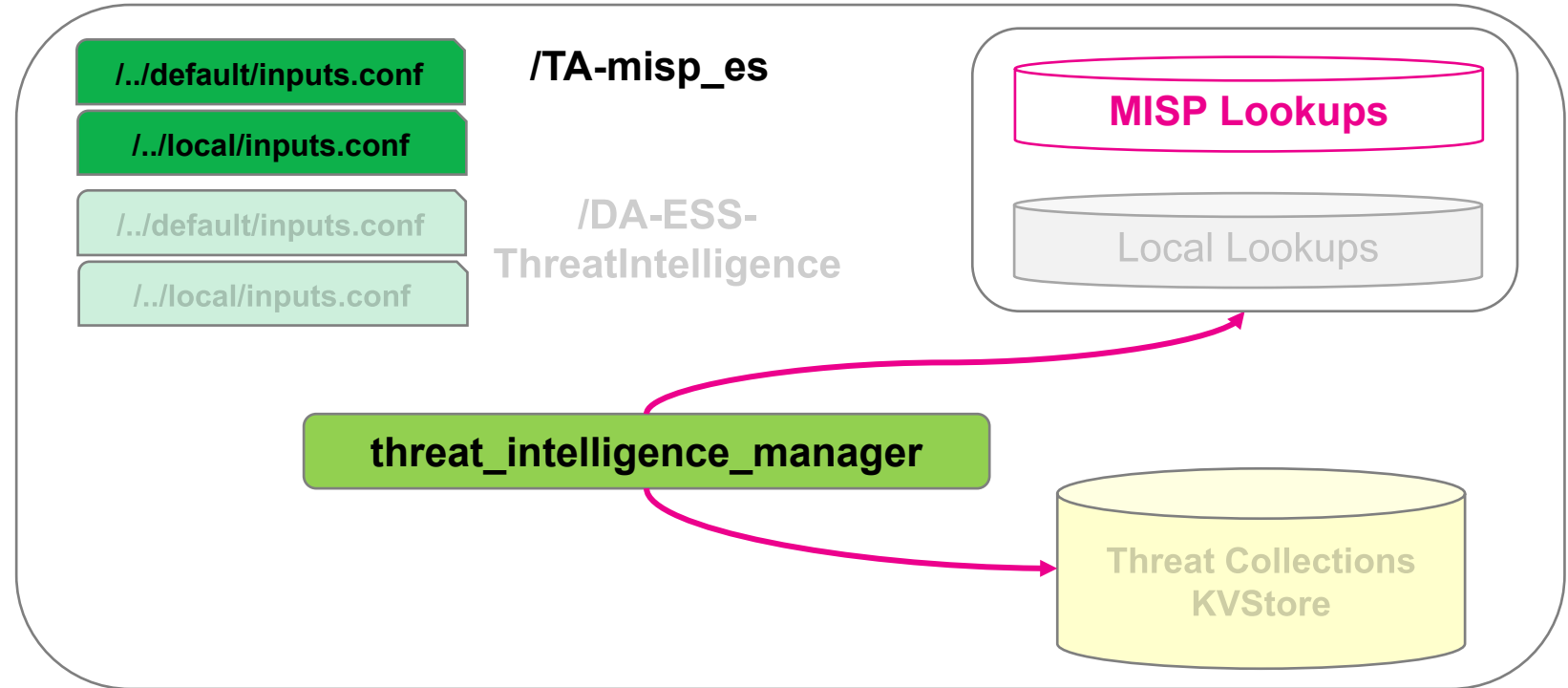
Using Your Own Lookups

Little more complexity

- I tried to take care of that for you in my app

Keep local indicators segmented from TIP

No additional coding, leverage TI Framework



Where to Integrate?

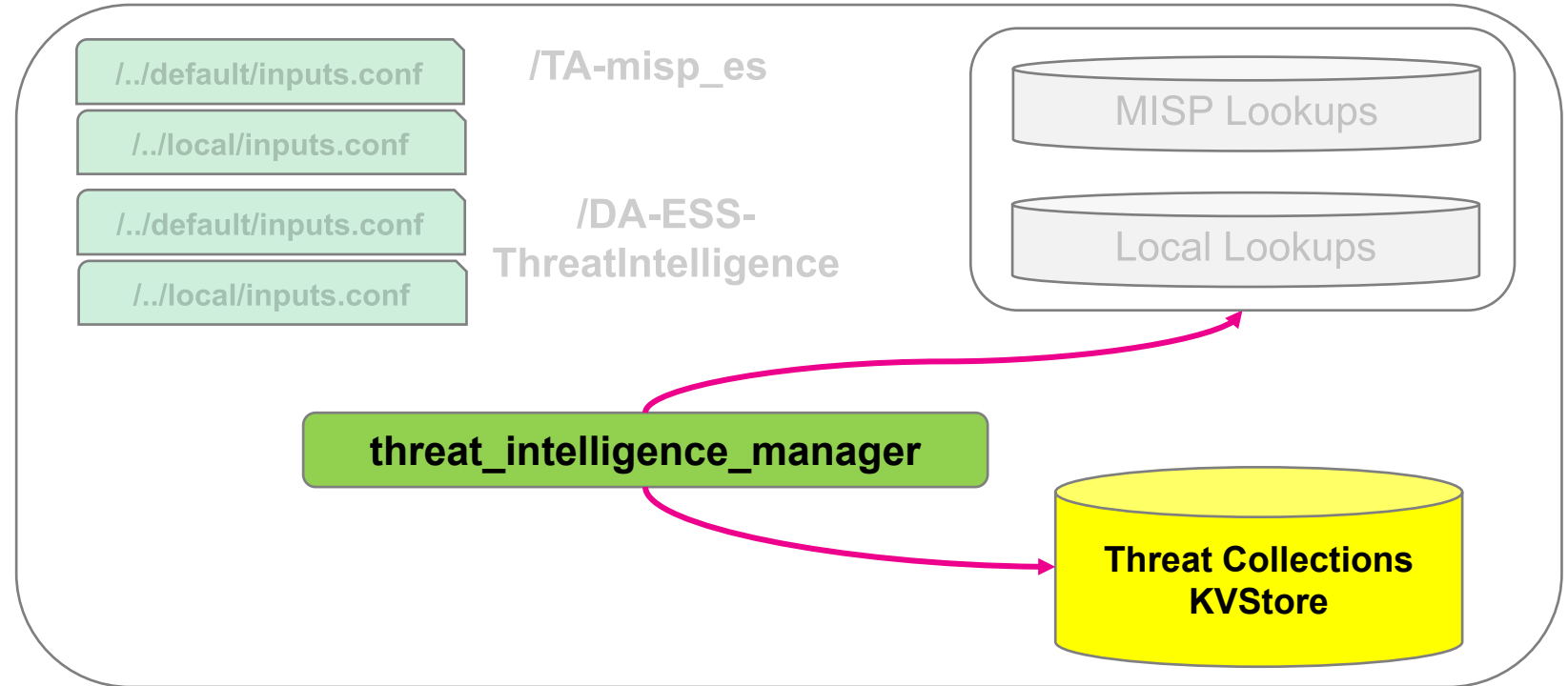
Writing directly to KVStore

This is where all indicators end up before correlation

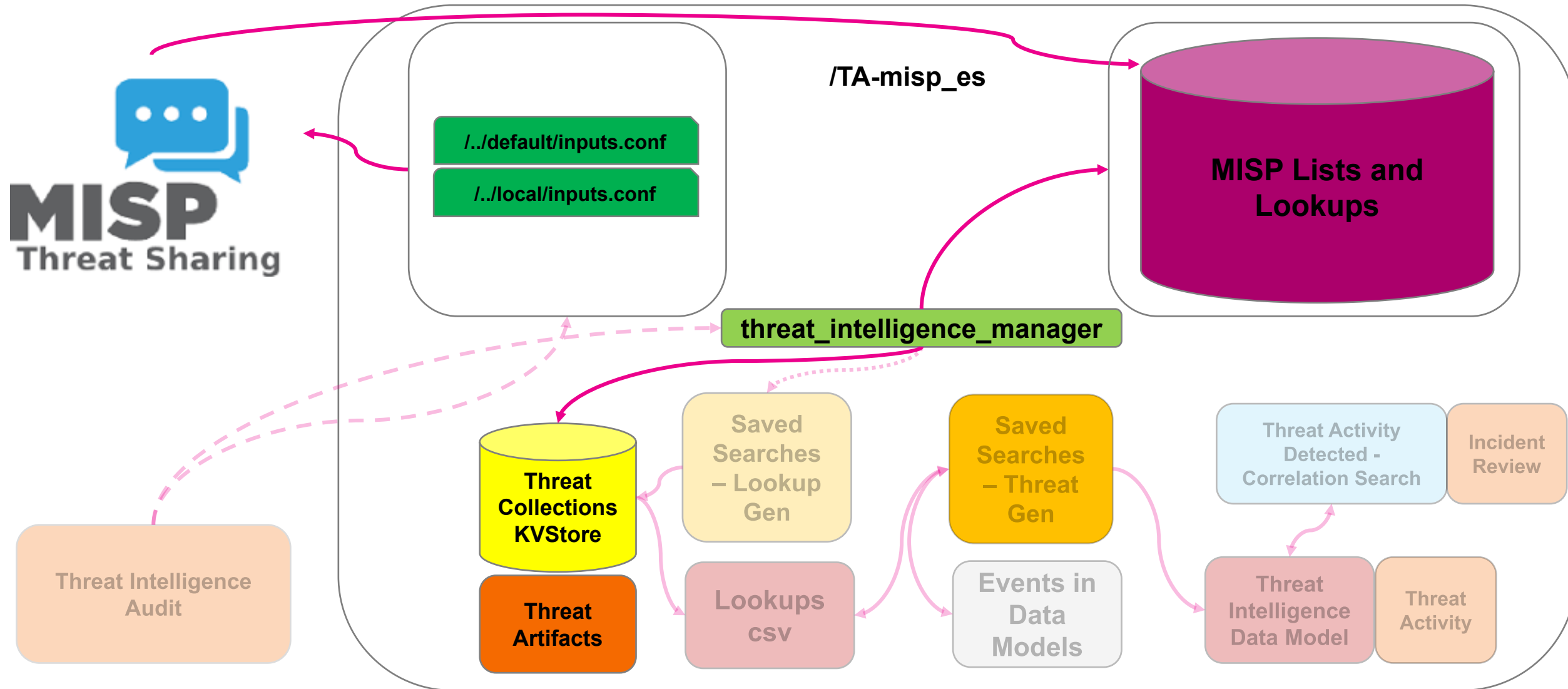
Bypass Threat Intelligence Manager modular input and the work it handles

No aging is set up there by default

Probably wouldn't integrate any deeper in the framework at that point, unless you wanted to ignore/scrap framework



Threat Intel Framework Data Flow



.conf Files for ES/MISP

inputs.conf

```
[threatlist://misp_es_domain_intel]
description = Threat intelligence pertaining to domains
disabled = false
type = threatlist
url = lookup://misp_es_domain_intel
```

Maps to Splunk Threat Collections

- Email, File, HTTP, IP/Domain, Registry

transforms.conf

```
[misp_es_domain_intel]
filename = misp_es_domain_intel.csv
```

Uses its Own Lookups

- Separate from Local Lookups
- local_ip_intel.csv, local_http_intel.csv, etc...

managed_configurations.conf

```
[lookup:misp_es_domain_intel]
endpoint    = /services/data/transforms/lookups/misp_es_domain_intel
label       = MISP to ES Domain Intel
description = Threat intelligence pertaining to domains
lookup_type = adhoc
```


ES Extension

Title	MISP_ES_ip_intel
Description	<input type="text" value="optional"/>
Search	<pre> mispgetioc misp_instance=MISP add_description=true category="External analysis ,Financial fraud,Internal reference,Network activity,Other,Payload delivery ,Payload installation,Payload type,Persistence mechanism,Person,Social network,Support Tool,Targeting data" type="ip-dst,ip-src" to_ids=true geteventtag=true warning_list=true limit=0 last=60d eval ip=misp_value eval description = tostring(misp_event_info)." ".tostring(misp_category)." ". tostring(misp_comment) eval weight = 1 table description,ip,weight outputlookup append=true misp_es_ip_intel</pre>

Threat Intelligence Audit



▼

6/15/20 4:10:08.000 PM

Threat

Threat Activity Detected (40.80.148.42)

Low

New

unassigned ▼

Description:

Threat activity (40.80.148.42) was discovered in the "src" field based on threat intelligence available in the ip_intel collection

Related Investigations:

Currently not investigated.

Additional Fields

Destination
Destination Expected
Destination PCI Domain
Destination Requires Antivirus
Destination Should Time Synchronize
Destination Should Update
Source
Source Expected
Source PCI Domain
Source Requires Antivirus
Source Should Time Synchronize
Source Should Update

Threat Category
Threat Collection
Threat Collection Key
Threat Description
Threat Group
Threat Key
Threat Match Field
Threat Match Value
Threat Source ID
Threat Source Path
Threat Source Type

threatlist
ip_intel
misp_es_ip_intel40.80.148.42
Threat intelligence pertaining to IPs
misp_es_ip_intel
misp_es_ip_intel
src
40.80.148.42
misp_es_ip_intel
/four/splunk/etc/apps/TA-
misp_es/lookups/misp_es_ip_intel.csv
CSV

Source And Destination Match
Time=157766400.000, i
104.358, src="40.80.14
field=src, threat_match_v
eat_key=misp_es_ip_inte
misp_es_ip_intel|40.8

User	Status
admin	✓ success
admin	✓ success

Risk Analysis saved 2020-06-15T16:10:08+0000

[View Adaptive Response Invocations](#)

Next Steps:

No Next Steps defined.



Helpful Links

ES Biology – Threat Intel Framework (conf17)

- Slides – <https://conf.splunk.com/files/2017/slides/enterprise-security-biology-dissecting-the-splunk-enterprise-security-threat-intelligence-framework.pdf>
- Video – <https://conf.splunk.com/files/2017/recordings/enterprise-security-biology-dissecting-the-splunk-enterprise-security-threat-intelligence-framework.mp4>

Blogs on Integrating Threat Intel with Enterprise Security

- MISP – https://www.splunk.com/en_us/blog/security/integrating-covid-or-any-threat-indicators-with-misp-and-enterprise-security.html
- Without TIP – https://www.splunk.com/en_us/blog/security/how-do-i-add-covid-threat-intelligence-from-the-internet-to-enterprise-security.html

Software & References

MISP42Splunk: <https://splunkbase.splunk.com/app/4335/>

MISP42Splunk (GitHub): <https://github.com/remg427/misp42splunk>

- Additional Documentation and Dashboard Sample:
<https://github.com/remg427/misp42splunk/tree/master/docs>

MISP Integration with ES (GitHub): https://github.com/splunk/TA-misp_es

ES Threat Intel Framework: <http://dev.splunk.com/view/enterprise-security/SP-CAA AFBC>



Thank You

Please provide feedback via the
SESSION SURVEY

