ES Biology IV: Integrating a Threat Intelligence Platform

John Stoner
Principal Security Strategist | Splunk
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 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.
#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

© 2020 SPLUNK INC.
Why This Presentation...
Threat Intel Framework Data Flow

- Threat Intelligence Providers
  - STIX/IOCs - ../local/data/threat_intel/
  - FireEye Default Content - ../default/data/threat_intel/
  - TAXII & All Threat Feeds - ../local/data/threat_intel/
  - STIX/IOC - ../local/data/threat_intel/

- Lists and Lookups

- /SA-ThreatIntelligence
  - /SA-ThreatIntelligence
  - /DA-ESS-ThreatIntelligence

- Threat Intelligence Data Model
  - Threat Activity
  - Incident Review

- Threat Collections KVStore
  - Threat Artifacts

- Saved Searches – Lookup Gen
  - Lookups csv

- Saved Searches – Threat Gen
  - Events in Data Models

- Threat Intelligence Downloads
  - Threat Intelligence Audit

- Threat Intelligence Manager
  -SplashEnterpriseSecurity Suite/local/inputs.conf

- Threat Activity Detected - Correlation Search
  - Threat Intelligence Data Model
  - Threat Activity
Numerous Threat Intel Platforms
Not Intended to Be an Endorsement or Survey of Them
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**
optional

**Search**
```
| 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
```

**Earliest time**
-24h@h

Time specifiers: y, mon, d, h, m, s Learn More

**Latest time**
now

Time specifiers: y, mon, d, h, m, s Learn More
Custom Commands
Collect / Search MISP Instance

```
| mispgetioc misp_instance=MISP last=180d
```

```
| mispgetioc misp_instance=MISP last=278d getuid=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
```

- 2 results (8/24/20 1:00:00:000 PM to 8/25/20 1:40:54:000 PM) No Event Sampling

Events (0) Patterns Statistics (2) Visualization

| misp_tag | misp_comment | misp_to_ids | misp_email_dst | misp_type | misp_timestamp | misp_attribute_id | misp_category | misp_object_id | misp_attribute_value | misp_value | misp_object
|-----------|--------------|-------------|----------------|-----------|----------------|------------------|--------------|----------------|----------------------|------------|-----------
| osint:source-type="block-or-filter-list" | True | sahro.bella7@post.cz | email-dst | 1585673954 | 56 | Payload delivery | 0 | 5e8376ca-f860-45eb-8866-273fac1f26b3 | sahro.bella7@post.cz |
| True | trala.cosh2@post.cz | email-dst | 1588812577 | 55 | Payload delivery | 0 | 5e83768d-3d48-4d20-8232-1eaaac1f26b3 | trala.cosh2@post.cz |
Customization

| mispgetioc misp_instance=MISP last=1d getuuuid=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
MISP Charts

Sample: 38  IP: 30  http: 14  file: 15  registry-key: 0  email: 6  link: 0  domain: 7

Virus sample  IP analysis  URL  file  Registry key  email address  link  domain name

MISP Events

Count by Category (Event classification)

Latest comments (Latest news analysis)

<table>
<thead>
<tr>
<th>eventid</th>
<th>timestamp</th>
<th>content</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>23.22.63.114</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>40.88.148.42</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>prangglassinebracket.jumpingcra.com</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>40.88.148.42</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>23.22.63.114</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>prangglassinebracket.jumpingcra.com</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>40.88.148.42</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>prangglassinebracket.jumpingcra.com</td>
</tr>
<tr>
<td>B</td>
<td>01/04/2020</td>
<td>3791.exe</td>
</tr>
</tbody>
</table>
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

MISP Lists and Lookups

/TA-misp_es

Threat Collections KVStore

/threat_intelligence_manager

Saved Searches – Threat Gen

Saved Searches – Lookup Gen

Lookups csv

Events in Data Models

Incident Review

Threat Activity Detected - Correlation Search

Threat Intelligence Data Model

Threat Activity

Threat Artifacts

Saved Searches – Threat Gen

lookup_gen

/TA-misp_es

../default/inputs.conf

../local/inputs.conf

Threat Audit

Threat Intelligence
.conf Files for ES/MISP

**inputs.conf**

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

**transforms.conf**

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

**managed_configurations.conf**

```plaintext
[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
```

Maps to Splunk Threat Collections
- Email, File, HTTP, IP/Domain, Registry

Uses its Own Lookups
- Separate from Local Lookups
- `local_ip_intel.csv`, `local_http_intel.csv`, etc…
## ES Extension

<table>
<thead>
<tr>
<th>Title</th>
<th>MISP_ES_ip_intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>optional</td>
</tr>
<tr>
<td>Search</td>
<td></td>
</tr>
</tbody>
</table>

```
| 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 |
```
Helpful Links

ES Biology – Threat Intel Framework (conf17)

Blogs on Integrating Threat Intel with Enterprise Security
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

Thank You

Please provide feedback via the SESSION SURVEY