SEMI-AUTOMATED CYBER THREAT INTELLIGENCE (ACT)

Training – FIRST CTI Symposium 2019 London

Martin Eian, Fredrik Borg, Geir Skjøtskift and Siri Bromander
Goal

To collect and organize our knowledge of threats to make it useful.
Data and Information
Semi-Automated...

- Analysis
- Enrichment
- Information Sharing
- Countermeasures
Semi-Automated Cyber Threat Intelligence (ACT)

The main objective of the research project is to develop a platform for cyber threat intelligence to uncover cyberattacks, cyber espionage and sabotage.

The project will result in new methods for data enrichment and data analysis to enable identification of threat agents, their motives, resources and attack methodologies.

In addition, the project will develop new methods, work processes and mechanisms for the generation and distribution of threat intelligence and countermeasures, to stop ongoing and prevent future attacks.
Data Model

- **Objects**
  - Global
  - Example: IP address

- **Facts**
  - Connected to one or two objects
  - Immutable
  - Timestamped
  - Owner
  - Role-based and explicit access control
  - Backed by evidence and comments

- **Placeholders**
Models, Taxonomies and Vocabularies

- **MITRE ATT&CK**
  - [https://attack.mitre.org](https://attack.mitre.org)
- **MITRE PRE-ATT&CK**
  - [https://attack.mitre.org/pre-attack/](https://attack.mitre.org/pre-attack/)
- **MISP galaxy**
  - [https://github.com/MISP/misp-galaxy](https://github.com/MISP/misp-galaxy)
- **STIX 2.0 vocabularies**
  - [https://oasis-open.github.io/cti-documentation/](https://oasis-open.github.io/cti-documentation/)
- Ryan Stillions’ DML model
Current OSINT Sources

- APTNotes
  - https://github.com/aptnotes/data
- APT & CyberCriminal Campaign Collection
  - https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- RSS Feeds
  - Infosec blogs
- mnemonic PassiveDNS
  - https://passivedns.mnemonic.no/
- Shadowserver IP-BGP
- VirusTotal
- MISP (circl.lu)
THE ACT PLATFORM
Platform Architecture – Core technologies

- Cassandra
- Elasticsearch
- Apache Nifi
- Apache OpenNLP
- Apache TinkerPop
Platform Architecture – Workflow orchestration

• Originally developed by NSA

• Open sourced and transferred to the Apache Foundation in 2014

• Manage flows of data supporting a large number of inputs and outputs:
  - HTTP, FTP, SCP, Kafka, Elasticsearch, JMS, Syslog, MongoDB, Hadoop, Cassandra, SMTP, POP3, etc
Platform Architecture – Graph database

• Looked into existing graph databases, but they lacked proper fine granular permissions (and many of them had commercial licenses that could not be used in the research project)

• Apache Tinkerpop implemented on top of Cassandra/Elasticsearch

• Graph queries opens up a range of possibilities that is not possible on a flat data structure
ACT Core

Backend

REST API

GUI

Apache TinkerPop

Cassandra

elasticsearch
<table>
<thead>
<tr>
<th>Method</th>
<th>Endpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>/v1/fact</td>
<td>Create a new Fact.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/fact/uuid[/fact]/access</td>
<td>Retrieve a Fact's ACL.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/fact/uuid[/fact]/access[/subject]</td>
<td>Grant a Subject access to a Fact.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/fact/uuid[/fact]/comments</td>
<td>Retrieve a Fact's comments.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/fact/uuid[/fact]/comments</td>
<td>Add a comment to a Fact.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/fact/uuid[/fact]/retract</td>
<td>Retract an existing Fact.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/fact/uuid[/id]</td>
<td>Retrieve a Fact by its UUID.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/factType</td>
<td>Create a new FactType.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/factType</td>
<td>List available FactTypes.</td>
</tr>
<tr>
<td>PUT</td>
<td>/v1/factType/uuid[/id]</td>
<td>Update an existing FactType.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/factType/uuid[/id]</td>
<td>Retrieve a FactType by its UUID.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/object[/type]/[/value]</td>
<td>Retrieve an Object by its type and value.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/object[/type]/[/value]/facts</td>
<td>Retrieve Facts bound to a specific Object.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/object[/type]/[/value]/traverse</td>
<td>Traverse the ObjectFact graph starting at an Object identified by its type and value.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/object[/type]/[/value]/traverse</td>
<td>Traverse the ObjectFact graph after performing an Object search.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/object/uuid[/id]</td>
<td>Retrieve an Object by its UUID.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/object/uuid[/id]/facts</td>
<td>Retrieve Facts bound to a specific Object.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/object/uuid[/id]/traverse</td>
<td>Traverse the ObjectFact graph starting at an Object identified by its UUID.</td>
</tr>
<tr>
<td>POST</td>
<td>/v1/objectType</td>
<td>List available ObjectTypes.</td>
</tr>
<tr>
<td>GET</td>
<td>/v1/objectType</td>
<td>Create a new ObjectType.</td>
</tr>
</tbody>
</table>
**Project description**

**python-act**

python-act is a library used to connect to the ACT platform.

The platform has a REST api, and the goal of this library is to expose all functionality in the API.

**Objects and Facts**

The act platform is built on two basic types, the object and fact.

Objects are universal elements that can be referenced uniquely by its value. An example of an object can be an IP address.

Facts are assertions or observations that ties objects together. A fact may or may not have a value describing further the fact.

Facts can be linked on or more objects. Below, the seenIn fact is linked to both an ipv4 object and report object, but the hasTitle fact is only linked to a report.

<table>
<thead>
<tr>
<th>Object type</th>
<th>Object value</th>
<th>Fact type</th>
<th>Fact value</th>
<th>Object type</th>
<th>Object value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>127.0.0.1</td>
<td>seenIn</td>
<td>report</td>
<td>ipv4</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>report</td>
<td>cbc80bb50c008944bf73(...)</td>
<td>hasTitle</td>
<td>Threat Intel Summary</td>
<td>cbc80bb50c008944bf73(...)</td>
<td></td>
</tr>
</tbody>
</table>
# Splunk Add-on - Queries

![Splunk Interface](image)

### New Search

<table>
<thead>
<tr>
<th>fact_value</th>
<th>fact_type</th>
<th>dest_object_type</th>
<th>source_object_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>usesTechnique</td>
<td>technique</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>threatActorAlias</td>
<td>threatActor</td>
<td>APT29</td>
</tr>
<tr>
<td>apt29-hammers-stealthy-tactics-definition-a.pdf</td>
<td>hasTitle</td>
<td>eaae8f5a6609590da627005cb5ad674d09106d323f189aae7f2242d4629ab0f4c</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>usesTool</td>
<td>tool</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>usesTechnique</td>
<td>technique</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>usesTool</td>
<td>tool</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>usesTechnique</td>
<td>technique</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>threatActorAlias</td>
<td>threatActor</td>
<td>APT29</td>
</tr>
<tr>
<td>-</td>
<td>usesTool</td>
<td>tool</td>
<td>APT29</td>
</tr>
</tbody>
</table>
**Splunk Add-on – Annotate search results**

```
source="carbanak.csv" dest_ip=179.43.140.82 | acta dest_ip
```

```
<table>
<thead>
<tr>
<th>dest_ip</th>
<th>usesC2ipv4</th>
<th>seenInreport</th>
</tr>
</thead>
<tbody>
<tr>
<td>179.43.140.82</td>
<td>c6ec176592ea26c4ee27974273e592ff 188f261e5fca94bd1fc1edc1aaefee8c0 6e9408c338e98a8bc166a8d4f8264019</td>
<td>9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb5523158909dad07e6b0f9491335ce4ce1550f64832b0c5396c2f5bb8f</td>
</tr>
<tr>
<td>179.43.140.82</td>
<td>c6ec176592ea26c4ec27974273e592ff</td>
<td>9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb5523158909dad07e6b0f9491335ce4ce1550f64832b0c5396c2f5bb8f</td>
</tr>
<tr>
<td>179.43.140.82</td>
<td>c6ec176592ea26c4ee27974273e592ff 188f261e5fca94bd1fc1edc1aaefee8c0 6e9408c338e98a8bc166a8d4f8264019</td>
<td>9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb5523158909dad07e6b0f9491335ce4ce1550f64832b0c5396c2f5bb8f</td>
</tr>
</tbody>
</table>
```
Threat Intelligence Platform - Summary

- Implemented
  - Core platform
  - API
  - GUI
  - Workflow orchestration
  - Graph queries

- Github repositories
  - https://github.com/mnemonic-no/act-api-python
  - https://github.com/mnemonic-no/act-bootstrap
  - https://github.com/mnemonic-no/act-frontend
  - https://github.com/mnemonic-no/act-platform
  - https://github.com/mnemonic-no/act-scio
  - https://github.com/mnemonic-no/act-splunk
  - https://github.com/mnemonic-no/act-triggers
  - https://github.com/mnemonic-no/act-workers
  - License: ISC (BSD compatible)
Before We Start
Accessing the GUI

- Read-only
  - https://act-eu1.mnemonic.no
  - https://act-eu2.mnemonic.no

- Tasks: /examples/
- API: /swagger/
- API-assignments: https://github.com/mnemonic-no/act-workshop-api (jupyter notebook you can test yourself if you are interested in testing the python API)
Introduction 1
Introduction 1 – Right Click / Left Click
Introduction 1 – History, Layouts and Filtering
Introduction 1 – Fact Types
Introduction 2

Try the following object queries and explore the graph:

- threatActor: APT3
- tactic: lateral-movement
- tool: foosace
- ipv4: 153.148.23[.]118
Task 1

Try the following object query:

• tool: remsec

Which threat actor is associated with this tool? Which techniques are associated with this threat actor? Can you find any reports that mention file hashes classified as remsec?
Task 2: Find the Report

Task 3

Explore Autonomous System Number 8048

• asn: 8048

What kind of malicious behaviour has been observed from this AS?

Where is the organization that owns AS8048 located?
Introduction 3 – Graph Query
Try to replace ‘mentions’ with ‘resolvesTo’ in the graph query (you can edit the URL).
Introduction 4 – Extended Graph Query
WORKSHOP – GRAPH QUERIES

With Great Power Comes Great Responsibility
Graph Query 1
Graph Query 2 – Show Edges
Graph Query 3 – 2 hops
Graph Query 4 – Filter Edges (Facts)
Graph Query 5 – Filter Nodes (Objects)
Task 4 - Subgraph
hash \rightarrow content \rightarrow uri \text{ with port number } 1337 \leftarrow \text{fqdn}
g.outE('represents').otherV().outE('connectsTo').otherV().where(outE().has('value','1337')).inE('componentOf').otherV().path().unfold()
g.outE('represents').otherV().outE('connectsTo').otherV().
not(where(outE().has('value','1337'))).inE('componentOf').otherV().path().unfold()

not(where()), not where(not())
Task 5: Find the IP Address Owner

The fqdn fsw.adobeus[.]com is mentioned in one report. A sinkhole IPv4 address is also mentioned in the same report. Which organization owns that sinkhole IPv4 address, and which country is it located in?

Hint: Fact Type ‘mentions’ and ‘memberOf’
Task 5 Solution
g.inE('mentions').otherV().outE('mentions').otherV().hasLabel('ipv4').where(outE('sinkhole')).outE('memberOf').otherV().outE('memberOf').otherV().inE('owns').otherV().outE('locatedIn').otherV().path().unfold()
Graph Query 6 – Unique Tool Usage
ASSIGNMENTS
CASE STUDY
Public Read-Only ACT Instance

https://act-eu1.mnemononic.no/examples/
FURTHER WORK
New Information Sources

- Security alerts
- Incidents
- Reputation lists
- Malware analysis systems
- STIX feeds
- ...

...
Graph Analytics

- Post. doc. @ UiO
- Post. doc. @ NTNU
Information Sharing

• Mechanism for sharing schema
• Format (STIX?)
• Trust models
Trust and Confidence

- Trust (source)
- Confidence (fact)
- Subjective Logic (quantify uncertainty)
GUI Improvements

• Context menu
  - Pre-defined graph queries
  - Download report
  - ...

• Timelines
• Share workspace
• Prune graph