SEMI-AUTOMATED CYBER THREAT INTELLIGENCE (ACT)

Training – FIRST Conference 2019 Edinburgh

Martin Eian, Geir Skjøtskift, Siri Bromander and Tom Spangebu

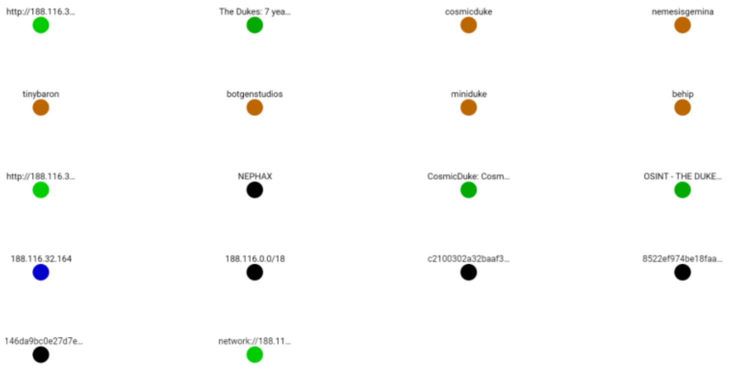
When	What
09:00 – 10:30	Introduction to ACT
10:30 – 10:45	Break
10:45 – 13:00	Assignments, case study
13:00 – 14:00	Lunch (not provided)
14:00 – 15:30	Recap, breakout (API/Graph queries)
15:30 – 15:45	Break
15:45 – 18:00	Practical work (build something)
18:30 – 19:00	Newbie reception
19:00 – 21:00	Icebreaker reception

Goal

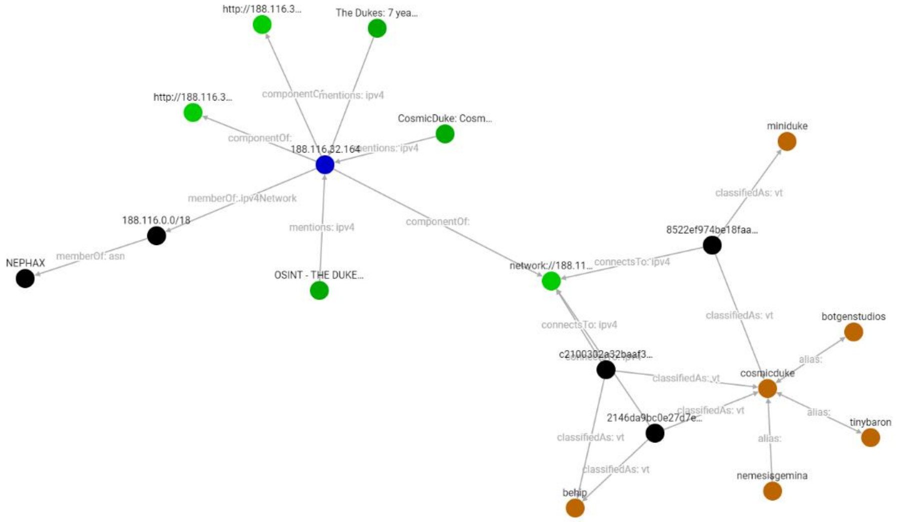
To collect and organize our knowledge of threats to make it useful

Data and Information

Data



Information



mnemonic

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.

NSM

Nordic Financial CERT

Kraft CERT

UiO Universitetet i Oslo

NTNU Norwegian University of Science and Technology

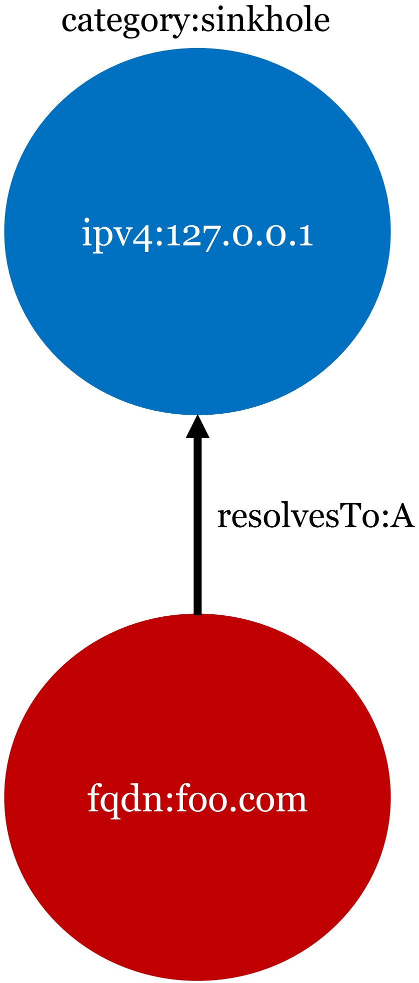
telenor

mnemonic

DATA MODEL

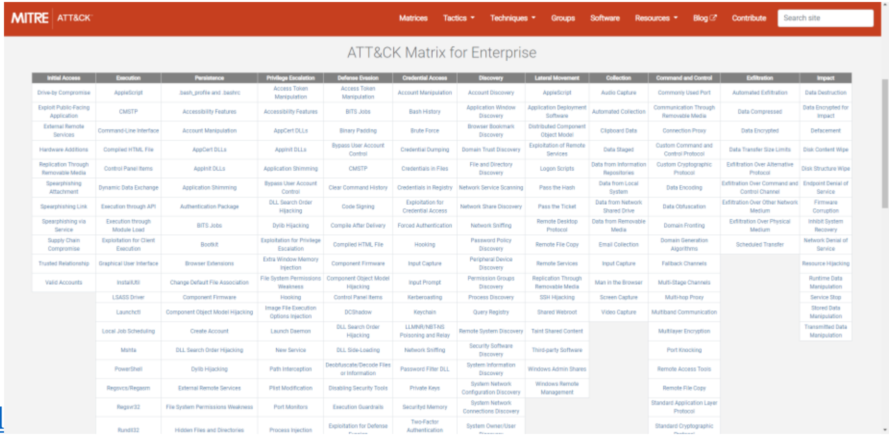
Data Model

- 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



Models, Taxonomies and Vocabularies

- MITRE ATT&CK
  - https://attack.mitre.org
- MITRE PRE-ATT&CK
  - https://attack.mitre.org/pre-attack/
- STIX 2.0 vocabularies
  - https://oasis-open.github.io/cti-documentation/
- Ryan Stillions' DML model
  - http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication	System Owner/User Discovery			Standard Cryptographic Protocol		

Current OSINT Sources

Import:

- APTNotes
  - https://github.com/aptnotes/data
- APT & CyberCriminal Campaign Collection
  - https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
- RSS Feeds
  - Infosec blogs
- MISP (circl.lu feed)
- MITRE ATT&CK

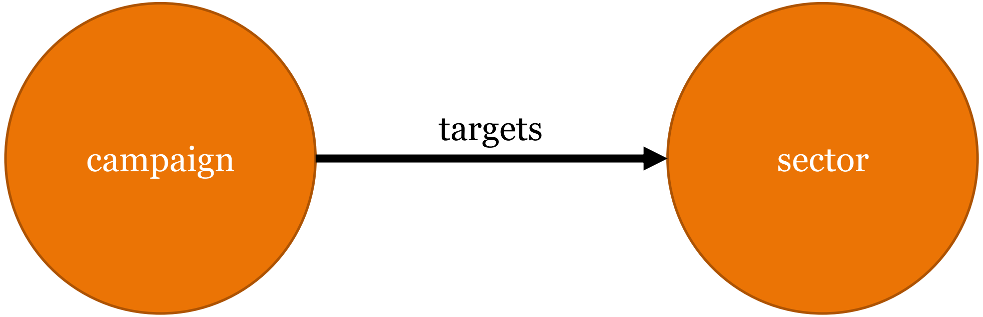
Enrich:

- mnemonic PassiveDNS
  - https://passivedns.mnemonic.no/
- Shadowserver IP-BGP
  - https://www.shadowserver.org/wiki/pmwiki.php/Services/IP-BGP
- VirusTotal

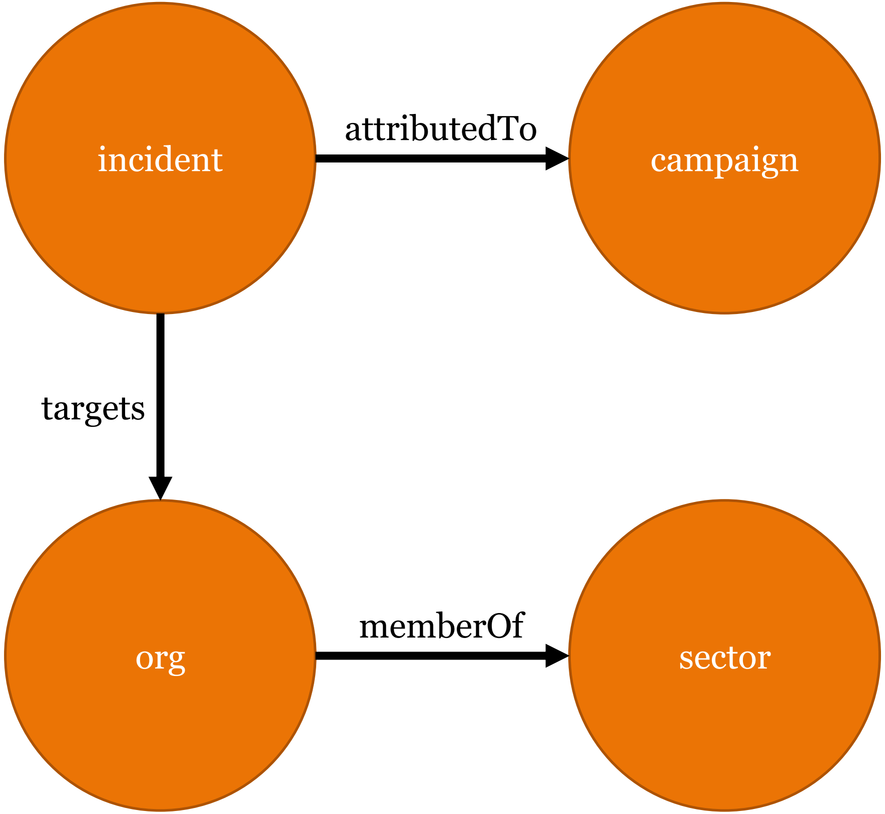
Problems

- Multiple ways to represent the same information
- Different names for the same thing
  - Threat actors
  - Malware

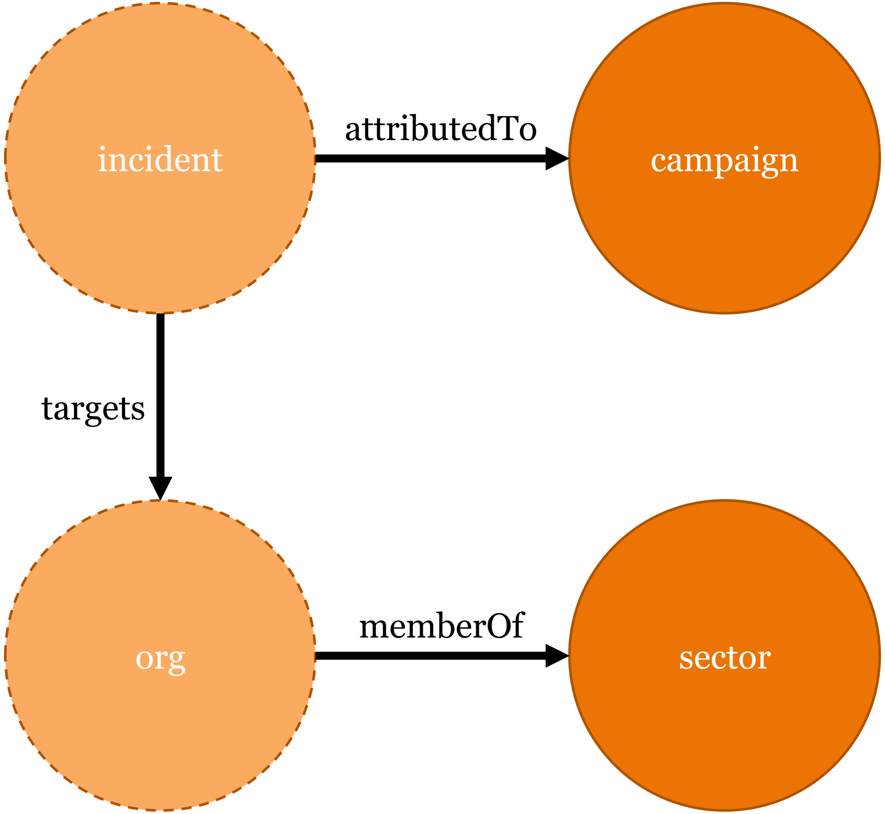
Example: Campaign targets sector



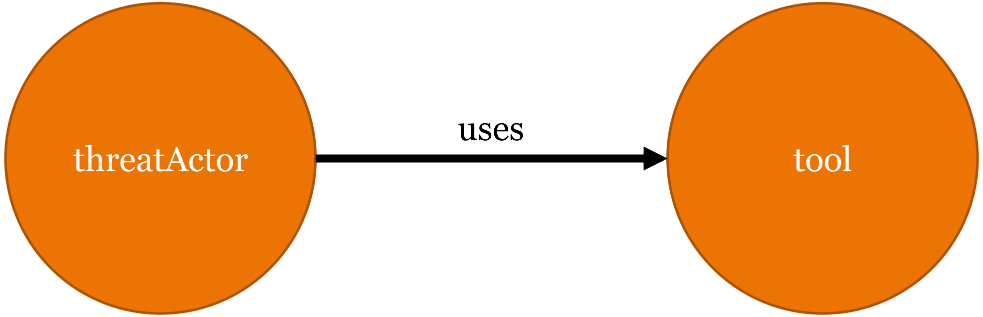
Example: Campaign targets sector



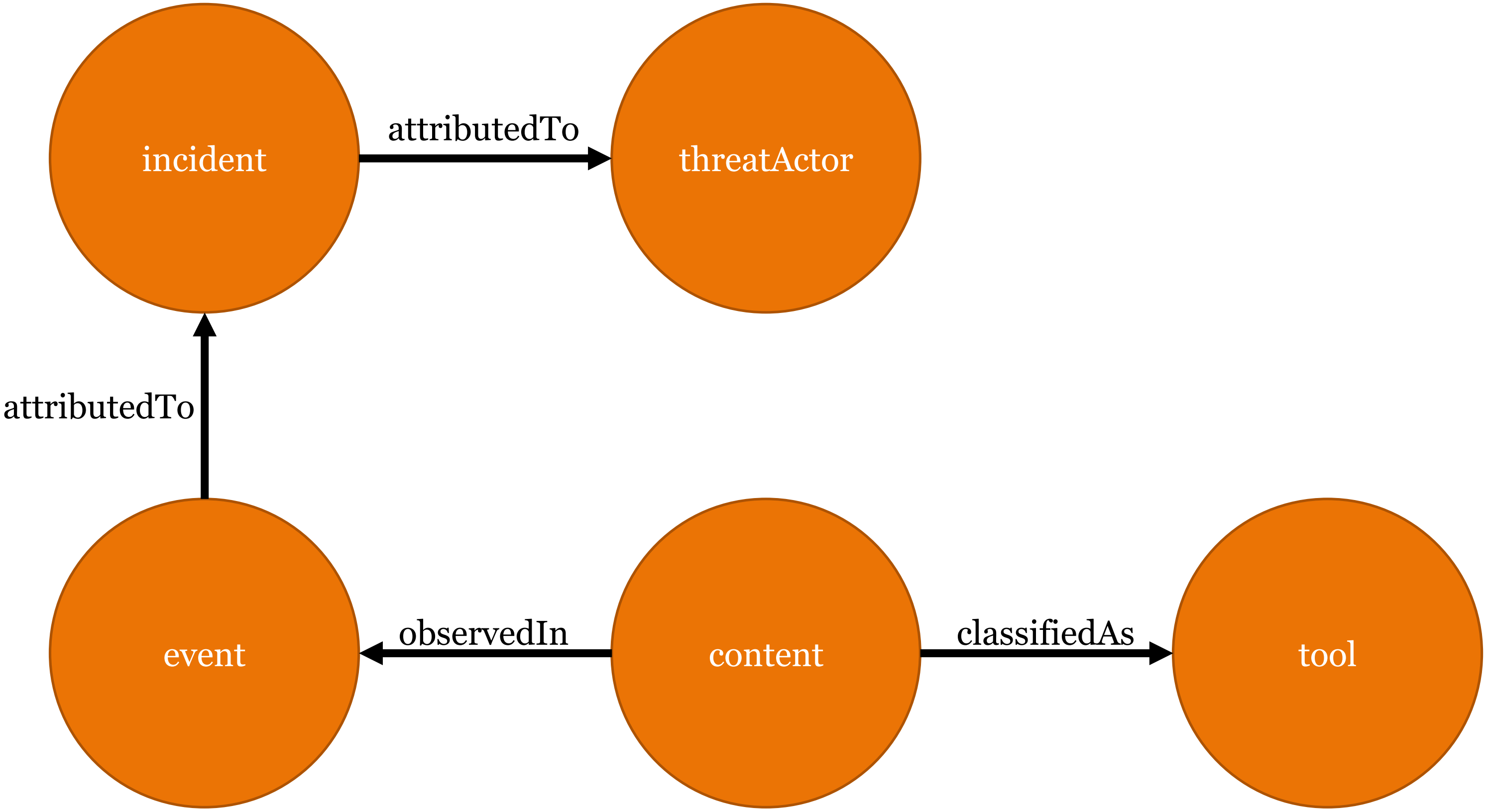
Example: Campaign targets sector



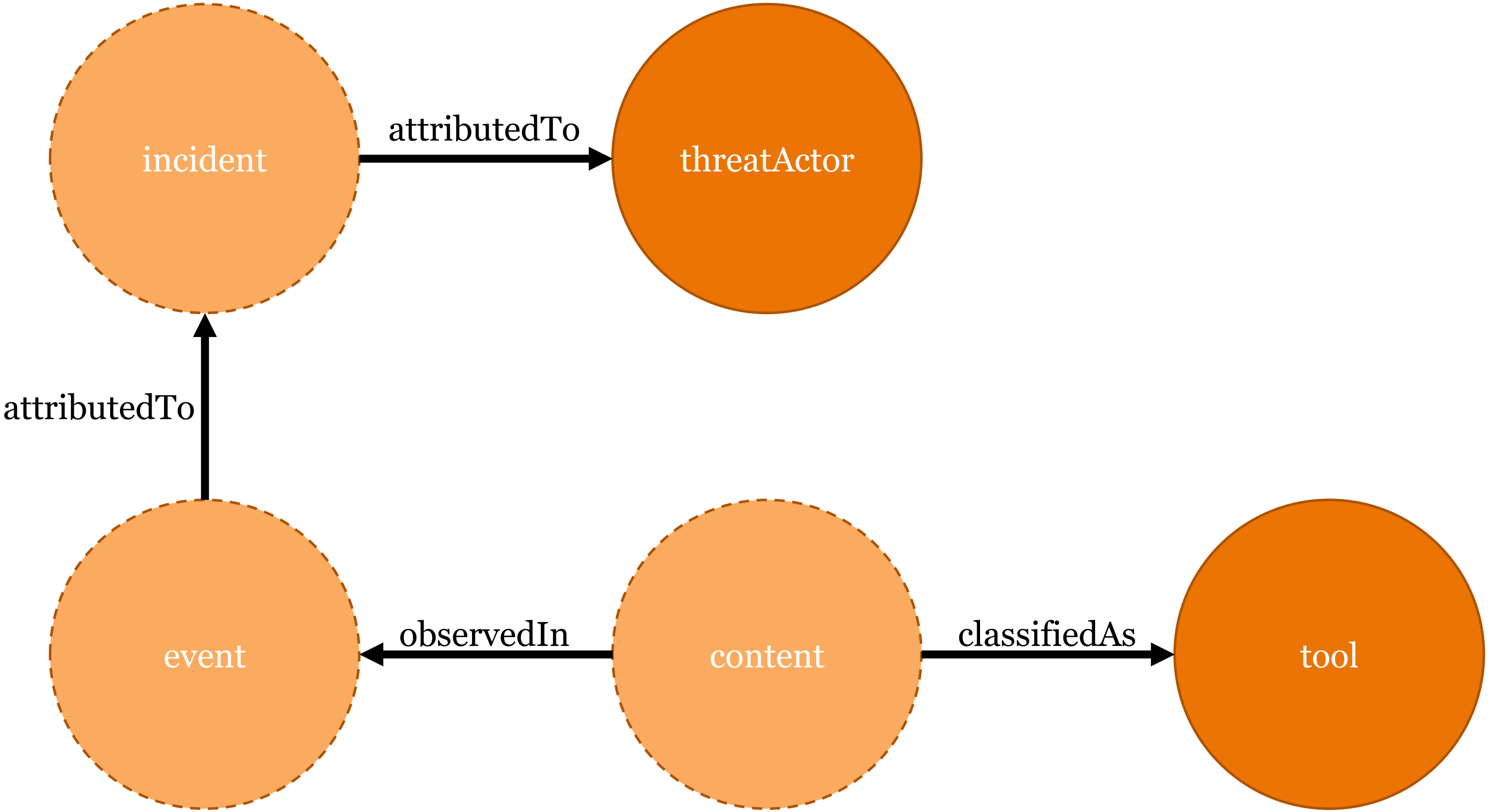
Example: Threat actor uses tool (ATT&CK)



Example: Threat actor uses tool (ATT&CK)

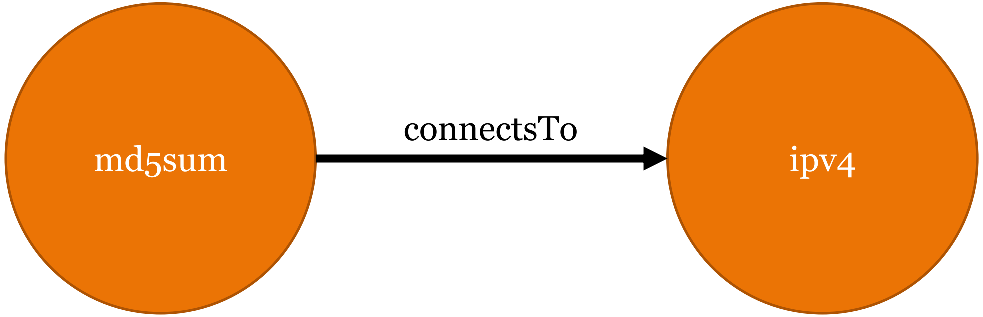


Example: Threat actor uses tool (ATT&CK)

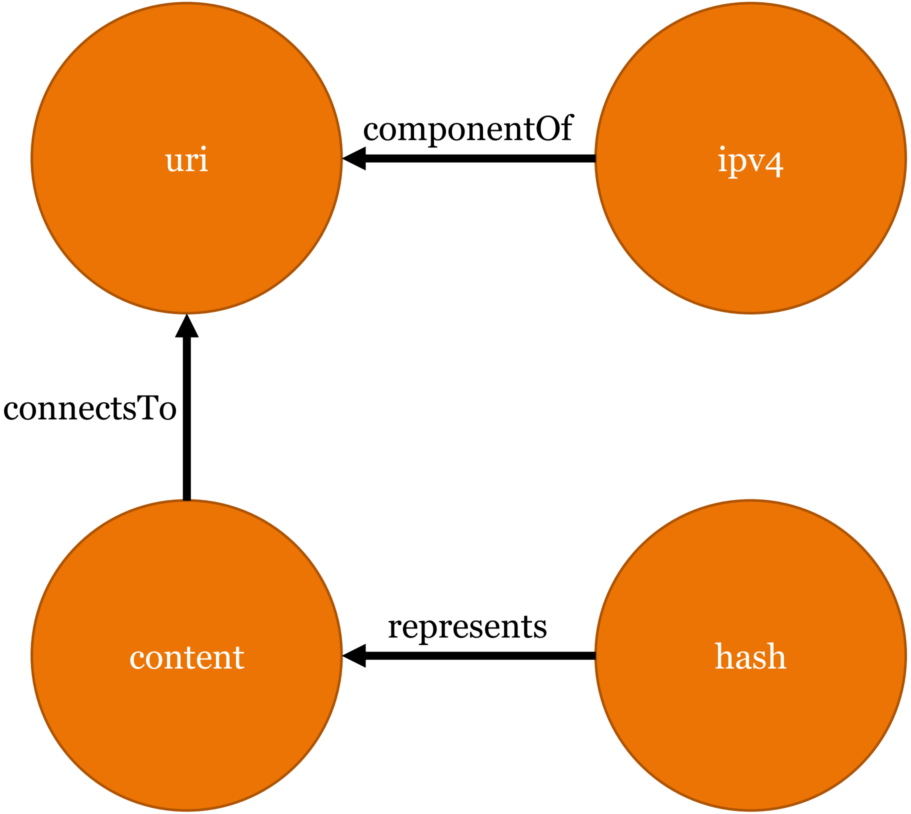


mnemonic

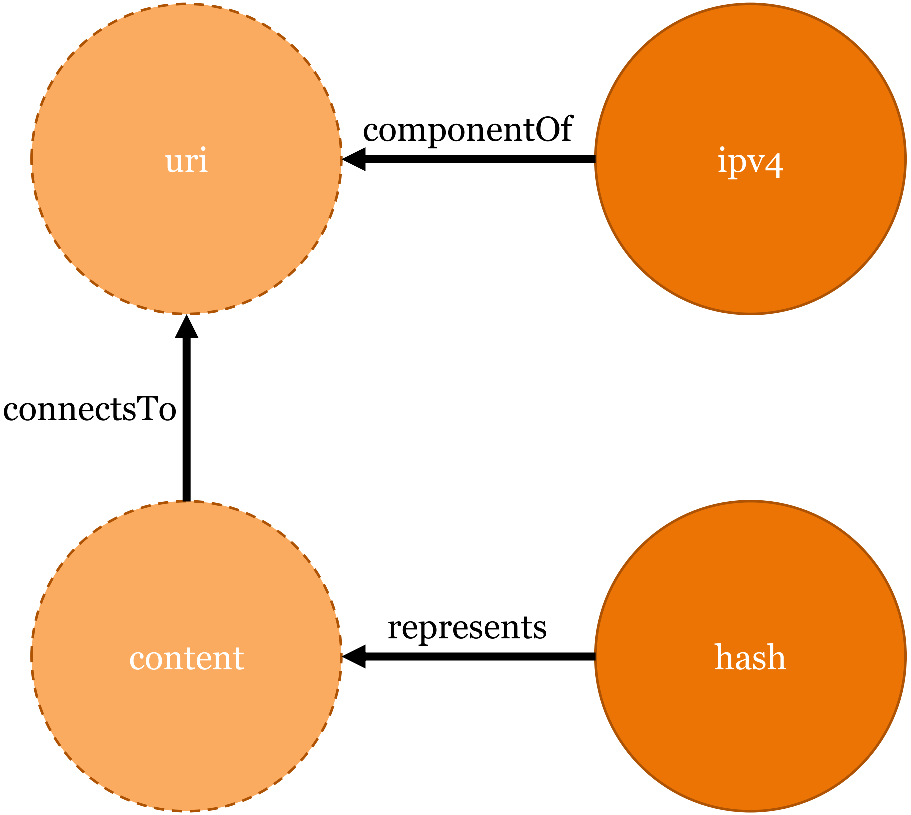
Example: md5sum connects to ipv4



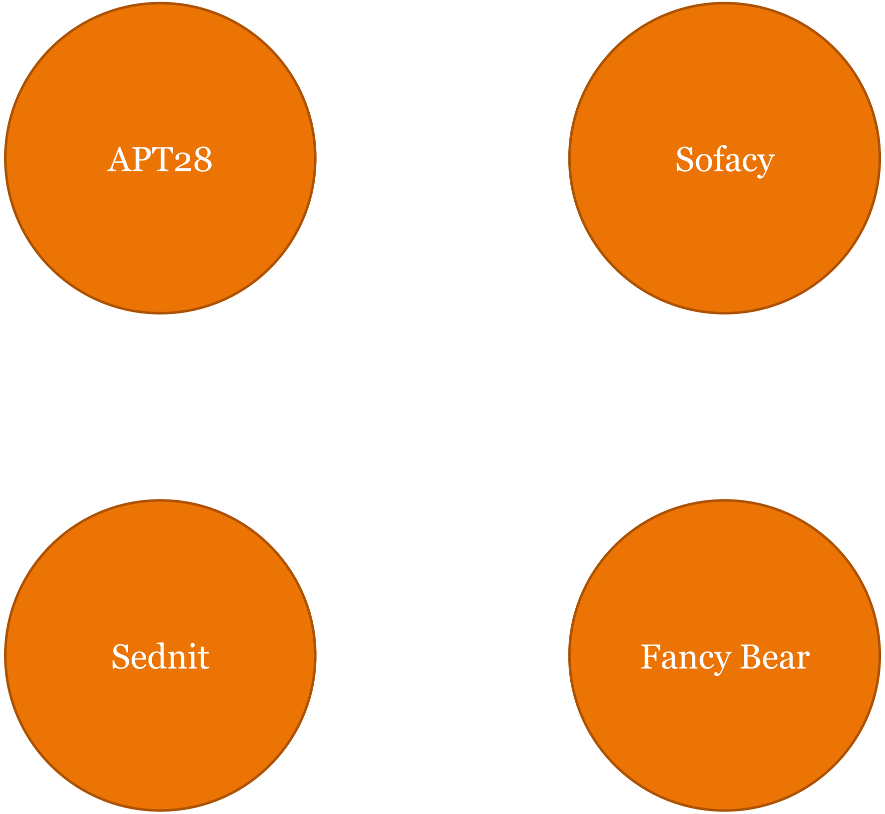
Example: md5sum connects to ipv4



Example: md5sum connects to ipv4



Different names



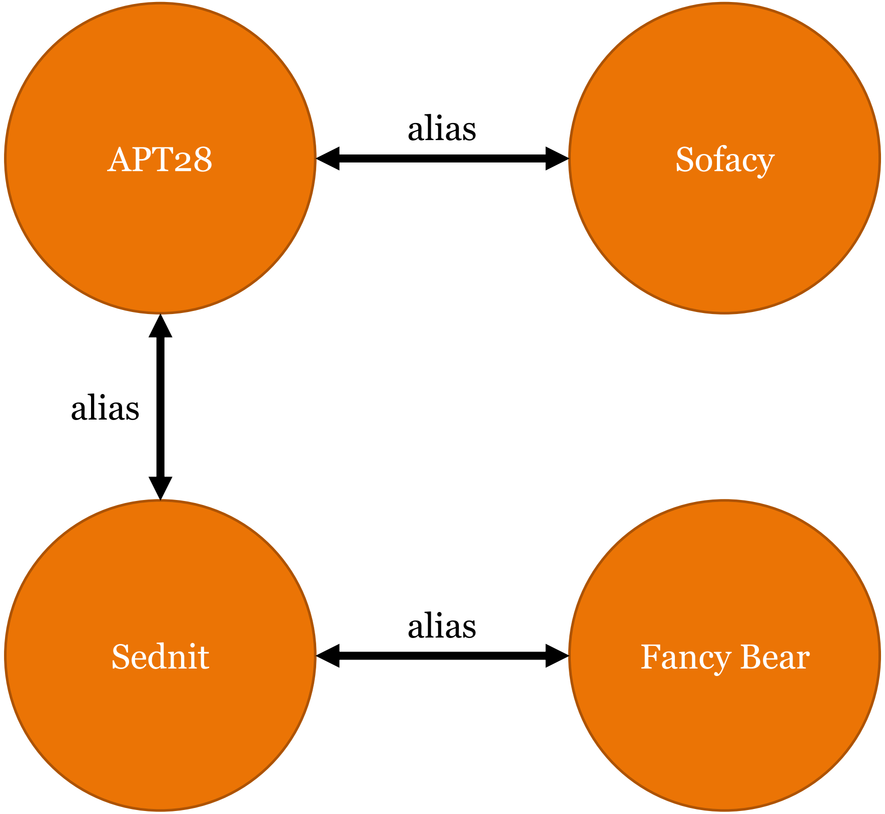
APT28

Sofacy

Sednit

Fancy Bear

Different names



APT28

alias

Sofacy

alias

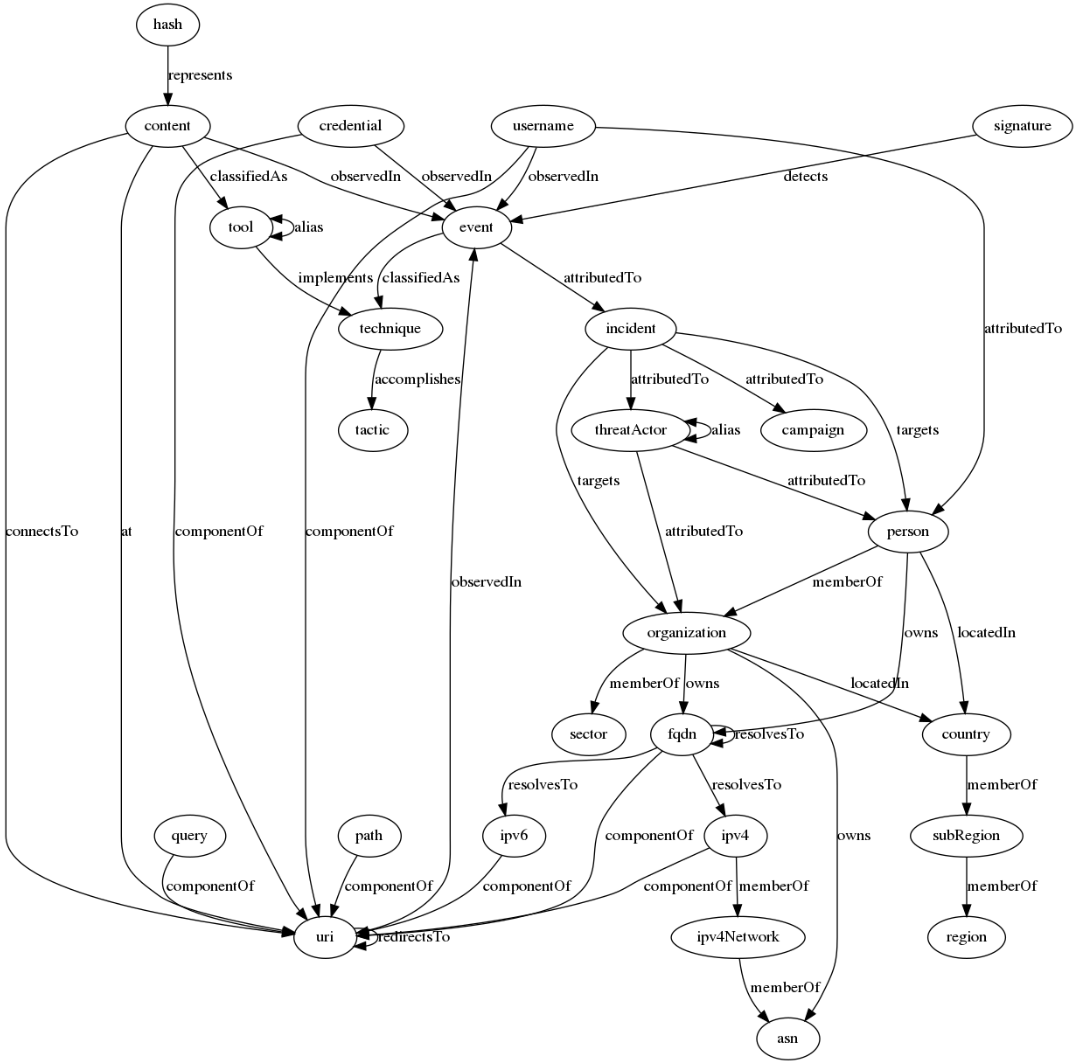
Sednit

alias

Fancy Bear

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



THE ACT PLATFORM

Platform Architecture – Core technologies

Cassandra

APACHE nifi

elasticsearch

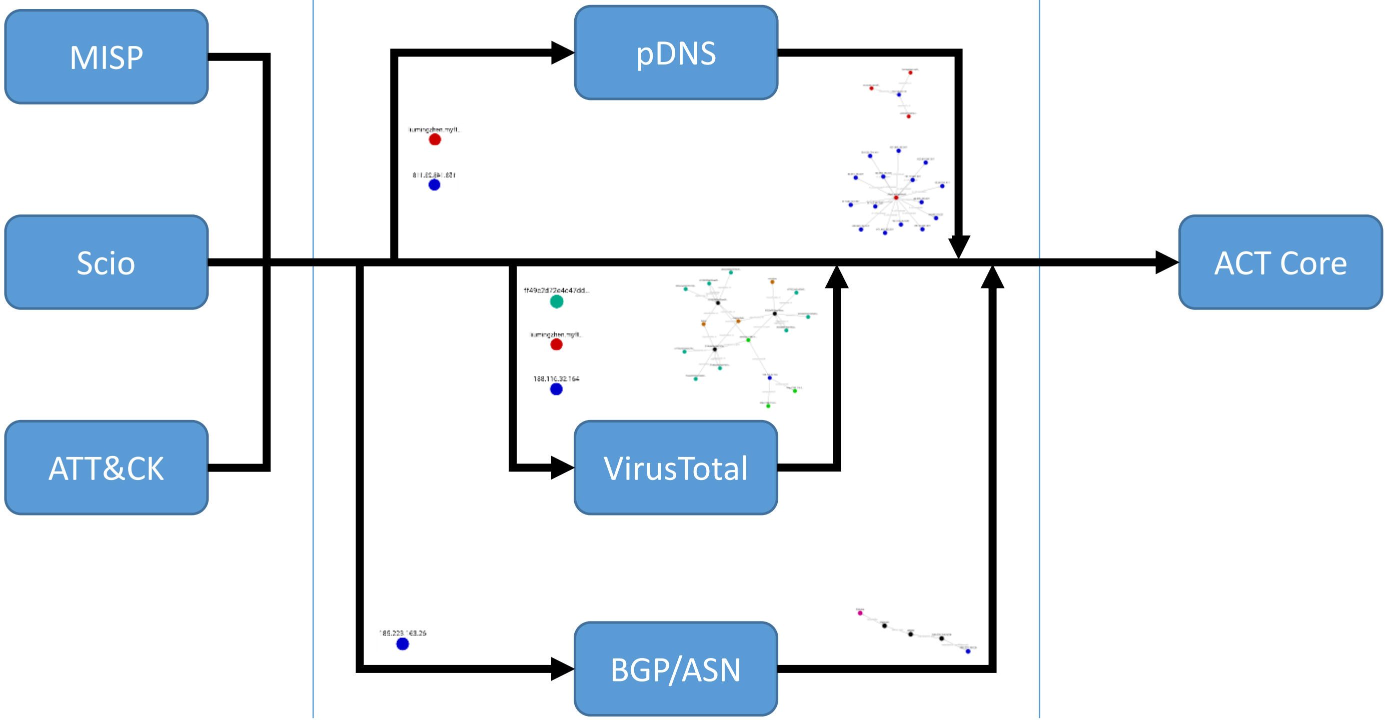
OPEN NLP™

Apache TinkerPop

Import

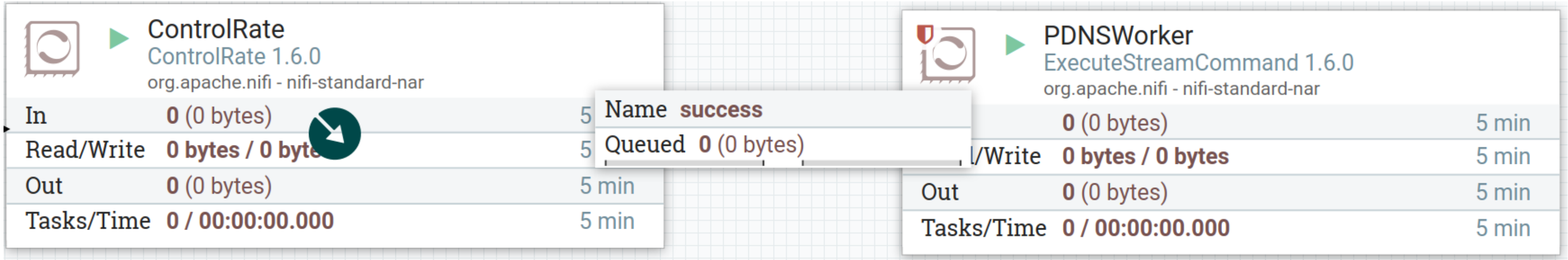
Enrich

Store



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



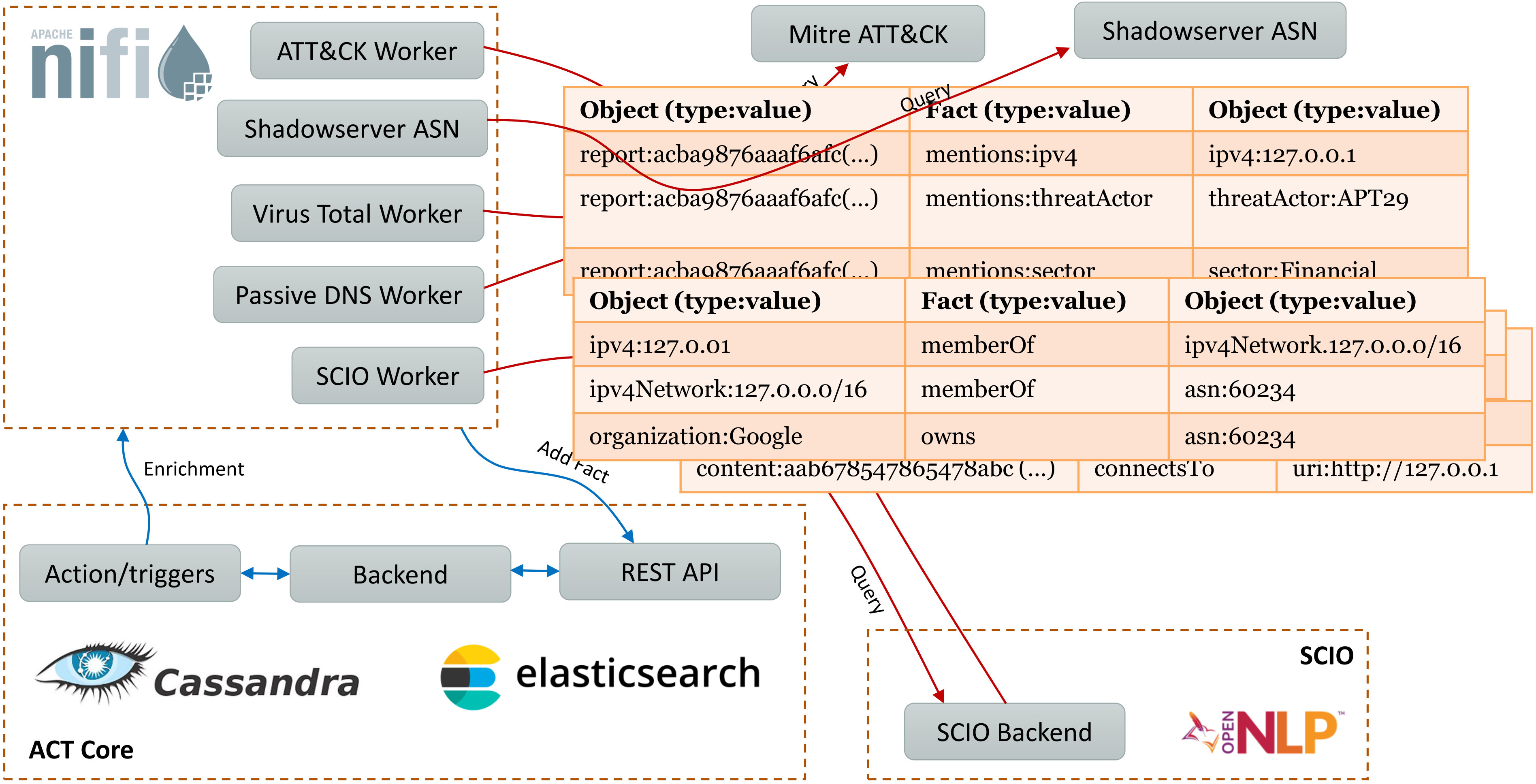
ControlRate
ControlRate 1.6.0
org.apache.nifi - nifi-standard-nar

In	**0** (0 bytes)	5
Read/Write	**0 bytes / 0 byt**	5
Out	**0** (0 bytes)	5 min
Tasks/Time	**0 / 00:00:00.000**	5 min

Name **success**
Queued **0** (0 bytes)

PDNSWorker
ExecuteStreamCommand 1.6.0
org.apache.nifi - nifi-standard-nar

	0 (0 bytes)	5 min
l/Write	**0 bytes / 0 bytes**	5 min
Out	**0** (0 bytes)	5 min
Tasks/Time	**0 / 00:00:00.000**	5 min



Object (type:value)	Fact (type:value)	Object (type:value)
report:acba9876aaaf6afc(...)	mentions:ipv4	ipv4:127.0.0.1
report:acba9876aaaf6afc(...)	mentions:threatActor	threatActor:APT29
report:acba9876aaaf6afc(...)	mentions:sector	sector:Financial

Object (type:value)	Fact (type:value)	Object (type:value)
ipv4:127.0.01	memberOf	ipv4Network.127.0.0.0/16
ipv4Network:127.0.0.0/16	memberOf	asn:60234
organization:Google	owns	asn:60234

content:aab678547865478abc (...)	connectsTo	uri:http://127.0.0.1

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)

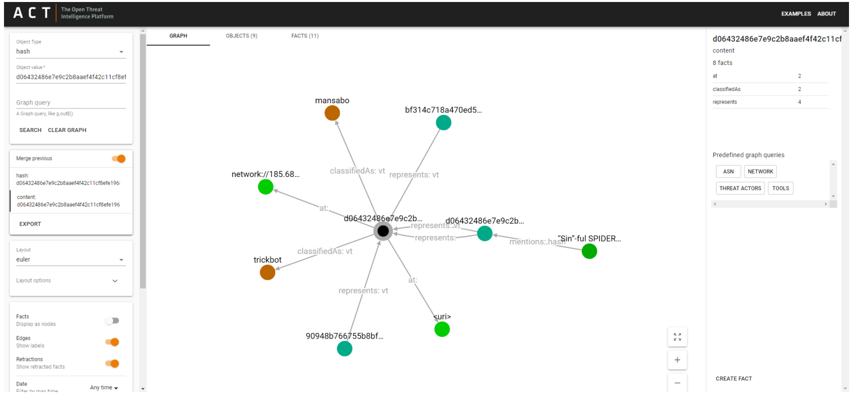
- Apache Tinkerpop implemented on top of Cassandra/Elasticsearch

- Graph queries opens up a range of possibilites that is not possible on a flat data structure

Apache TinkerPop

Gremlin

$G = (V, E)$



Object Type
hash

Object value *
d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query
A Graph query, like g.outE()

Merge previous

hash:
d06432486e7e9c2b8aaef4f42c11cf8efe196

content:
d06432486e7e9c2b8aaef4f42c11cf8efe196

Layout
euler

Facts
Display as nodes

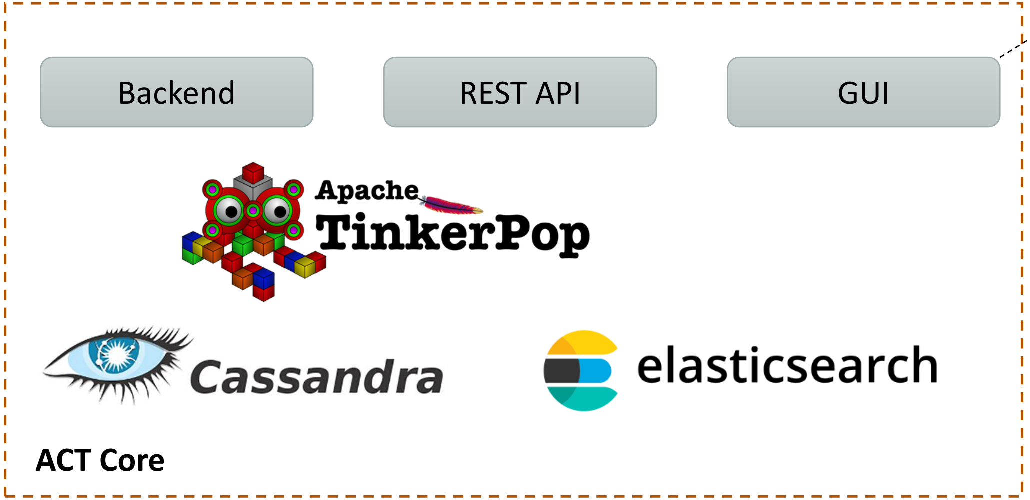
Edges
Show labels

Retractions
Show retracted facts

Date
Filter by max time
Any time

d06432486e7e9c2b8aaef4f42c11cf
content
8 facts

at	2
classifiedAs	2
represents	4



Backend

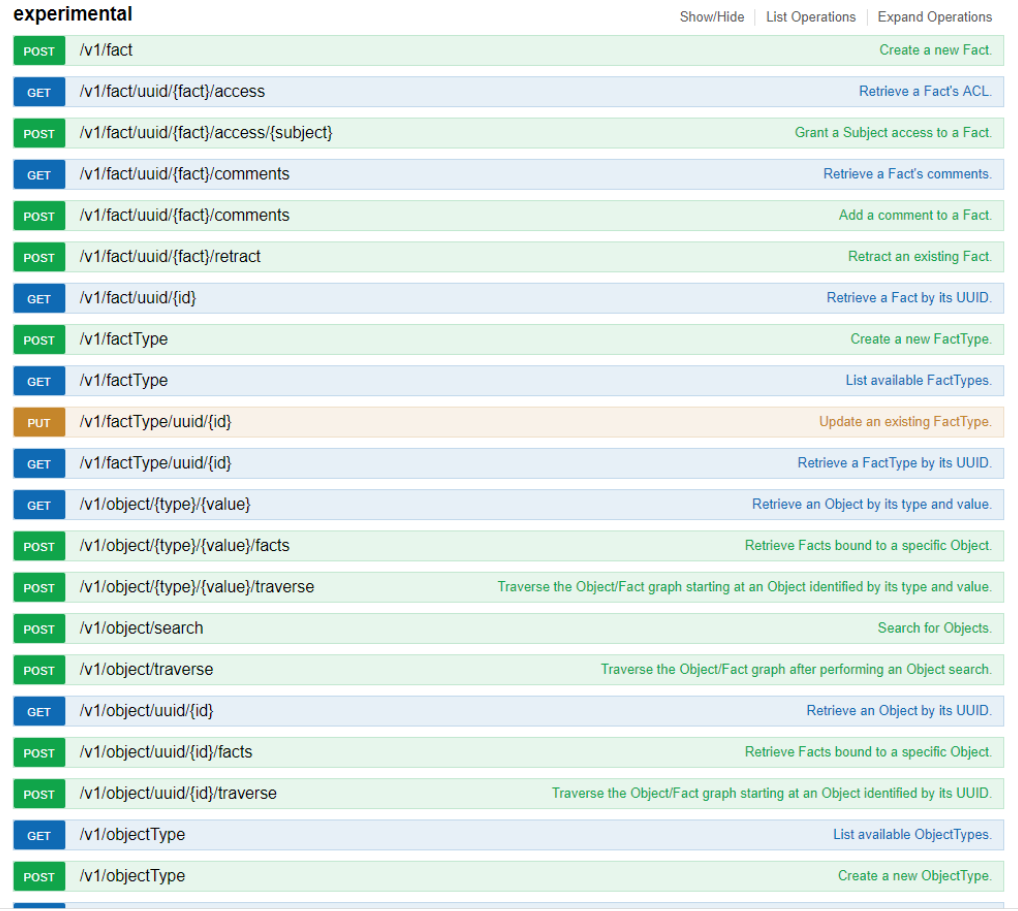
REST API

GUI

ACT Core

mnemonic

API - Swagger

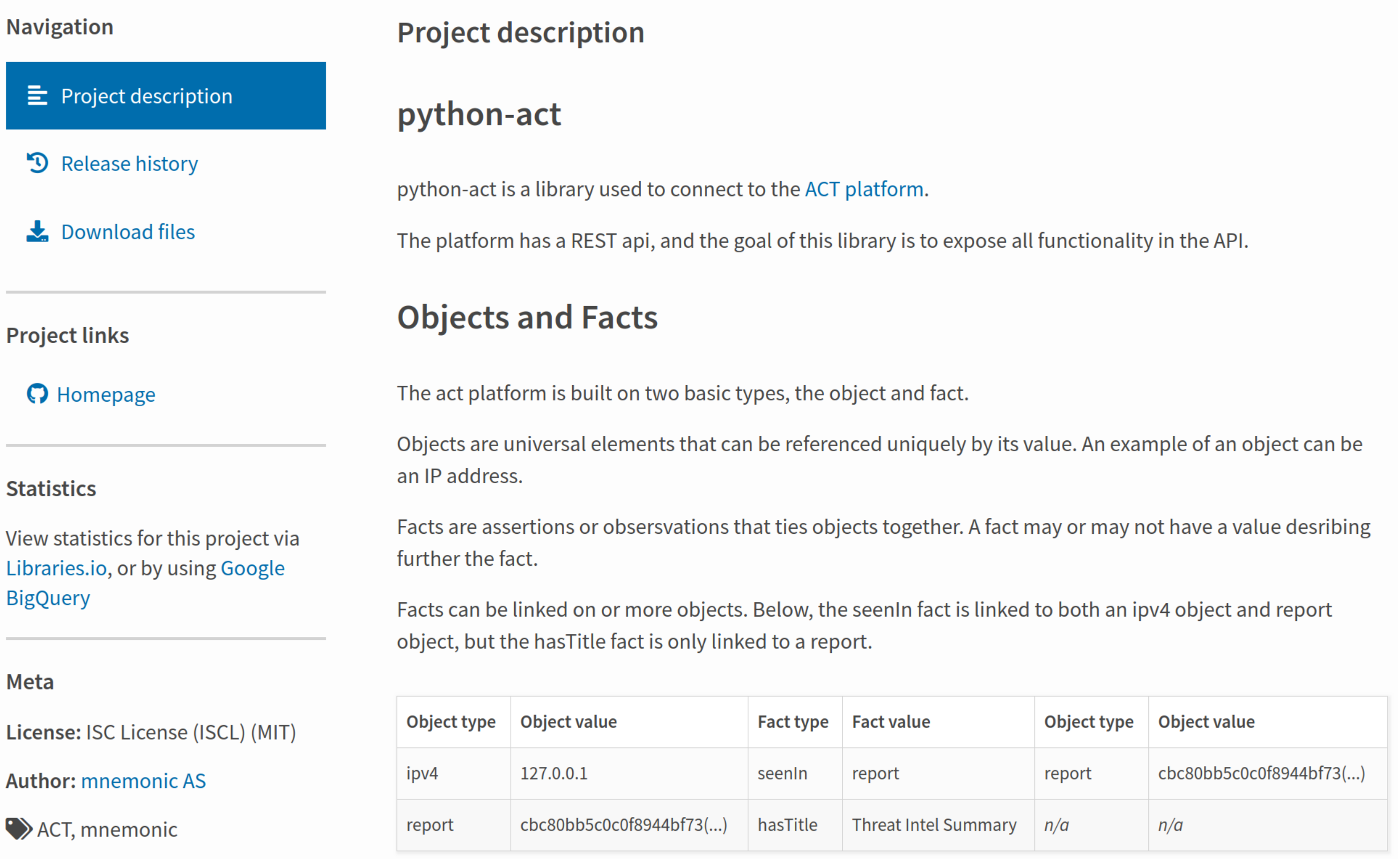


experimental

Show/Hide | List Operations | Expand Operations

POST	/v1/fact	Create a new Fact.
GET	/v1/fact/uuid/{fact}/access	Retrieve a Fact's ACL.
POST	/v1/fact/uuid/{fact}/access/{subject}	Grant a Subject access to a Fact.
GET	/v1/fact/uuid/{fact}/comments	Retrieve a Fact's comments.
POST	/v1/fact/uuid/{fact}/comments	Add a comment to a Fact.
POST	/v1/fact/uuid/{fact}/retract	Retract an existing Fact.
GET	/v1/fact/uuid/{id}	Retrieve a Fact by its UUID.
POST	/v1/factType	Create a new FactType.
GET	/v1/factType	List available FactTypes.
PUT	/v1/factType/uuid/{id}	Update an existing FactType.
GET	/v1/factType/uuid/{id}	Retrieve a FactType by its UUID.
GET	/v1/object/{type}/{value}	Retrieve an Object by its type and value.
POST	/v1/object/{type}/{value}/facts	Retrieve Facts bound to a specific Object.
POST	/v1/object/{type}/{value}/traverse	Traverse the Object/Fact graph starting at an Object identified by its type and value.
POST	/v1/object/search	Search for Objects.
POST	/v1/object/traverse	Traverse the Object/Fact graph after performing an Object search.
GET	/v1/object/uuid/{id}	Retrieve an Object by its UUID.
POST	/v1/object/uuid/{id}/facts	Retrieve Facts bound to a specific Object.
POST	/v1/object/uuid/{id}/traverse	Traverse the Object/Fact graph starting at an Object identified by its UUID.
GET	/v1/objectType	List available ObjectTypes.
POST	/v1/objectType	Create a new ObjectType.

API – Python library (act-api on pypi)



Project links

Homepage

Statistics

View statistics for this project via Libraries.io, or by using Google BigQuery

Meta

License: ISC License (ISCL) (MIT)

Author: mnemonic AS

ACT, mnemonic

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.

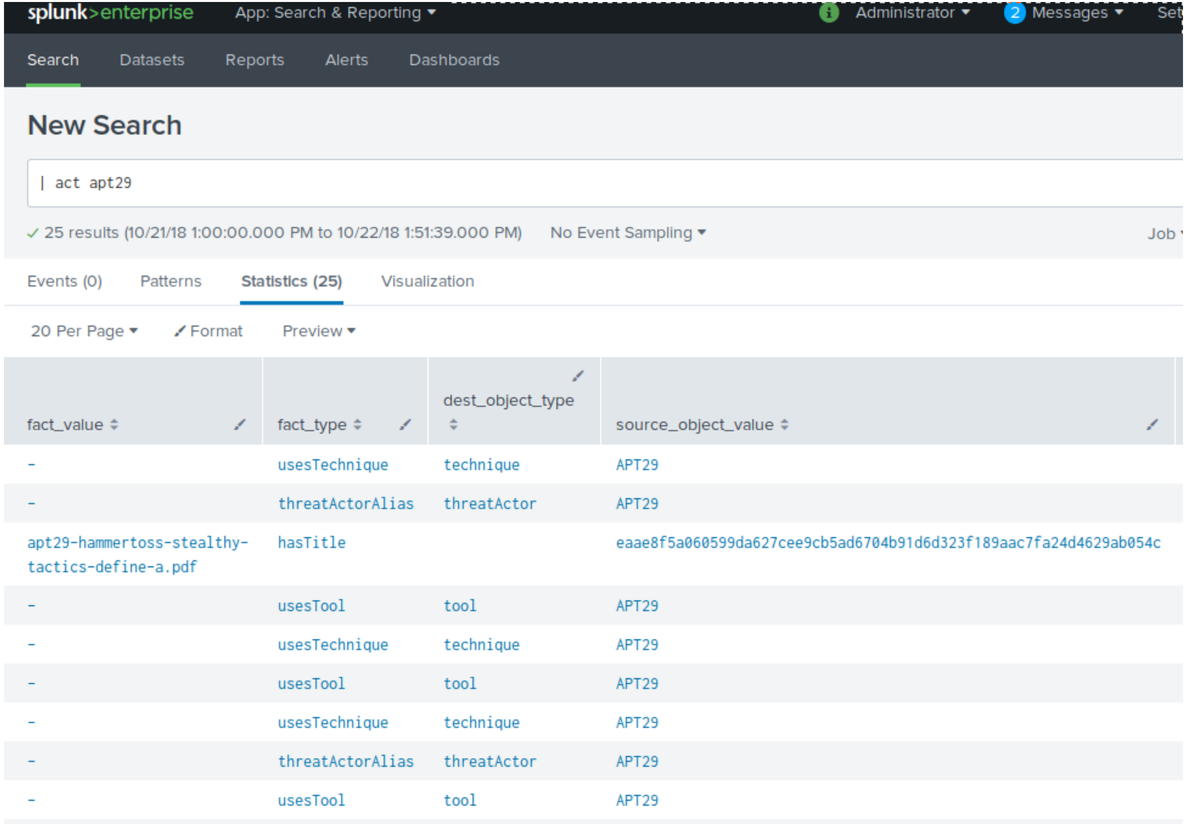
Objects are universal elements that can be referenced uniquely by its value. An example of an object can be an IP address.

Facts are assertions or obsersvations that ties objects together. A fact may or may not have a value desribing 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.

Object type	Object value	Fact type	Fact value	Object type	Object value
ipv4	127.0.0.1	seenIn	report	report	cbc80bb5c0c0f8944bf73(...)
report	cbc80bb5c0c0f8944bf73(...)	hasTitle	Threat Intel Summary	*n/a*	*n/a*

Splunk Add-on - Queries

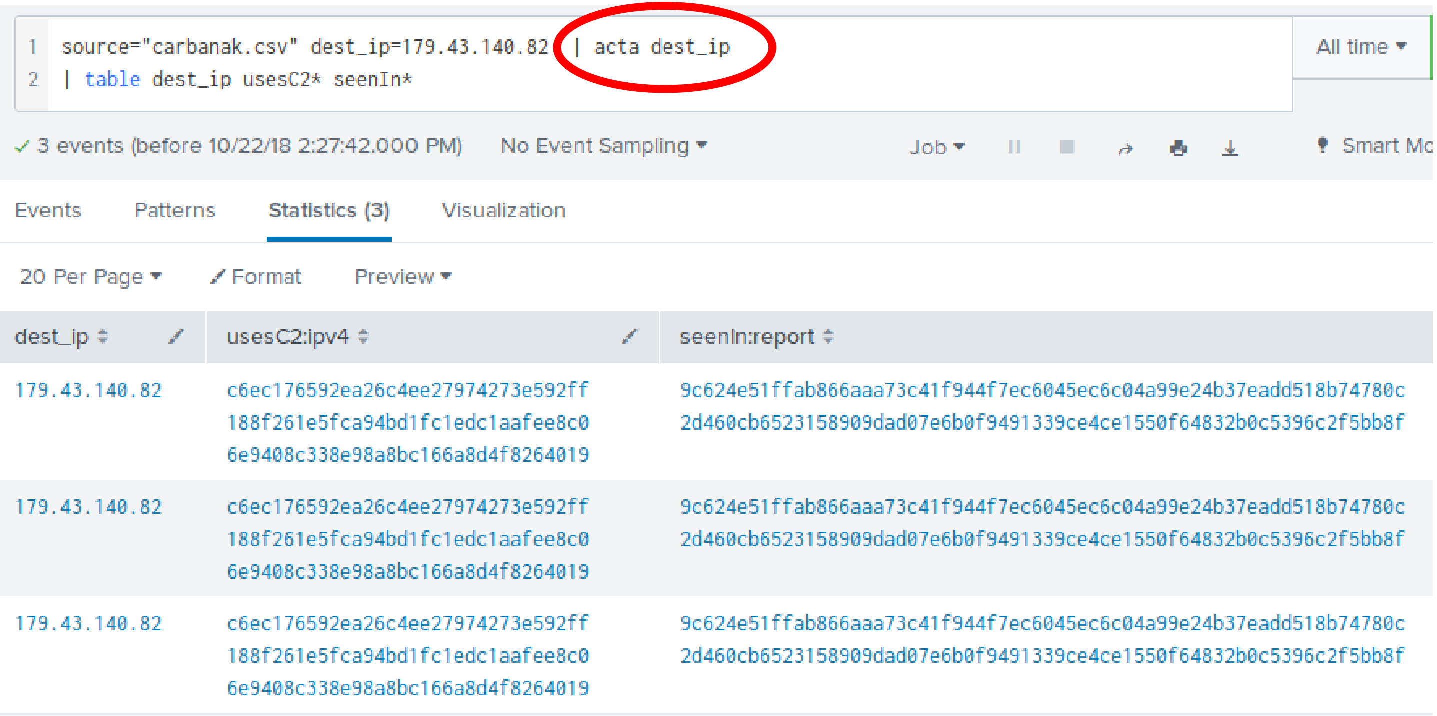


```
| act apt29
```

✓ 25 results (10/21/18 1:00:00.000 PM to 10/22/18 1:51:39.000 PM)

fact_value	fact_type	dest_object_type	source_object_value
-	usesTechnique	technique	APT29
-	threatActorAlias	threatActor	APT29
apt29-hammertoss-stealthy-tactics-define-a.pdf	hasTitle		eaae8f5a060599da627cee9cb5ad6704b91d6d323f189aac7fa24d4629ab054c
-	usesTool	tool	APT29
-	usesTechnique	technique	APT29
-	usesTool	tool	APT29
-	usesTechnique	technique	APT29
-	threatActorAlias	threatActor	APT29
-	usesTool	tool	APT29

Splunk Add-on – Annotate search results



```
source="carbanak.csv" dest_ip=179.43.140.82 | acta dest_ip
| table dest_ip usesC2* seenIn*
```

✓ 3 events (before 10/22/18 2:27:42.000 PM) No Event Sampling ▾

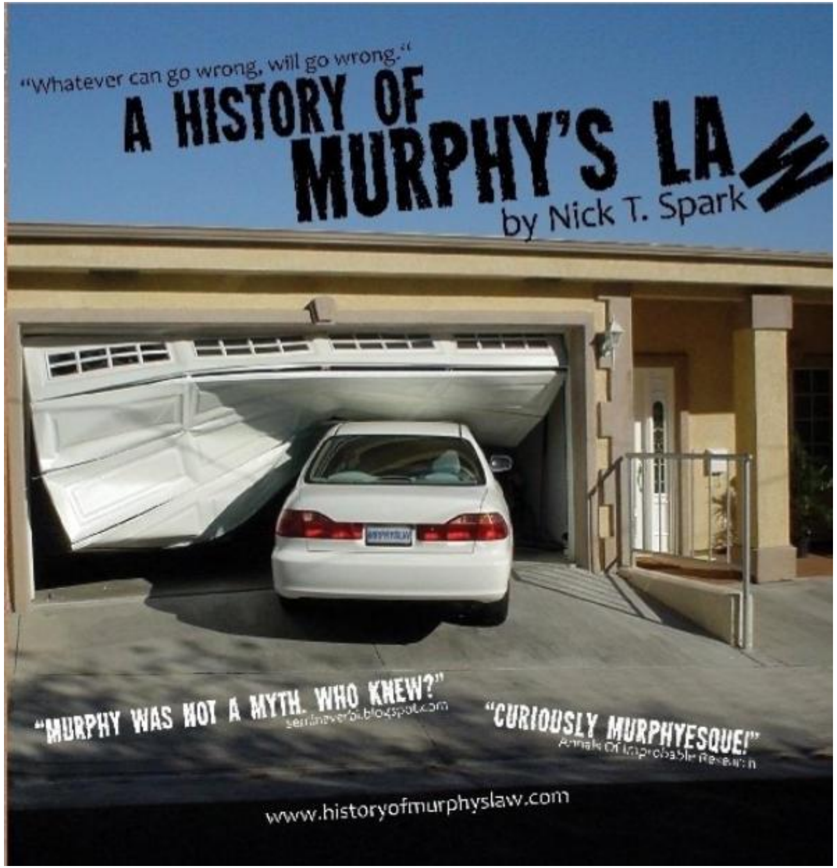
dest_ip	usesC2:ipv4	seenIn:report
179.43.140.82	c6ec176592ea26c4ee27974273e592ff 188f261e5fca94bd1fc1edc1aafee8c0 6e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f
179.43.140.82	c6ec176592ea26c4ee27974273e592ff 188f261e5fca94bd1fc1edc1aafee8c0 6e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f
179.43.140.82	c6ec176592ea26c4ee27974273e592ff 188f261e5fca94bd1fc1edc1aafee8c0 6e9408c338e98a8bc166a8d4f8264019	9c624e51ffab866aaa73c41f944f7ec6045ec6c04a99e24b37eadd518b74780c 2d460cb6523158909dad07e6b0f9491339ce4ce1550f64832b0c5396c2f5bb8f

Threat Intelligence Platform - Summary

- Github repositories
  - https://github.com/mnemonic-no/act (installation docs)
  - 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)
- Public AWS instance
  - https://act-eu1.mnemonic.no

TRAINING - INTRODUCTION

Before We Start


"Whatever can go wrong, will go wrong."
A HISTORY OF MURPHY'S LAW
by Nick T. Spark
"MURPHY WAS NOT A MYTH. WHO KNEW?"
seminaverbi.blogspot.com
"CURIOUSLY MURPHYESQUE!"
Annals Of Improbable Research
www.historyofmurphyslaw.com

Periscope Film LLC [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

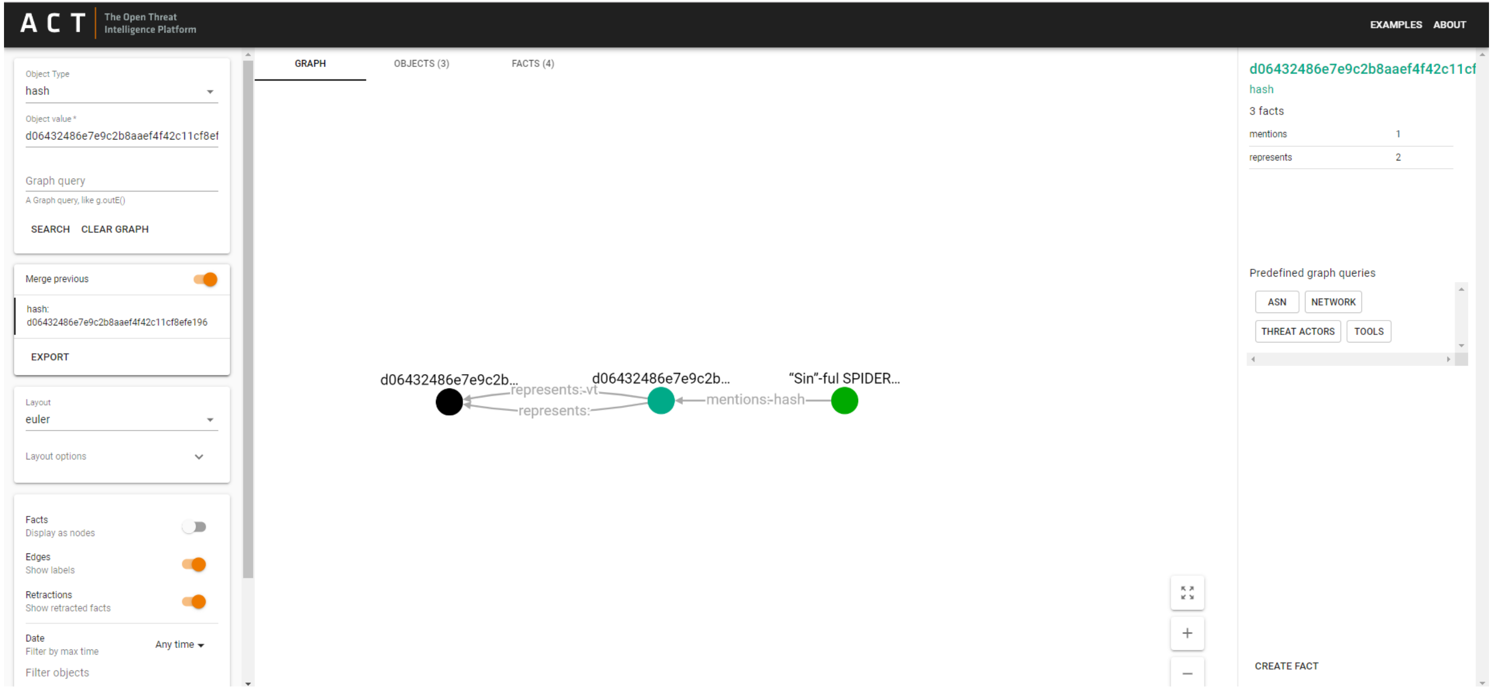
Accessing the read-only AWS instance

GUI:
https://act-eu1.mnemonic.no

Tasks:
https://act-eu1.mnemonic.no/examples/

API:
https://act-eu1.mnemonic.no/swagger/

Introduction 1



Object Type: hash

Object value *: d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query

A Graph query, like g.outE()

Merge previous

hash: d06432486e7e9c2b8aaef4f42c11cf8efe196

Layout: euler

Layout options

Facts — Display as nodes

Edges — Show labels

Retractions — Show retracted facts

Date — Filter by max time: Any time

Filter objects

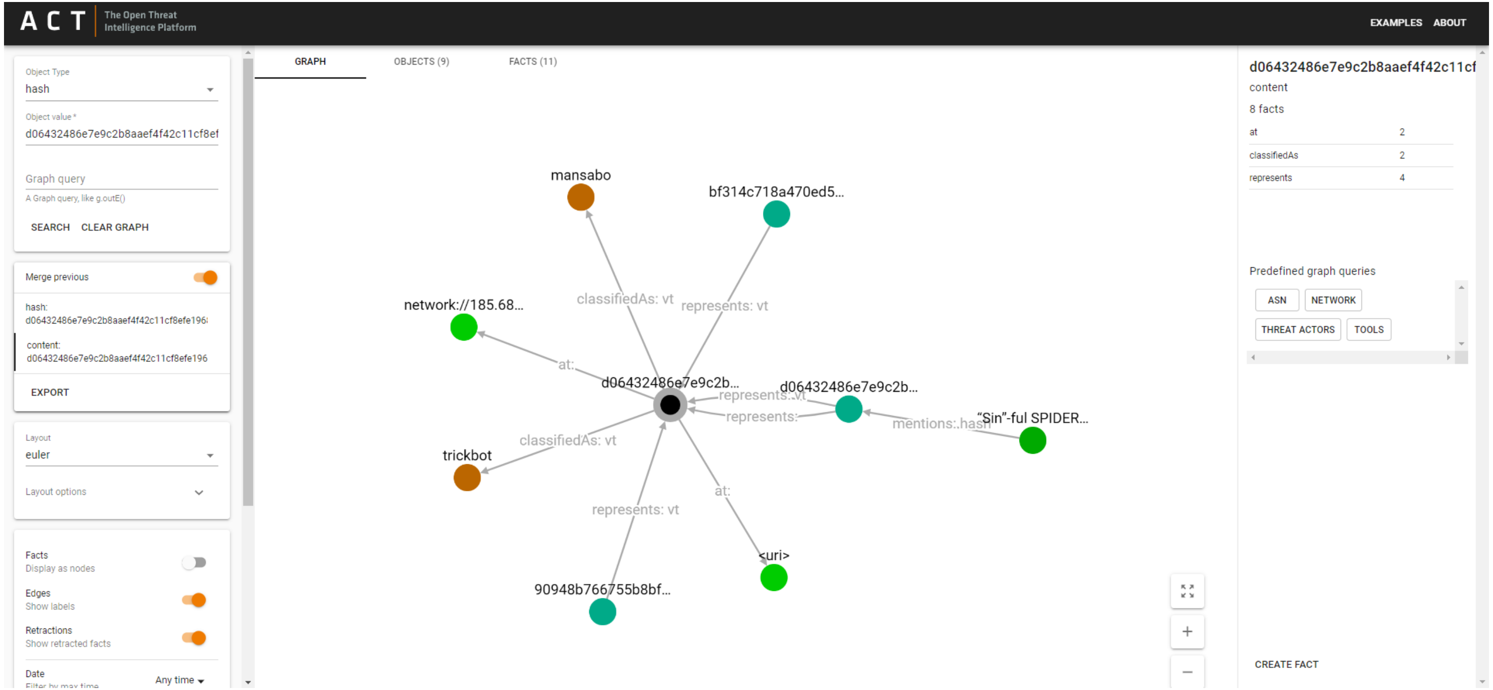
d06432486e7e9c2b8aaef4f42c11cf

hash

3 facts

mentions	1
represents	2

Introduction 1 – Click and Double-click



Object Type
hash

Object value *
d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query
A Graph query, like g.outE()

Merge previous

hash:
d06432486e7e9c2b8aaef4f42c11cf8efe196

content:
d06432486e7e9c2b8aaef4f42c11cf8efe196

Layout
euler

Facts
Display as nodes

Edges
Show labels

Retractions
Show retracted facts

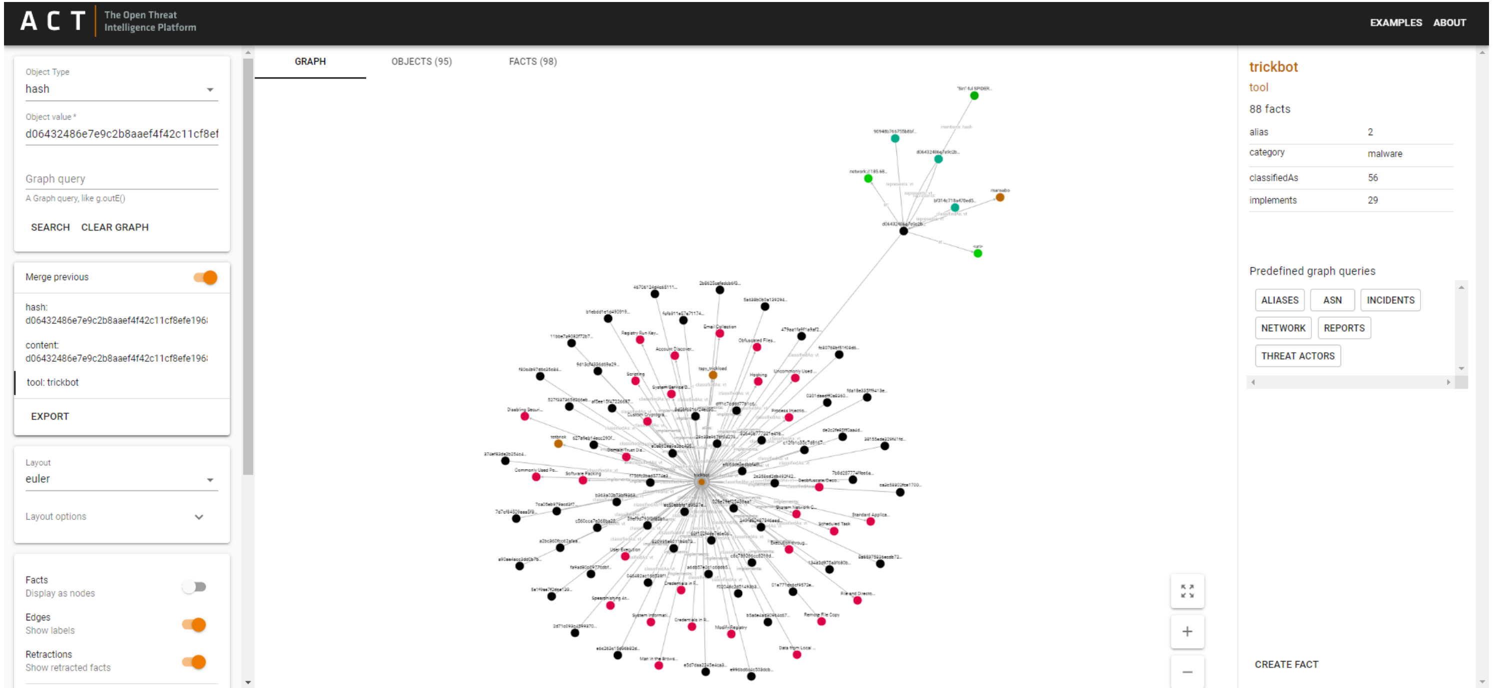
Date
Filter by max time
Any time

d06432486e7e9c2b8aaef4f42c11cf
content
8 facts

at	2
classifiedAs	2
represents	4

Predefined graph queries

Introduction 1 – History, Layouts and Filtering



Object Type: hash

Object value *: d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query
A Graph query, like g.outE()

Merge previous

hash: d06432486e7e9c2b8aaef4f42c11cf8efe196

content: d06432486e7e9c2b8aaef4f42c11cf8efe196

tool: trickbot

Layout: euler

Layout options

Facts
Display as nodes

Edges
Show labels

Retractions
Show retracted facts

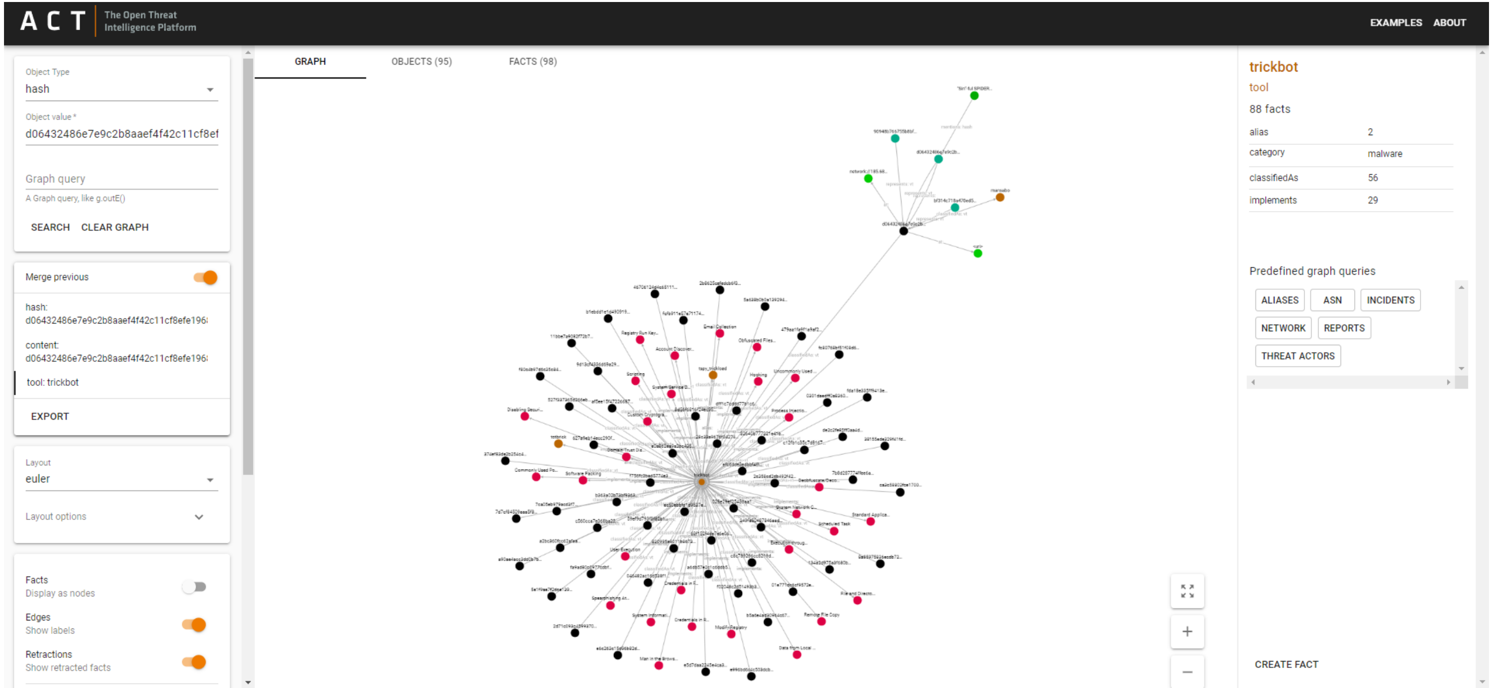
trickbot
tool
88 facts

alias	2
category	malware
classifiedAs	56
implements	29

Predefined graph queries

mnemonic

Introduction 1 – Fact Types



Object Type
hash

Object value *
d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query
A Graph query, like g.outE()

Merge previous

hash:
d06432486e7e9c2b8aaef4f42c11cf8efe196

content:
d06432486e7e9c2b8aaef4f42c11cf8efe196

tool: trickbot

Layout
euler

Layout options

Facts
Display as nodes

Edges
Show labels

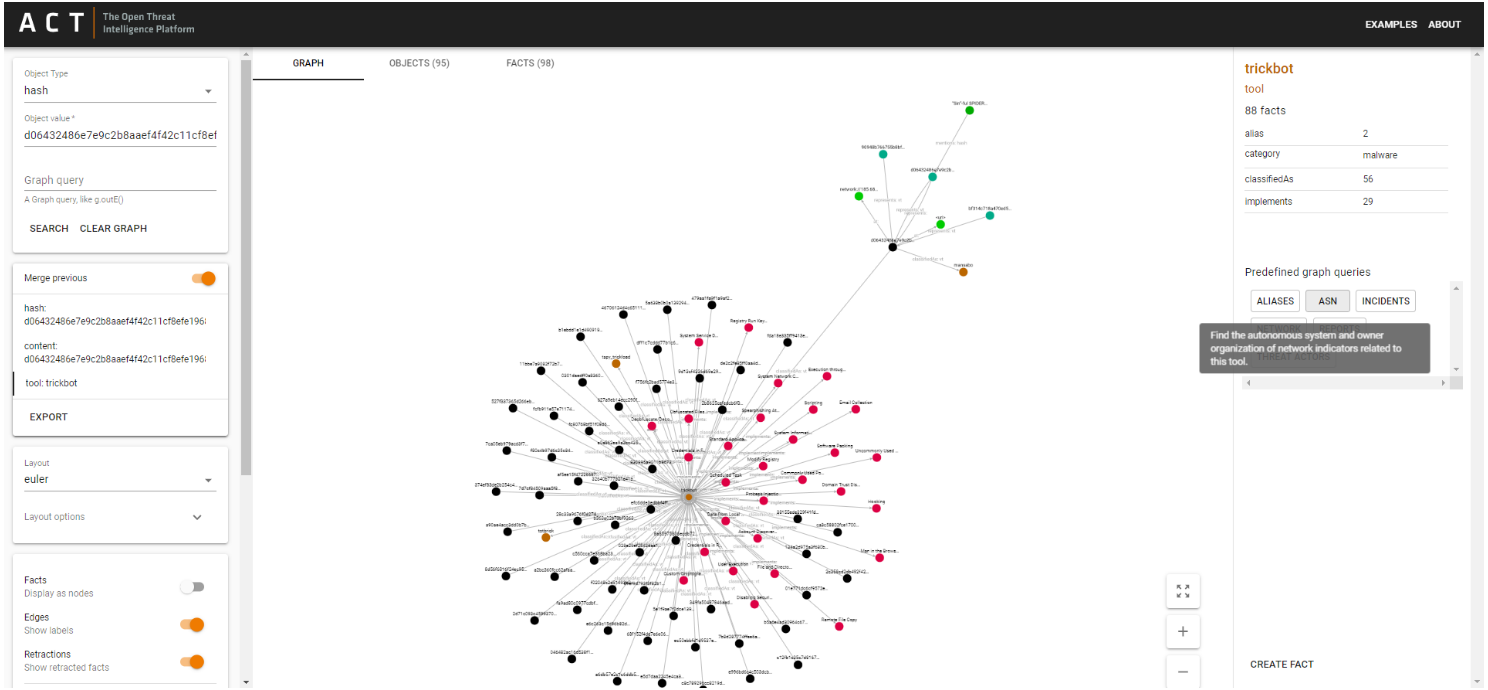
Retractions
Show retracted facts

trickbot
tool
88 facts

alias	2
category	malware
classifiedAs	56
implements	29

Predefined graph queries

Introduction 1 – Graph Queries



Object Type: hash

Object value *: d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query

A Graph query, like g.outE()

Merge previous

hash: d06432486e7e9c2b8aaef4f42c11cf8efe196

content: d06432486e7e9c2b8aaef4f42c11cf8efe196

tool: trickbot

Layout: euler

Layout options

Facts – Display as nodes

Edges – Show labels

Retractions – Show retracted facts

trickbot

tool

88 facts

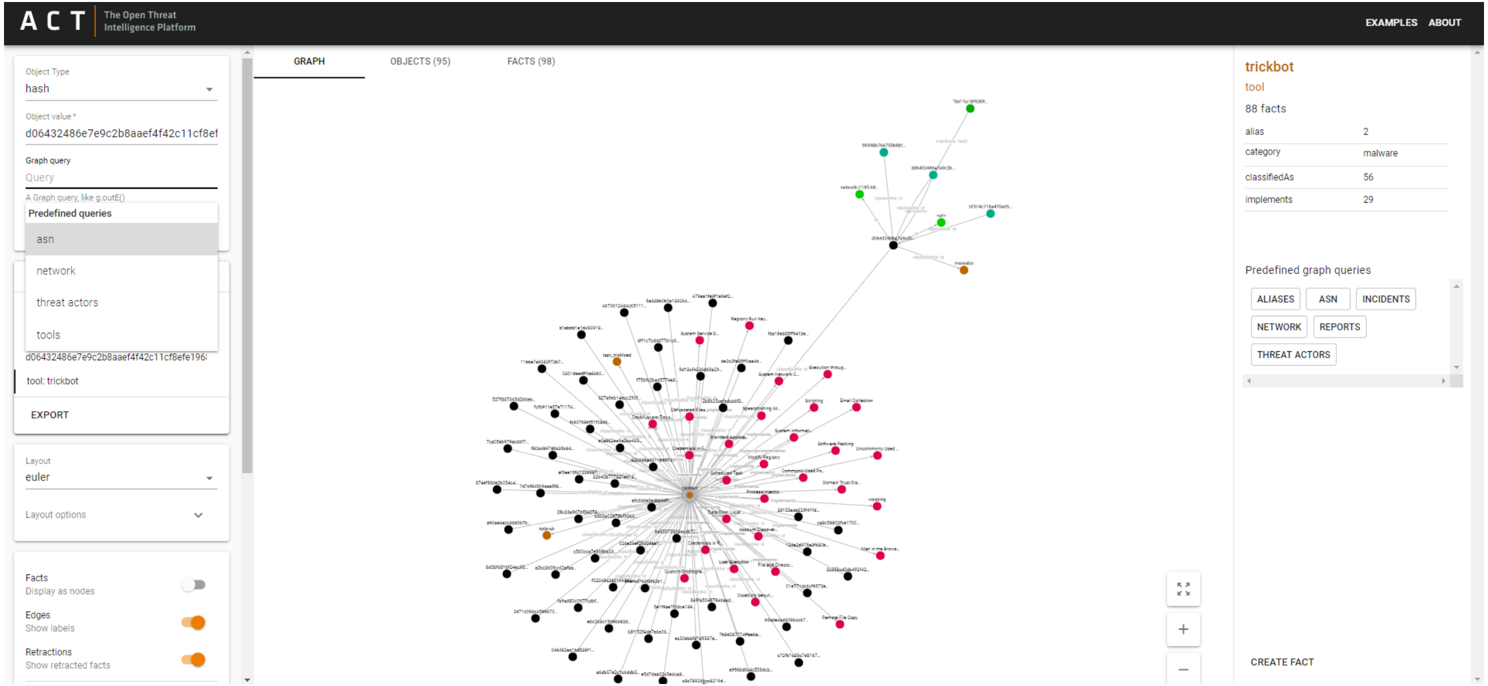
alias	2
category	malware
classifiedAs	56
implements	29

Predefined graph queries

ALIASES · ASN · INCIDENTS · NETWORK · REPORTS · THREAT ACTORS

Find the autonomous system and owner organization of network indicators related to this tool.

Introduction 1 – Graph Queries



Object Type
hash

Object value *
d06432486e7e9c2b8aaef4f42c11cf8ef

Graph query
Query
A Graph query, like g.outE()

Predefined queries
- asn
- network
- threat actors
- tools

d06432486e7e9c2b8aaef4f42c11cf8efe196

tool: trickbot

Layout
euler

Facts
Display as nodes

Edges
Show labels

Retractions
Show retracted facts

trickbot
tool
88 facts

alias	2
category	malware
classifiedAs	56
implements	29

Predefined graph queries

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

Try the following object query:

ipv4: 188.116.32[.]164

Try to find reports, threat actors, tools and any other information related to this IP address.

Task 3

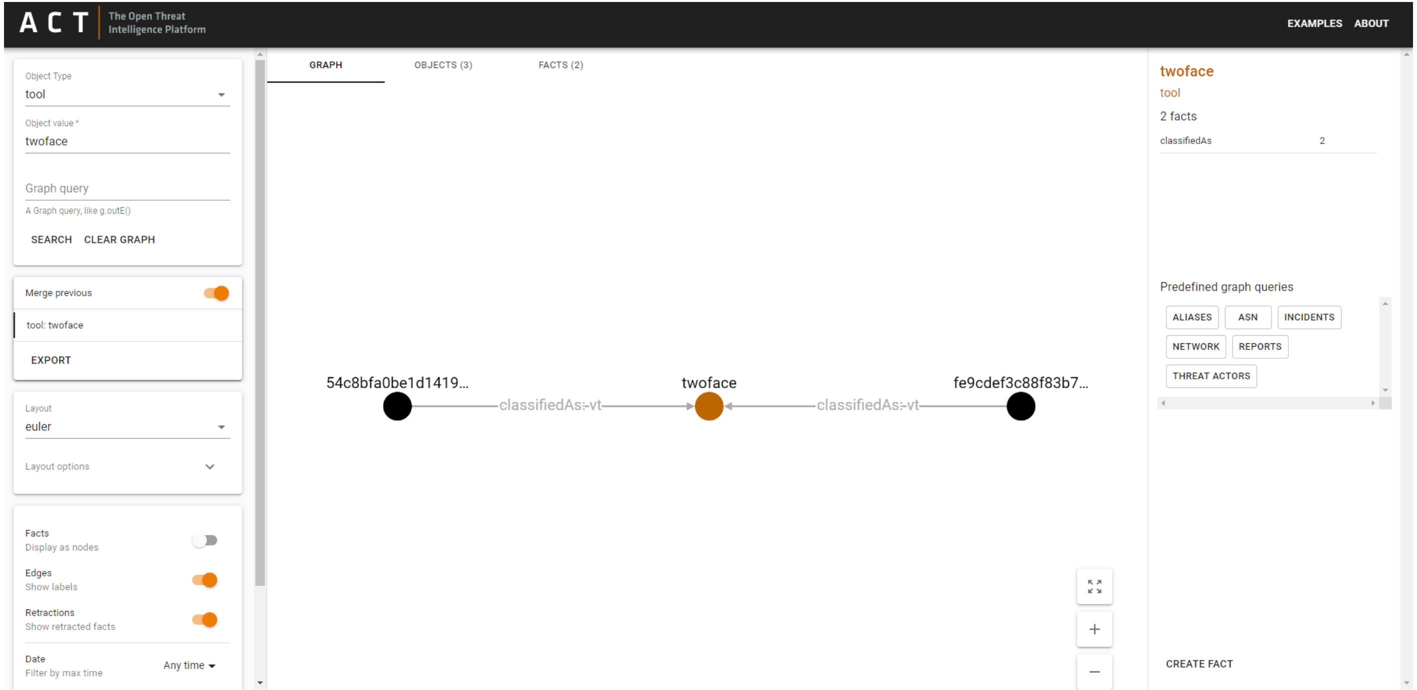
Explore Autonomous System Number 8048

- asn: 8048

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

Where is the organization that owns AS8048 located?

Introduction 3 – Aliases



ACT The Open Threat Intelligence Platform

Object Type: tool

Object value *: twoface

Graph query

A Graph query, like g.outE()

Merge previous

tool: twoface

Layout: euler

Facts – Display as nodes

Edges – Show labels

Retractions – Show retracted facts

Date – Filter by max time: Any time

twoface

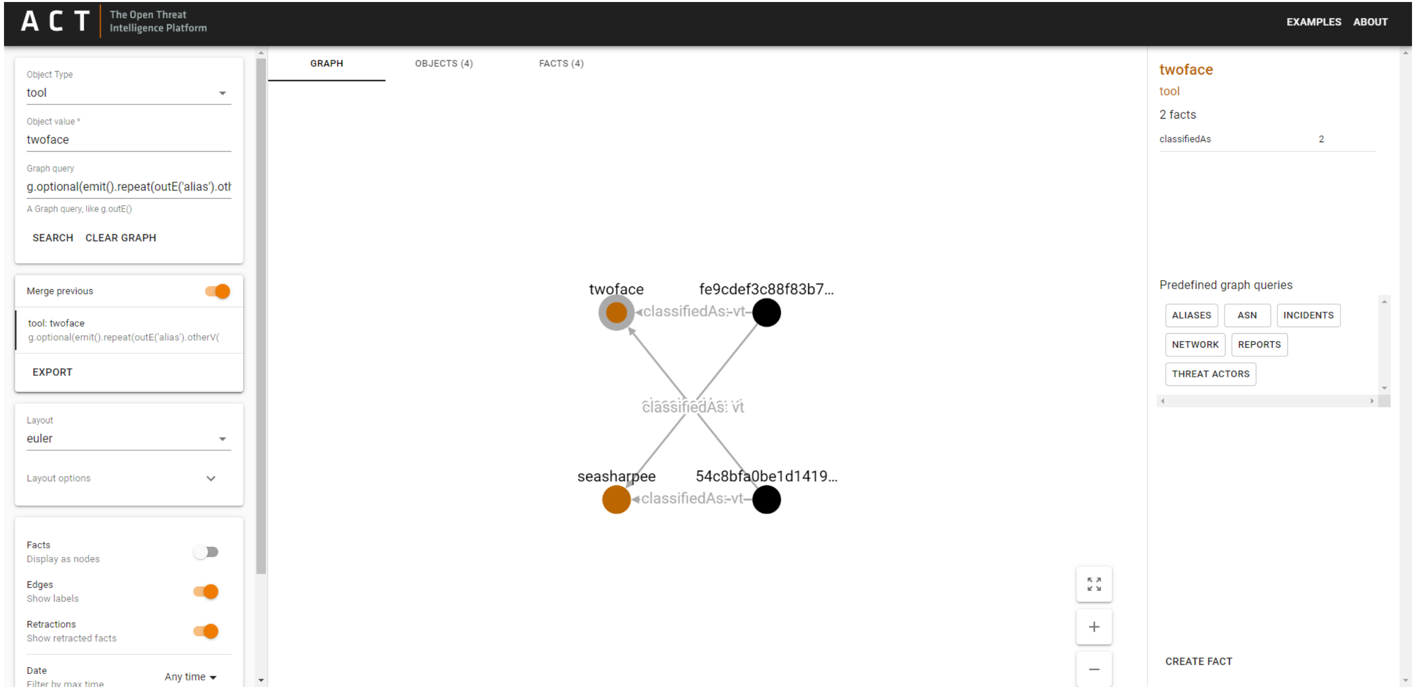
tool

2 facts

classifiedAs 2

Predefined graph queries

Introduction 3 – Aliases



A C T The Open Threat Intelligence Platform

EXAMPLES ABOUT

Object Type: tool

Object value *: twoface

Graph query: g.optional(emit().repeat(outE('alias').ot

A Graph query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

tool: twoface
g.optional(emit().repeat(outE('alias').otherV(

EXPORT

Layout: euler

Layout options

Facts: Display as nodes

Edges: Show labels

Retractions: Show retracted facts

Date: Filter by max time — Any time

GRAPH OBJECTS (4) FACTS (4)

twoface

tool

2 facts

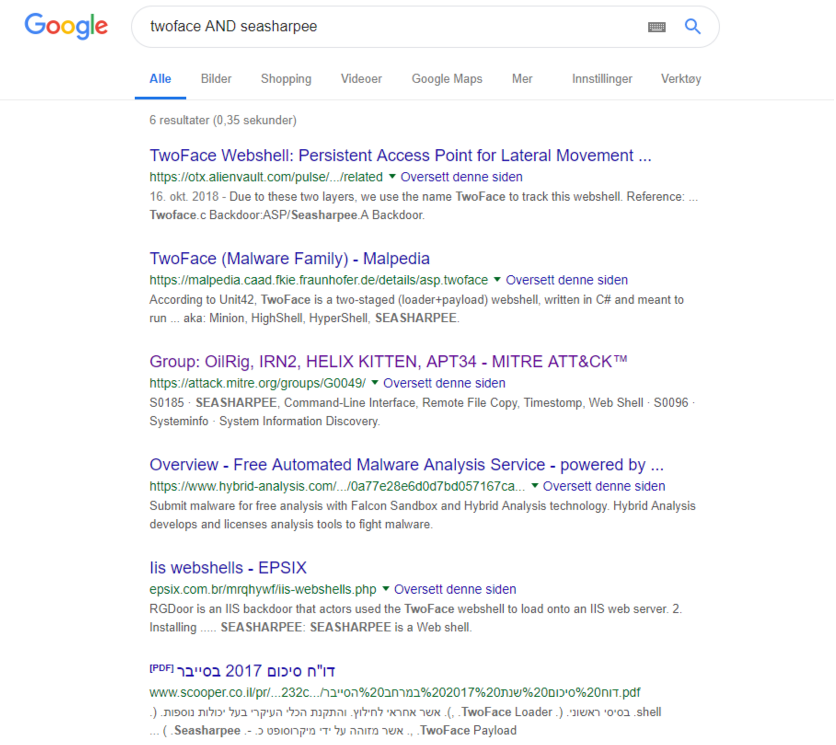
classifiedAs	2

Predefined graph queries

ALIASES ASN INCIDENTS NETWORK REPORTS THREAT ACTORS

CREATE FACT

Introduction 3 – Aliases



twoface AND seasharpee

6 resultater (0,35 sekunder)

TwoFace Webshell: Persistent Access Point for Lateral Movement ...
https://otx.alienvault.com/pulse/.../related ▾ Oversett denne siden
16. okt. 2018 - Due to these two layers, we use the name **TwoFace** to track this webshell. Reference: ... **Twoface**.c Backdoor:ASP/**Seasharpee**.A Backdoor.

TwoFace (Malware Family) - Malpedia
https://malpedia.caad.fkie.fraunhofer.de/details/asp.twoface ▾ Oversett denne siden
According to Unit42, **TwoFace** is a two-staged (loader+payload) webshell, written in C# and meant to run ... aka: Minion, HighShell, HyperShell, **SEASHARPEE**.

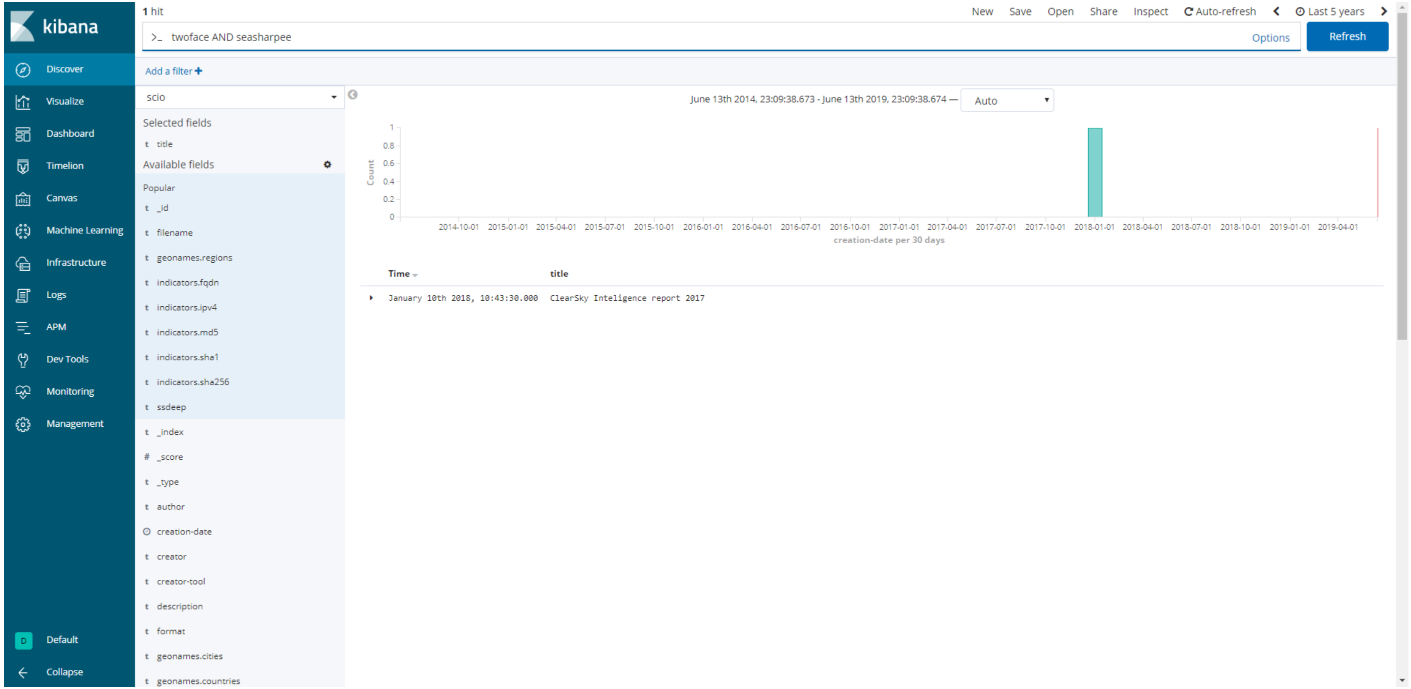
Group: OilRig, IRN2, HELIX KITTEN, APT34 - MITRE ATT&CK™
https://attack.mitre.org/groups/G0049/ ▾ Oversett denne siden
S0185 · **SEASHARPEE**, Command-Line Interface, Remote File Copy, Timestomp, Web Shell · S0096 · Systeminfo · System Information Discovery.

Overview - Free Automated Malware Analysis Service - powered by ...
https://www.hybrid-analysis.com/.../0a77e28e6d0d7bd057167ca... ▾ Oversett denne siden
Submit malware for free analysis with Falcon Sandbox and Hybrid Analysis technology. Hybrid Analysis develops and licenses analysis tools to fight malware.

Iis webshells - EPSIX
epsix.com.br/mrqhywf/iis-webshells.php ▾ Oversett denne siden
RGDoor is an IIS backdoor that actors used the **TwoFace** webshell to load onto an IIS web server. 2. Installing ..... **SEASHARPEE**: **SEASHARPEE** is a Web shell.

[PDF] דו"ח סיכום 2017 בסייבר
www.scooper.co.il/pr/...232c.../דוח%20סיכום%20שנת%202017%20במרחב%20הסייבר.pdf
shell. בסיסי ראשוני. (.**TwoFace** Loader .(,. אשר אחראי לחילוץ. והתקנת הכלי העיקרי בעל יכולות נוספות. (.
TwoFace Payload. ,. אשר מזוהה על ידי מיקרוסופט כ. -. **Seasharpee**.) ...

Introduction 3 – Aliases



1 hit

>_ twoface AND seasharpee

scio

June 13th 2014, 23:09:38.673 - June 13th 2019, 23:09:38.674 — Auto

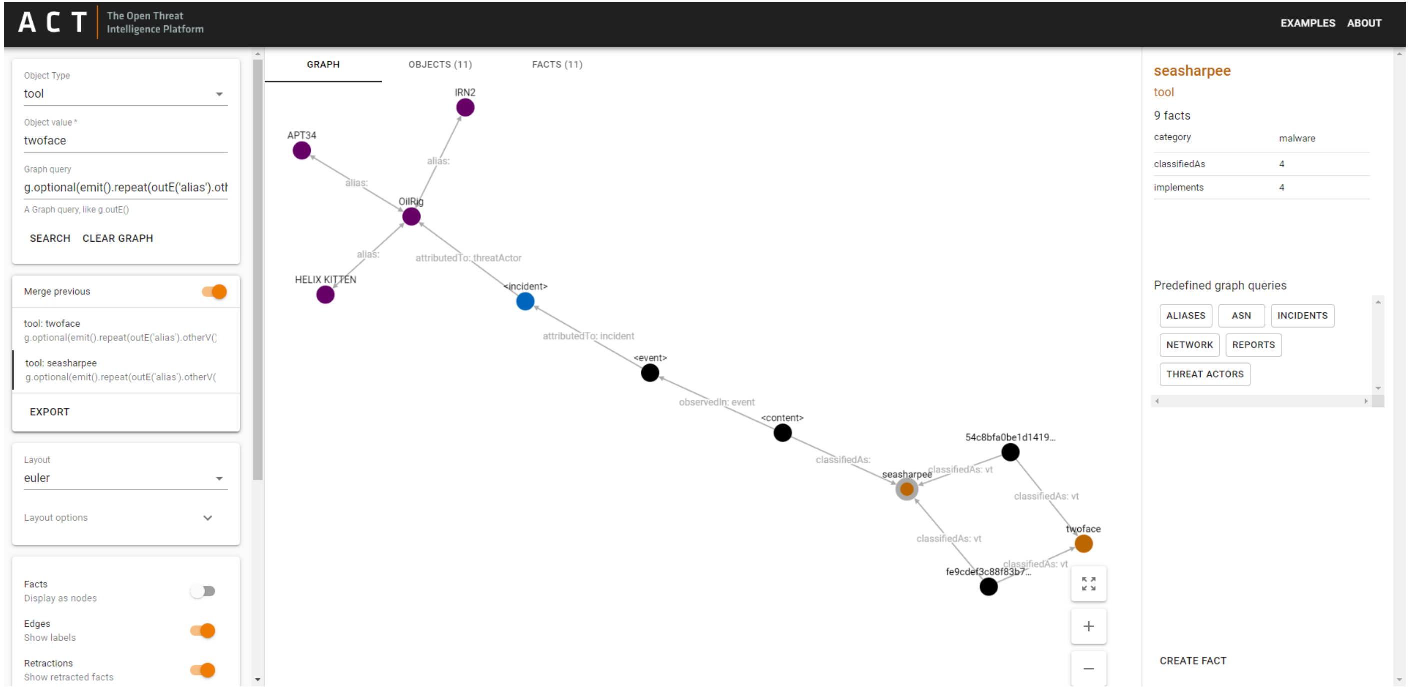
Time	title
January 10th 2018, 10:43:30.000	ClearSky Inteligence report 2017

Introduction 3 – Aliases

https://www.clearskysec.com/wp-content/uploads/2018/01/ClearSky_cyber_intelligence_report_2017.pdf

“The Webshell is named **TwoFace** as it is comprised by two components. The first is named TwoFace Loader, a basic and preliminary shell that extracts and installs the second component, a more advances tool named TwoFace Payload (identified by Microsoft as **Seasharpee**). These tools are written in #C, and run on Webservers that support ASP.NET.”

Introduction 3 – Aliases



Object Type
tool

Object value *
twoface

Graph query
g.optional(emit().repeat(outE('alias').ot

A Graph query, like g.outE()

SEARCH CLEAR GRAPH

Merge previous

tool: twoface
g.optional(emit().repeat(outE('alias').otherV(

tool: seasharpee
g.optional(emit().repeat(outE('alias').otherV(

EXPORT

Layout
euler

Layout options

Facts
Display as nodes

Edges
Show labels

Retractions
Show retracted facts

seasharpee
tool
9 facts

category	malware
classifiedAs	4
implements	4

Predefined graph queries

ALIASES ASN INCIDENTS
NETWORK REPORTS
THREAT ACTORS

CREATE FACT

Task 4

Try to find an alias for the tool ‘gulpix’. Then try to find a publically available, credible source that confirms your findings.

ASSIGNMENTS

CASE STUDY

mnemonic

BREAKOUT: API, GRAPH QUERIES, EXPLORATION

mnemonic

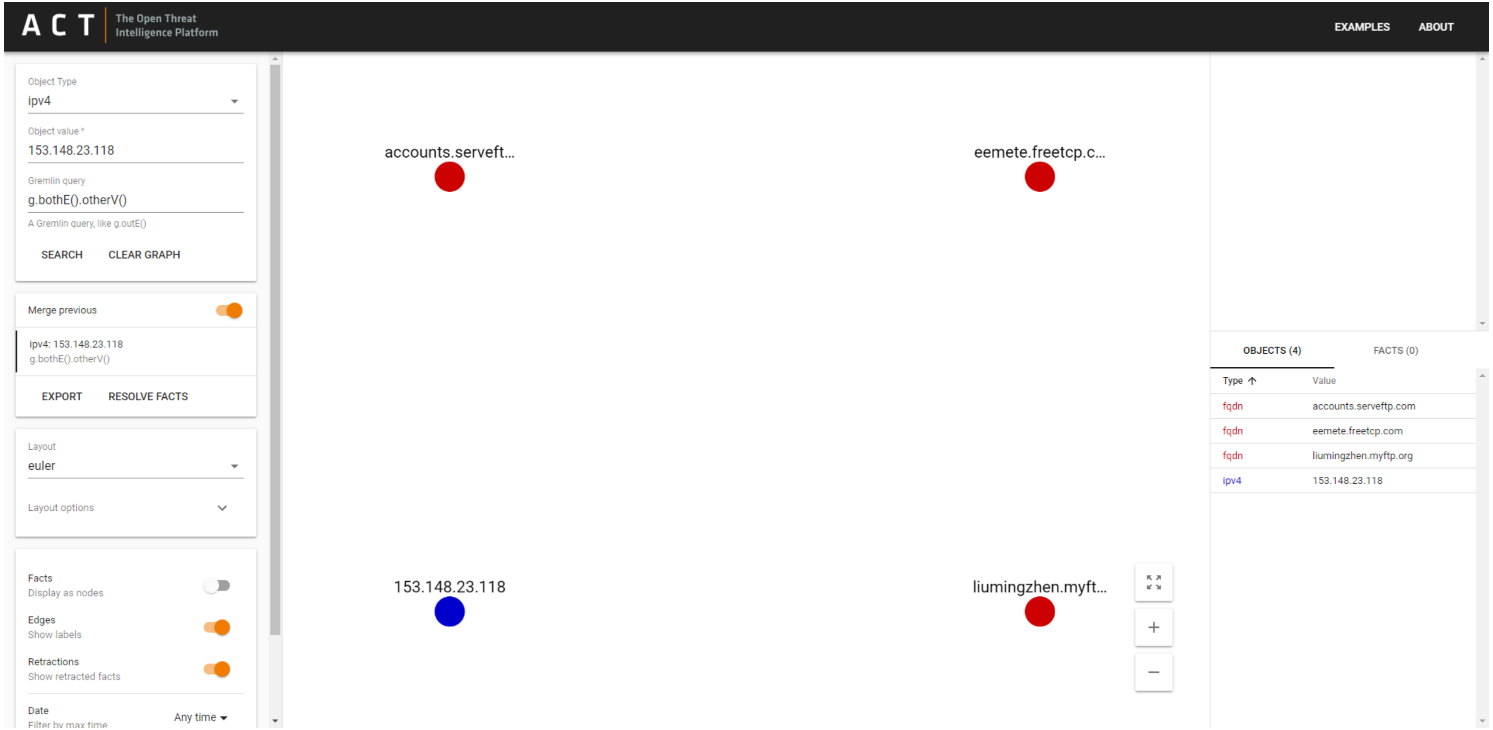
Breakout: API/workers, graph queries, exploration

- API/workers - Geir
  - https://github.com/mnemonic-no/act-workshop-api
  - https://github.com/mnemonic-no/act-api-python
  - https://github.com/mnemonic-no/act-workers
- Graph queries - Martin
  - http://tinkerpop.apache.org/docs/current/reference/
  - https://github.com/mnemonic-no/act-frontend/blob/master/src/config.json
- Exploration

GRAPH QUERIES

With Great Power Comes Great Responsibility

Graph Query 1



Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query: g.bothE().otherV()

A Gremlin query, like g.outE()

Merge previous

ipv4: 153.148.23.118
g.bothE().otherV()

Layout: euler

Facts – Display as nodes

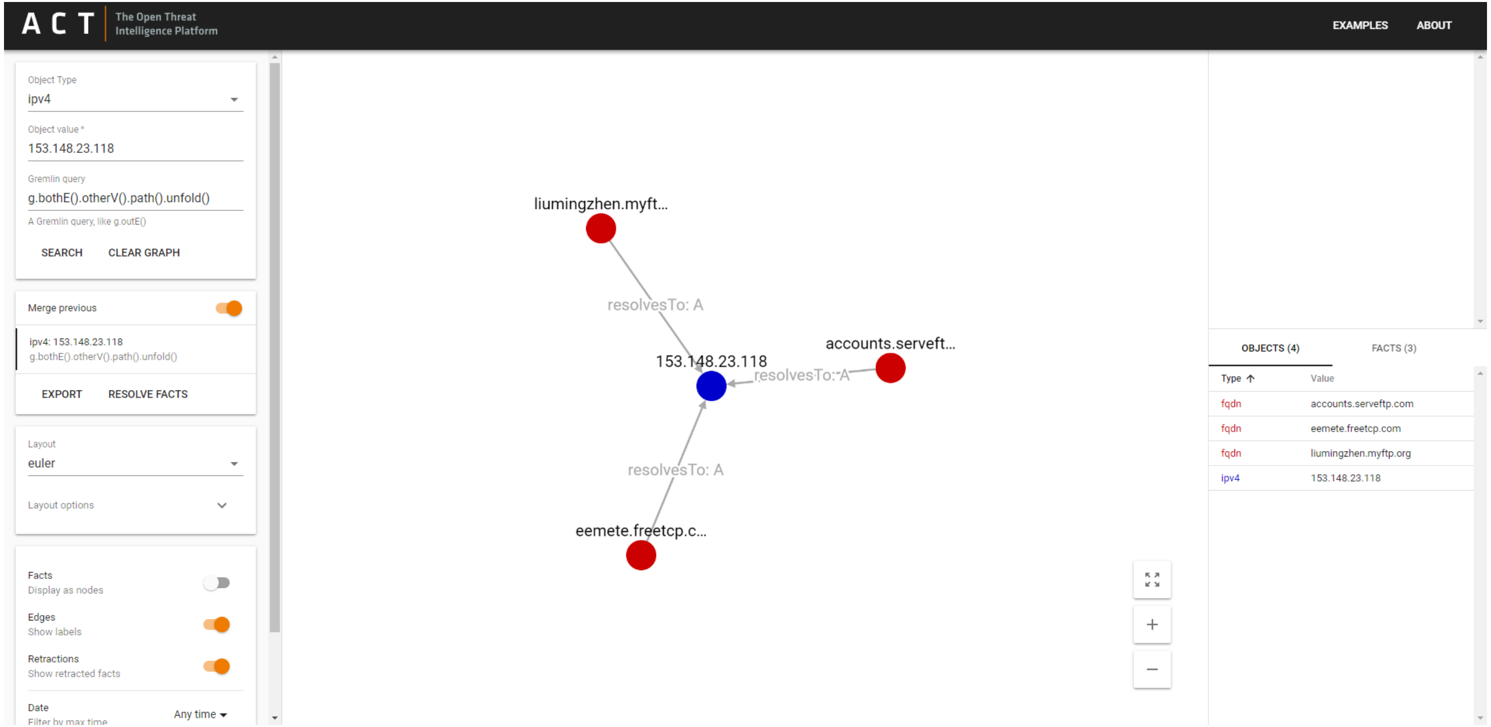
Edges – Show labels

Retractions – Show retracted facts

Date – Filter by max time: Any time

Type	Value
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118

Graph Query 2 – Show Edges



Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query: g.bothE().otherV().path().unfold()

A Gremlin query, like g.outE()

Merge previous

ipv4: 153.148.23.118
g.bothE().otherV().path().unfold()

Layout: euler

Layout options

Facts
Display as nodes

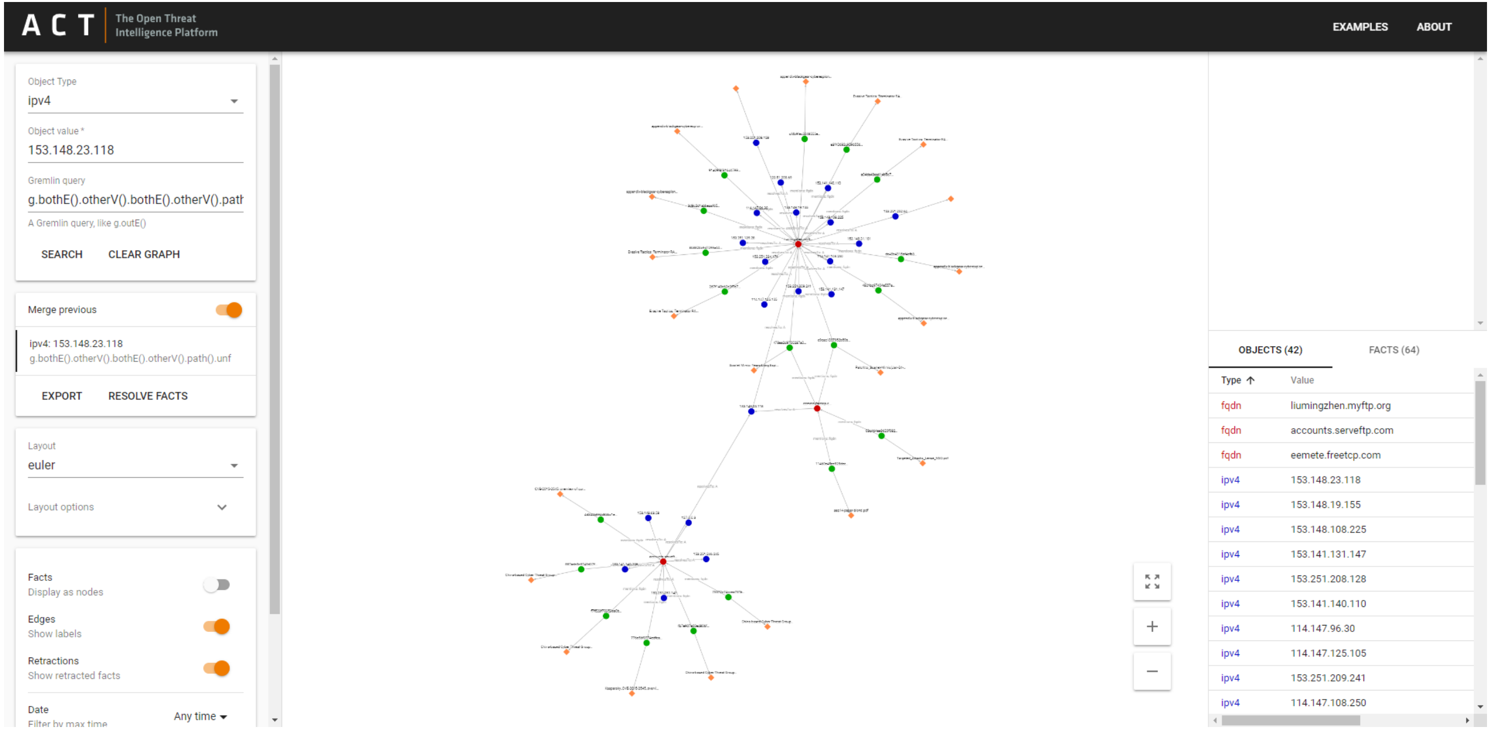
Edges
Show labels

Retractions
Show retracted facts

Date
Filter by max time: Any time

Type ↑	Value
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118

Graph Query 3 – 2 hops



Object Type
ipv4

Object value *
153.148.23.118

Gremlin query
g.bothE().otherV().bothE().otherV().patl

A Gremlin query, like g.outE()

Merge previous

ipv4: 153.148.23.118
g.bothE().otherV().bothE().otherV().path().unf

Layout
euler

Layout options

Facts
Display as nodes

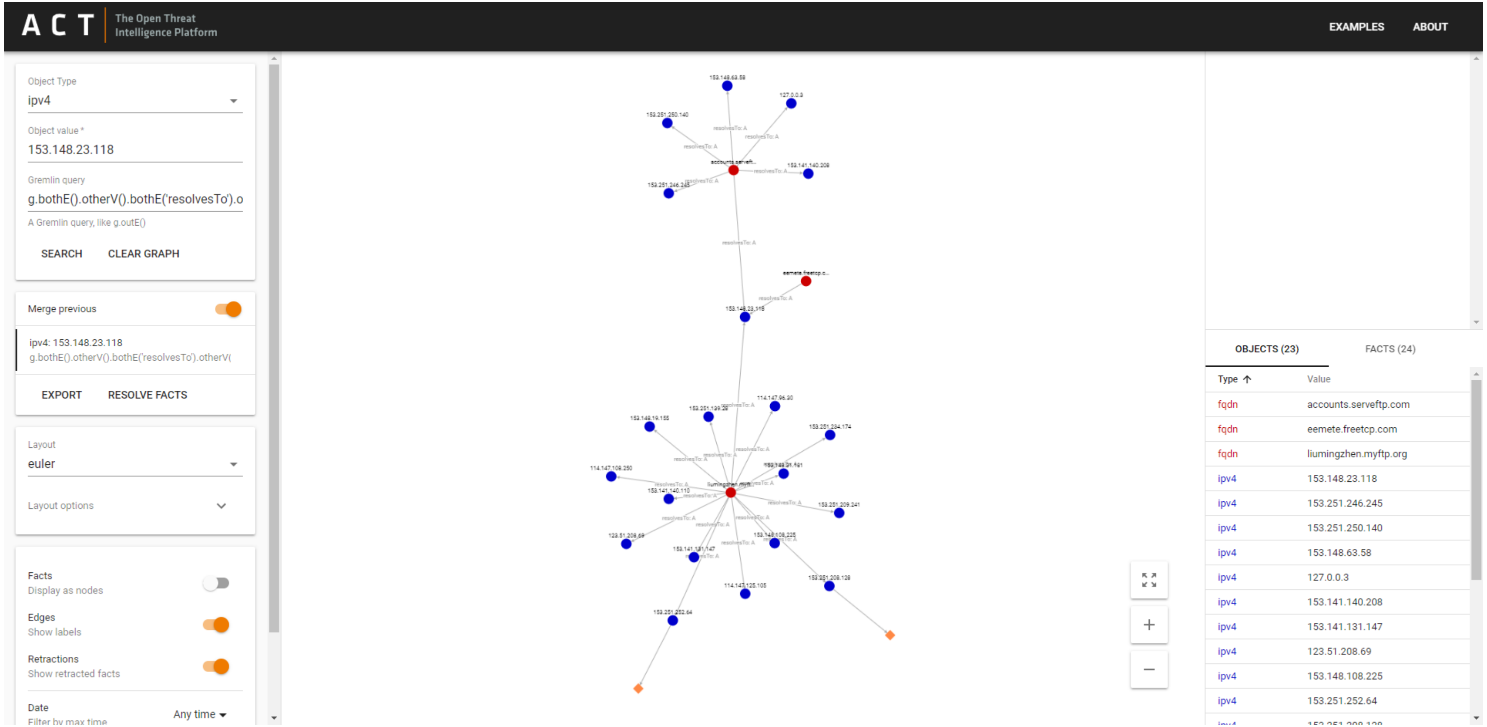
Edges
Show labels

Retractions
Show retracted facts

Date
Filter by max time
Any time

Type ↑	Value
fqdn	liumingzhen.myftp.org
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
ipv4	153.148.23.118
ipv4	153.148.19.155
ipv4	153.148.108.225
ipv4	153.141.131.147
ipv4	153.251.208.128
ipv4	153.141.140.110
ipv4	114.147.96.30
ipv4	114.147.125.105
ipv4	153.251.209.241
ipv4	114.147.108.250

Graph Query 4 – Filter Edges (Facts)



Object Type: ipv4

Object value *: 153.148.23.118

Gremlin query: g.bothE().otherV().bothE('resolvesTo').o

A Gremlin query, like g.outE()

Merge previous ●

ipv4: 153.148.23.118
g.bothE().otherV().bothE('resolvesTo').otherV(

Layout: euler

Layout options

Facts
Display as nodes ○

Edges
Show labels ●

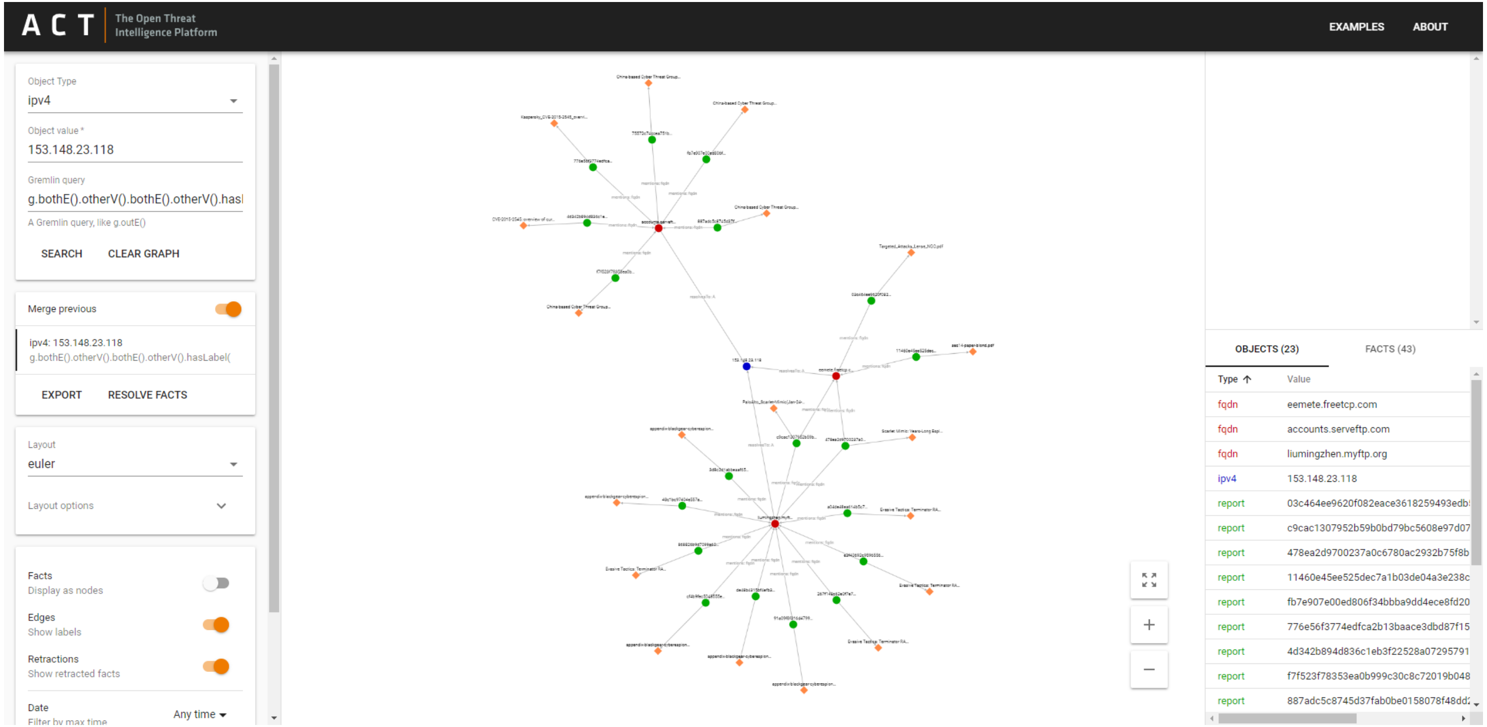
Retractions
Show retracted facts ●

Date
Filter by max time: Any time

OBJECTS (23) FACTS (24)

Type ↑	Value
fqdn	accounts.serveftp.com
fqdn	eemete.freetcp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118
ipv4	153.251.246.245
ipv4	153.251.250.140
ipv4	153.148.63.58
ipv4	127.0.0.3
ipv4	153.141.140.208
ipv4	153.141.131.147
ipv4	123.51.208.69
ipv4	153.148.108.225
ipv4	153.251.252.64

Graph Query 5 – Filter Nodes (Objects)



Object Type
ipv4

Object value *
153.148.23.118

Gremlin query
g.bothE().otherV().bothE().otherV().hasl

A Gremlin query, like g.outE()

Merge previous

ipv4: 153.148.23.118
g.bothE().otherV().bothE().otherV().hasLabel(

Layout
euler

Layout options

Facts
Display as nodes

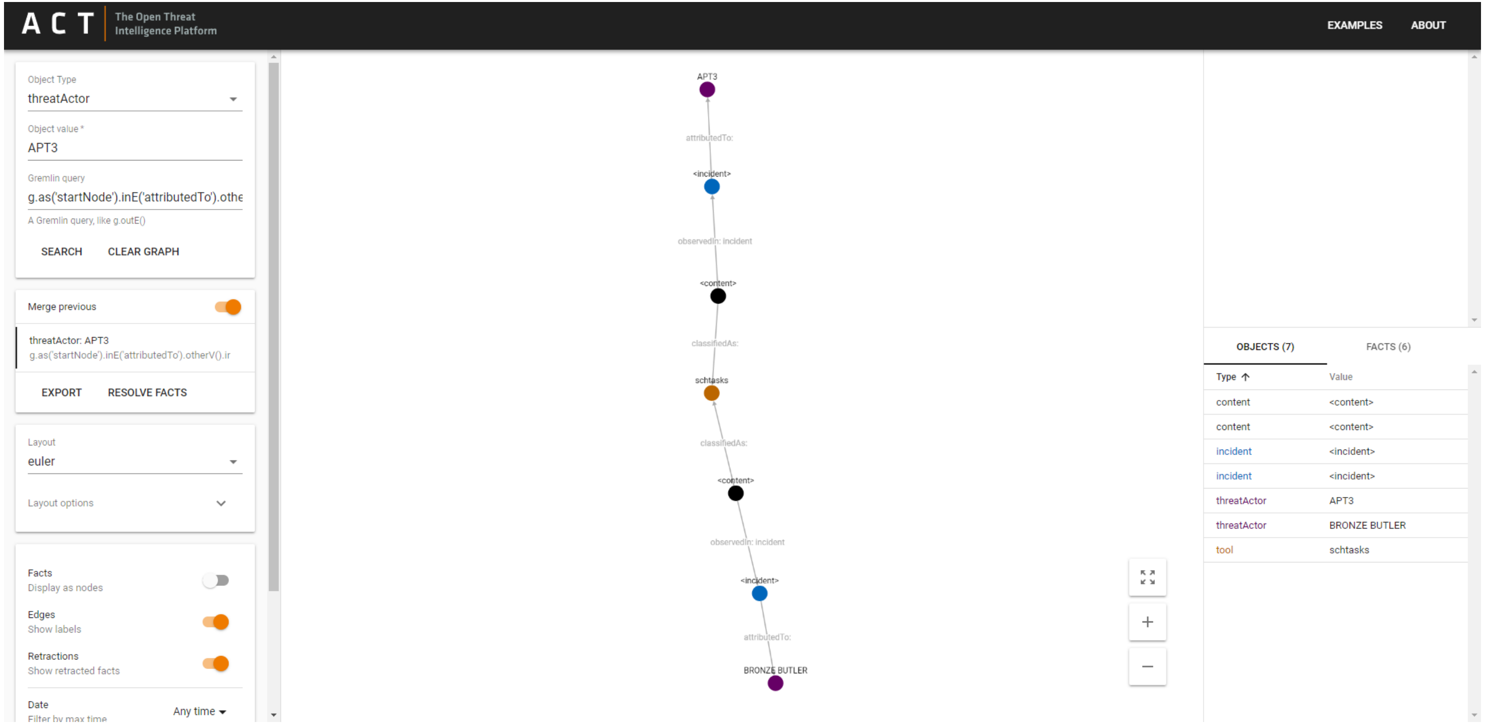
Edges
Show labels

Retractions
Show retracted facts

Date
Filter by max time
Any time

Type ↑	Value
fqdn	eemete.freetcp.com
fqdn	accounts.serveftp.com
fqdn	liumingzhen.myftp.org
ipv4	153.148.23.118
report	03c464ee9620f082eace3618259493edb
report	c9cac1307952b59b0bd79bc5608e97d07
report	478ea2d9700237a0c6780ac2932b75f8b
report	11460e45ee525dec7a1b03de04a3e238c
report	fb7e907e00ed806f34bbba9dd4ece8fd20
report	776e56f3774edfca2b13baace3dbd87f15
report	4d342b894d836c1eb3f22528a07295791
report	f7f523f78353ea0b999c30c8c72019b048
report	887adc5c8745d37fab0be0158078f48dd2

Graph Query 6 – Unique Tool Usage



Object Type
threatActor

Object value *
APT3

Gremlin query
g.as('startNode').inE('attributedTo').othe

A Gremlin query, like g.outE()

Merge previous

threatActor: APT3
g.as('startNode').inE('attributedTo').otherV().ir

Layout
euler

Layout options

Facts
Display as nodes

Edges
Show labels

Retractions
Show retracted facts

Date
Filter by max time
Any time

Type ↑	Value
content	<content>
content	<content>
incident	<incident>
incident	<incident>
threatActor	APT3
threatActor	BRONZE BUTLER
tool	schtasks

Public Read-Only ACT Instance

https://act-eu1.mnemonic.no/examples/

FURTHER WORK

New Information Sources

- Security events
- Incidents
- Reputation lists
- Malware analysis systems
- STIX feeds
- …

Information Sharing

- Mechanism for sharing schema
- Format (STIX?)
- Trust models

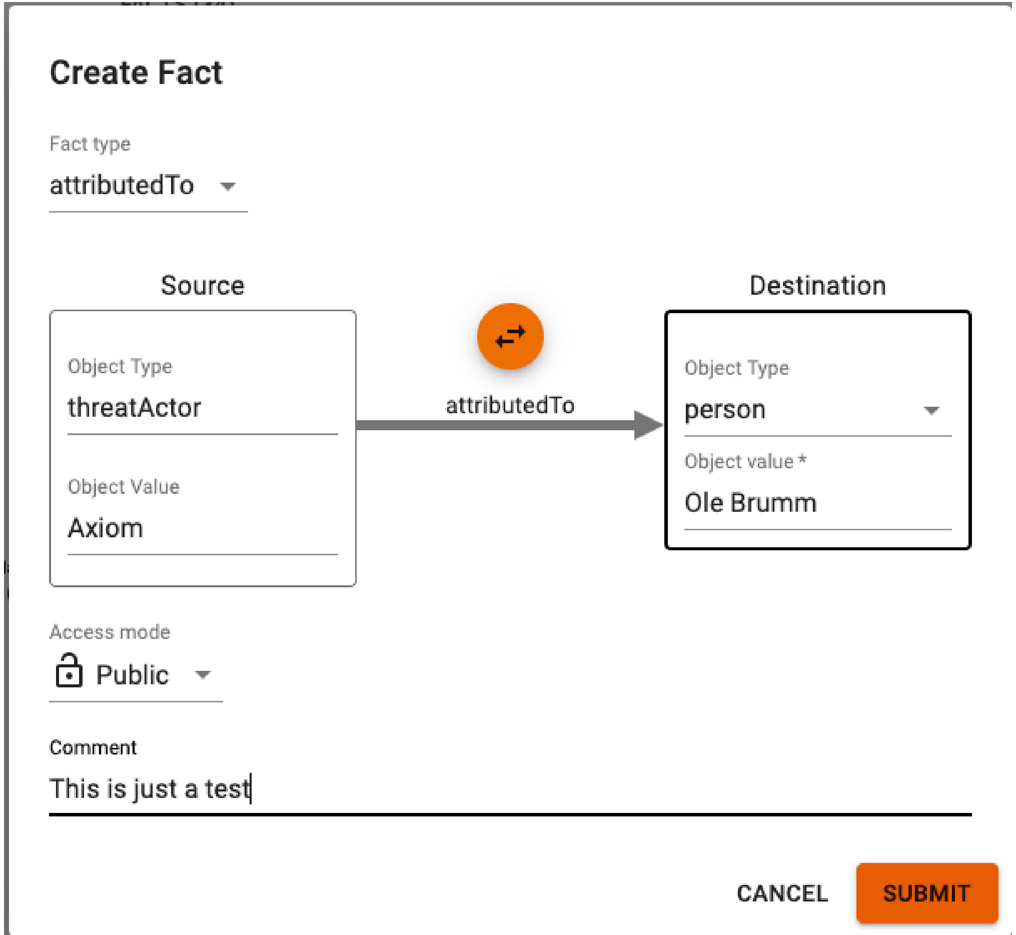
Trust and Confidence

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

GUI Improvements

- Timelines
- Share workspace
- Prune graph

GUI Improvements



Create Fact

Fact type: attributedTo

Source

Object Type: threatActor

Object Value: Axiom

Destination

Object Type: person

Object value *: Ole Brumm

Access mode: Public

Comment: This is just a test

?