Vertex

Synapse Bootcamp

Module 19

Introduction to Threat Intelligence in Synapse

v0.4 - May 2024

Objectives

- Describe the key components of Synapse's threat intel model
- Use the Research Tool to lift and explore threat intel data
- Understand the purpose of the Threat Intel Workflow
- Use the Workflow to view, create, and link threat intel data

Threat Intel in Synapse

Threat Intel Model

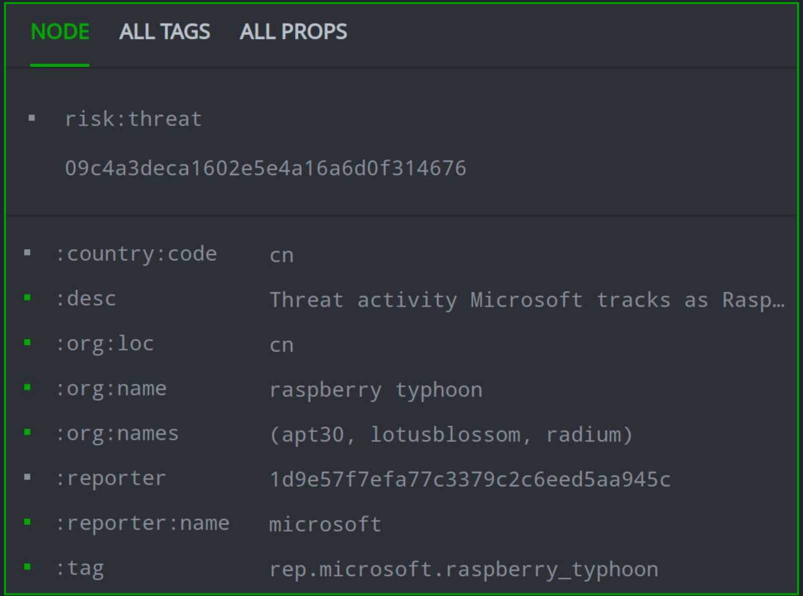
- Define forms to represent important concepts and activity
    - "Threat group", "vulnerability", "compromise"
- The form records essential information
    - Who / what / when / where / why / how
- Because information is **structured** we can query it!

Threat Intel Forms

Category	Example Data	Forms
risk:*	Threat clusters Malware Families Vulnerabilities Activity	risk:threat risk:tool:software risk:vuln risk:alert risk:attack risk:compromise
ou:*	Threats / targets / victims Industries Campaigns Goals Techniques	ou:org ou:industry ou:campaign ou:goal ou:technique
it:*	Malware / software	it:prod:soft

risk:threat

Threat Cluster / risk:threat	
Property	**Description**
:country:code / :org:loc	Optional ISO2 country code and / or location string for the threat
:desc	Brief description of the threat
:org:name / :org:names	Primary & alternate names for the threat
:reporter:name	Organization reporting on the threat
:tag	Tag to annotate nodes associated with the threat



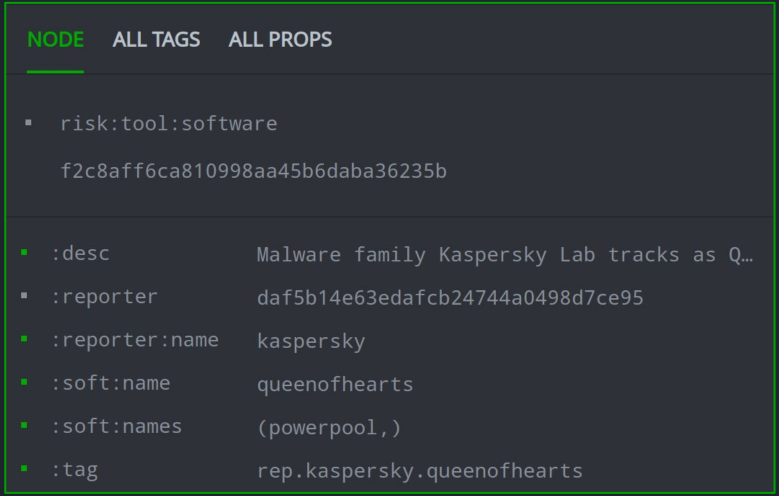
```
▪  risk:threat
   09c4a3deca1602e5e4a16a6d0f314676

▪  :country:code     cn
▪  :desc             Threat activity Microsoft tracks as Rasp…
▪  :org:loc          cn
▪  :org:name         raspberry typhoon
▪  :org:names        (apt30, lotusblossom, radium)
▪  :reporter         1d9e57f7efa77c3379c2c6eed5aa945c
▪  :reporter:name    microsoft
▪  :tag              rep.microsoft.raspberry_typhoon
```

risk:tool:software

Software / `risk:tool:software`	
Property	**Description**
`:desc`	Brief description of the software
`:reporter:name`	Organization reporting on the software

`:soft:name /`
`:soft:names`
	Primary & alternate names for the software

`:tag`	Tag used to annotate nodes associated with the software



```
risk:tool:software
f2c8aff6ca810998aa45b6daba36235b

:desc            Malware family Kaspersky Lab tracks as Q…
:reporter        daf5b14e63edafcb24744a0498d7ce95
:reporter:name   kaspersky
:soft:name       queenofhearts
:soft:names      (powerpool,)
:tag             rep.kaspersky.queenofhearts
```

Threat Intel Activity

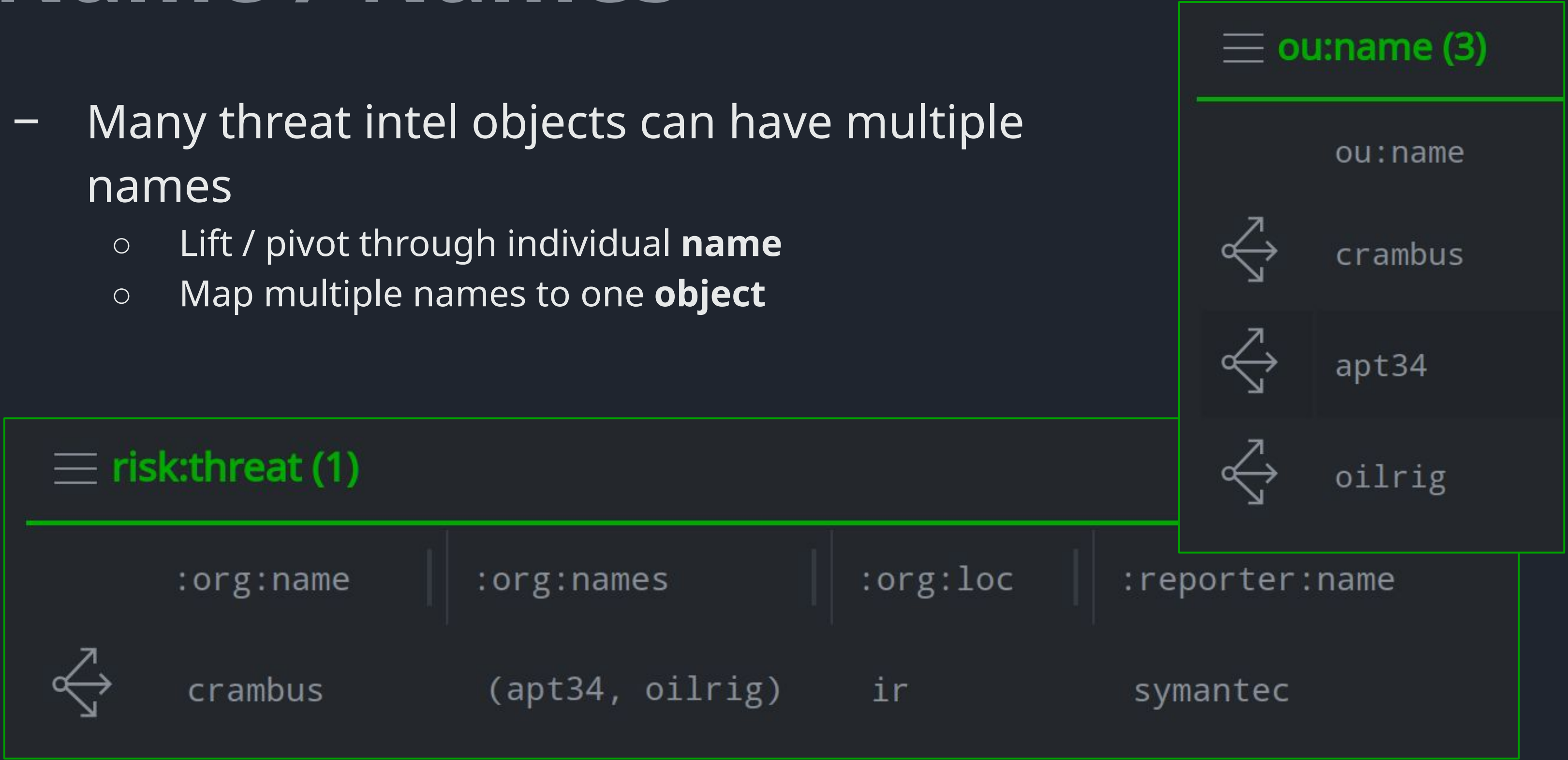
- Capture key information about activity at various levels

Activity	Description	Can be Associated With
`risk:alert`	Notification of a risk, vulnerability, or threat	`risk:attack`
`risk:attack`	Unauthorized action attempted against a target	`risk:compromise` `ou:campaign`
`risk:compromise`	One or more unauthorized actions successfully carried out against a target	`ou:campaign`
`ou:campaign`	A set of activity carried out by an organization to achieve a goal	`ou:conflict`

Common Properties

Name / Names

- Many threat intel objects can have multiple names
  - Lift / pivot through individual **name**
  - Map multiple names to one **object**



ou:name (3)

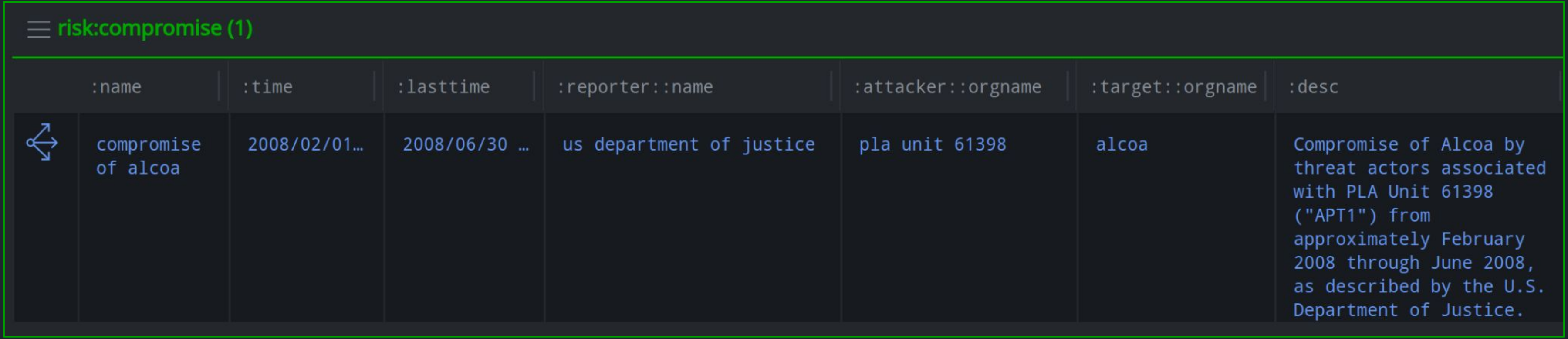
ou:name
crambus
apt34
oilrig

risk:threat (1)

:org:name	:org:names	:org:loc	:reporter:name
crambus	(apt34, oilrig)	ir	symantec

Reporter / Reporter Name

- Use when the **source** is important
- Reporting on threats and malware varies widely
  - Microsoft vs. Mandiant vs. Kaspersky…
- Reporting on vulnerabilities or compromises may not

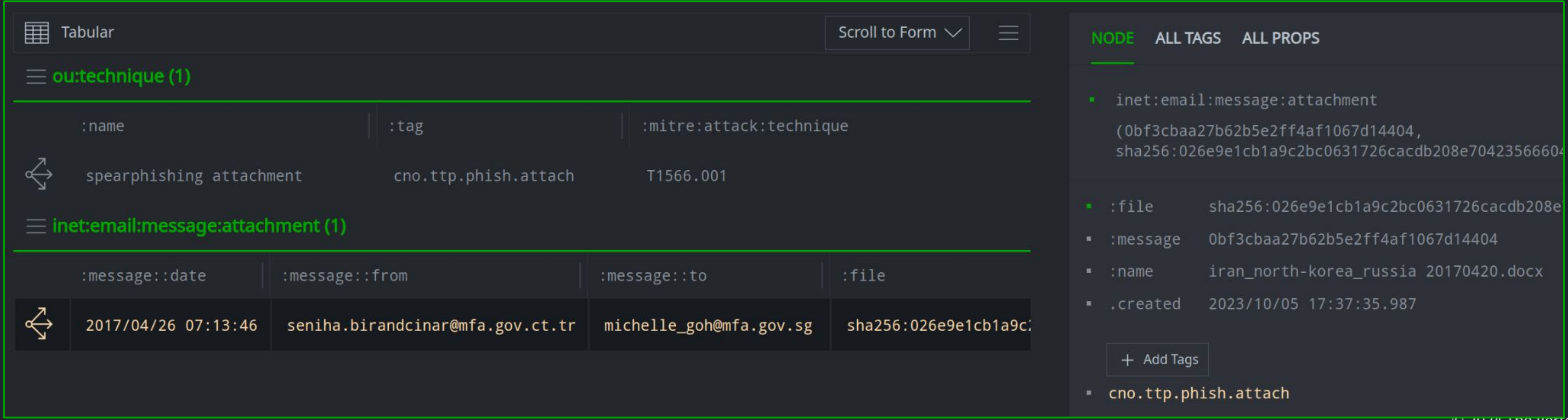


risk:compromise (1)

	:name	:time	:lasttime	:reporter::name	:attacker::orgname	:target::orgname	:desc
	compromise of alcoa	2008/02/01…	2008/06/30 …	us department of justice	pla unit 61398	alcoa	Compromise of Alcoa by threat actors associated with PLA Unit 61398 ("APT1") from approximately February 2008 through June 2008, as described by the U.S. Department of Justice.

Tag

- As **labels**, tags give us context
  - #rep.eset.sednit ("ESET associates this with Sednit")
  - What the heck is "Sednit" ?
- With the `:tag` property:
  - We link the tag to "what the tag represents"
  - We can use the tag to annotate "evidence"



ou:technique (1)

:name	:tag	:mitre:attack:technique
spearphishing attachment	cno.ttp.phish.attach	T1566.001

inet:email:message:attachment (1)

:message::date	:message::from	:message::to	:file
2017/04/26 07:13:46	seniha.birandcinar@mfa.gov.ct.tr	michelle_goh@mfa.gov.sg	sha256:026e9e1cb1a9c

inet:email:message:attachment

(0bf3cbaa27b62b5e2ff4af1067d14404,
sha256:026e9e1cb1a9c2bc0631726cacdb208e704235666604

:file	sha256:026e9e1cb1a9c2bc0631726cacdb208e
:message	0bf3cbaa27b62b5e2ff4af1067d14404
:name	iran_north-korea_russia 20170420.docx
.created	2023/10/05 17:37:35.987

- cno.ttp.phish.attach

Threat Intel Relationships

Threat Intel Relationships

- Threat intel objects commonly connected by **light edges**
- Uses:

```
risk:threat -(uses)> risk:tool:software
```

```
risk:attack -(uses)> ou:technique
```

- Targets:

```
risk:threat -(targets)> ou:org
```

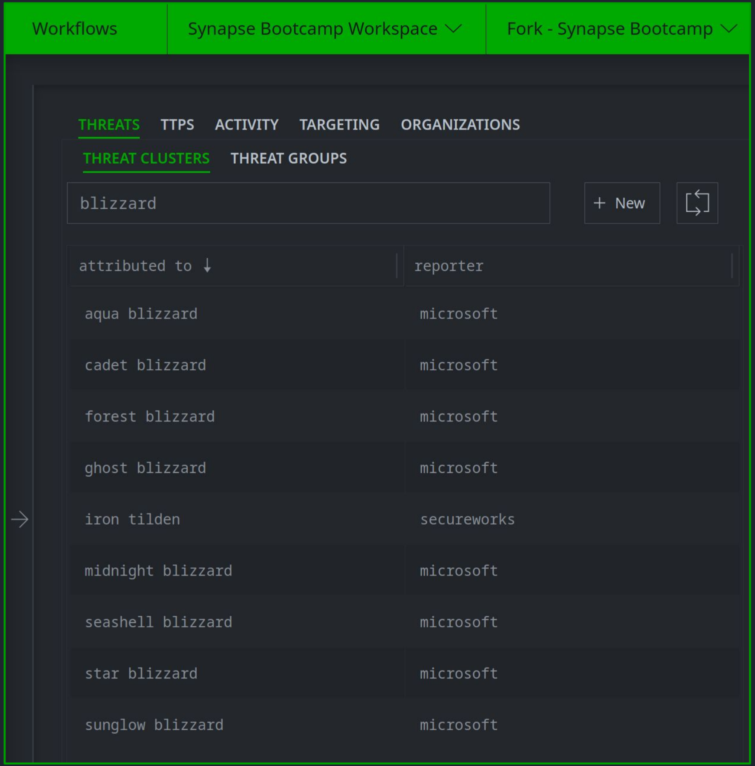
```
risk:threat -(targets)> pol:country
```

Threat Intel Demo

Vertex Threat Intel Workflow

Threat Intel Workflow

- Installed by the Vertex-Threat-Intel Power-Up
- Custom UI to work with threat data
  - Search / view / create threat intel objects
  - Link / unlink objects
    - -(uses)>
    - -(targets)>
    - -(refs)>
- **Simplifies** working with threat data



attributed to ↓	reporter
aqua blizzard	microsoft
cadet blizzard	microsoft
forest blizzard	microsoft
ghost blizzard	microsoft
iron tilden	secureworks
midnight blizzard	microsoft
seashell blizzard	microsoft
star blizzard	microsoft
sunglow blizzard	microsoft

Threat Intel Workflow Demo

Workflow vs. Research Tool

Workflow	Research Tool
Work with key forms / properties	Work with all forms / properties
Custom UI to focus on specific tasks	Designed for generic analysis
Simple and intuitive	Powerful and flexible

You can easily switch between the Workflow and the Research Tool!

Summary

- The **threat intel** model captures "higher level" threat data
  - View and query just like other data
  - Compare and contrast reporting
  - Cross-reference reporting across organizations
- The **threat intel workflow** makes it easier to work with threat data
  - Easily view, create, and link objects