



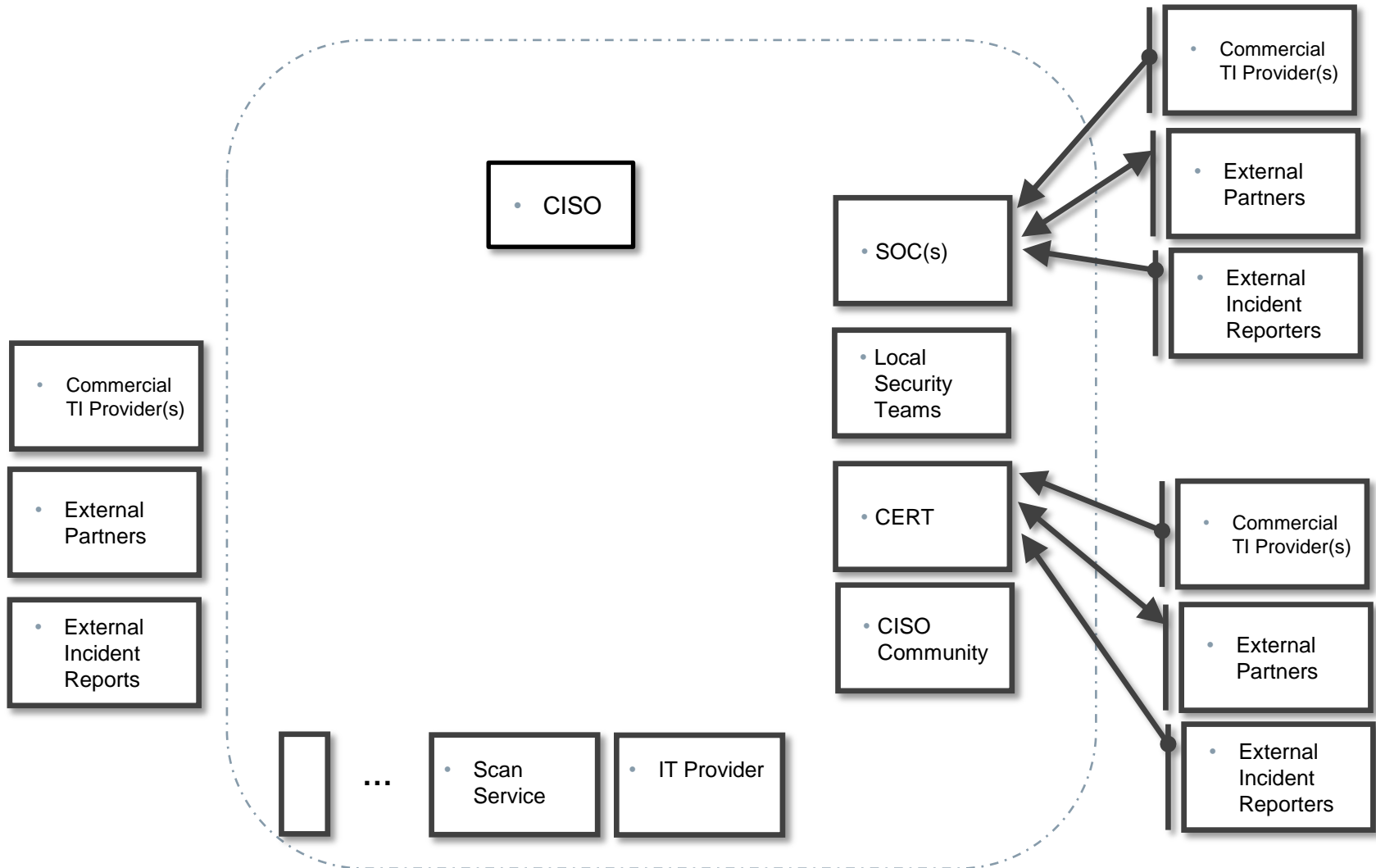
B. Grobauer, S. Berger, J. Göbel, T. Schreck, J. Wallinger | Siemens CERT

The MANTIS Framework Cyber-Threat Intelligence Mgmt. for CERTs

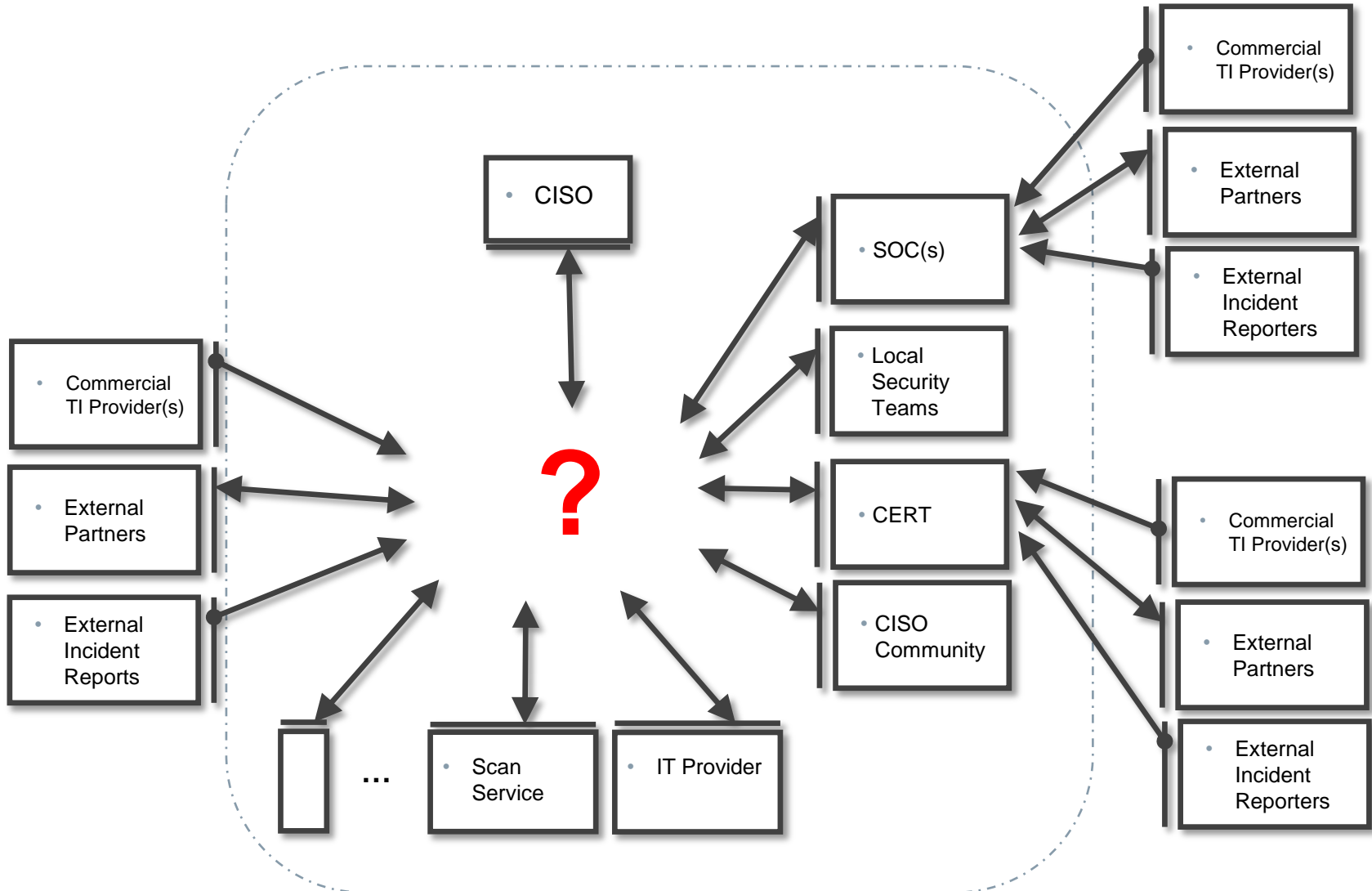
Note

- MANTIS is available as Open Source under GPL v2+ from <https://github.com/siemens/django-mantis>
- At time of this presentation (2014-06-24), the publicly available revision is MANTIS 0.2.0
- The examples shown in this talk are based on MANTIS 0.3.0
- MANTIS 0.3.0 will be released within the next few weeks:
 - either follow the repository on github
 - or subscribe to the MANTIS mailing list by sending a mail to mantis-ti-discussion-join@lists.trusted-introducer.org.

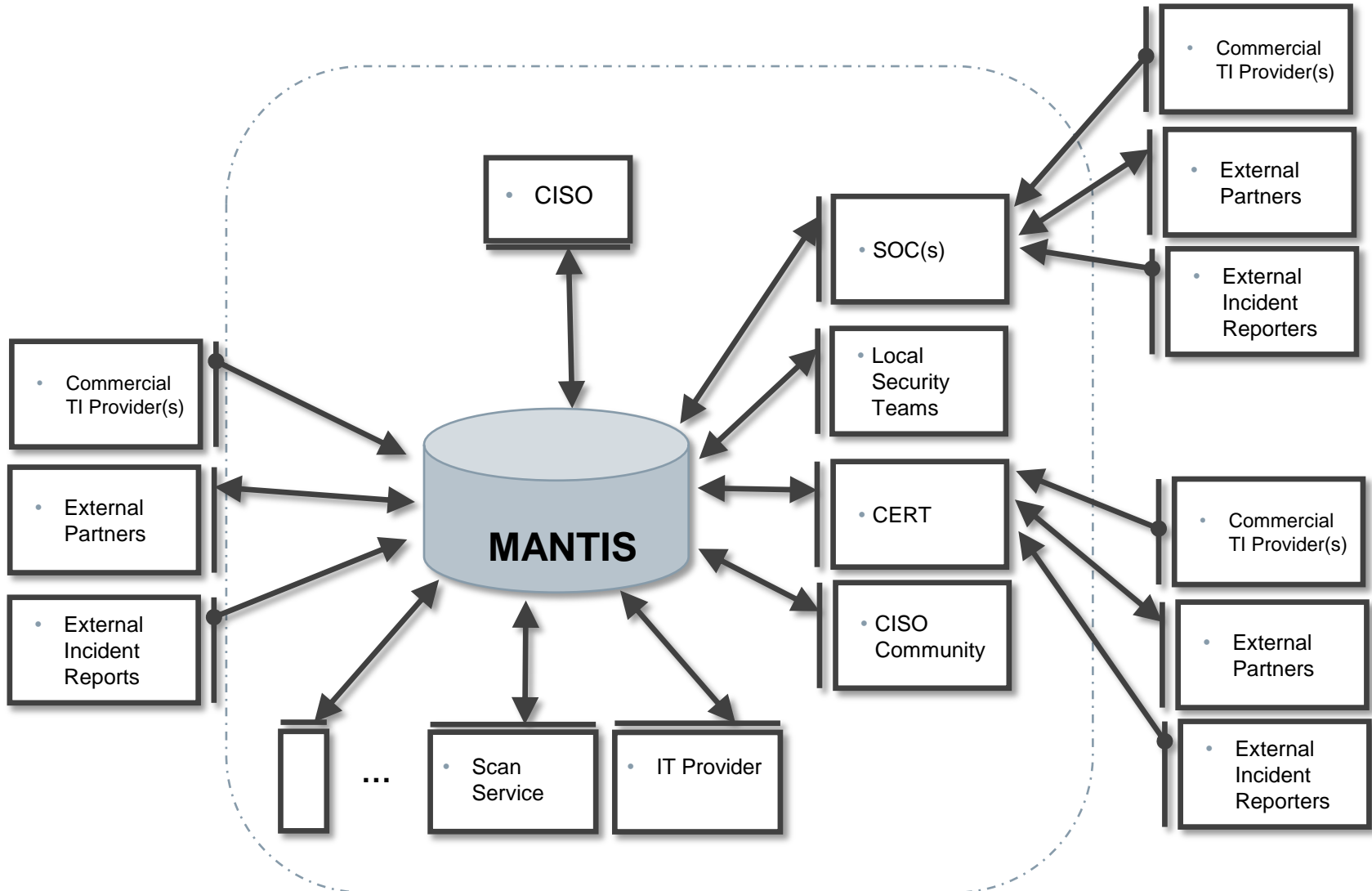
In a big corporation, there are many sources of cyber threat intelligence



... and we need the full picture!



With MANTIS, we are working towards a tool that provides us with this full picture!



Today, there are several open-source tools that cover aspects of cyber threat intelligence management ...
... what are their distinguishing features?



MISP

MANTIS

AVALANCHE

One person's incident is everyone's defense

(upcoming fall 2014 as Open Source)

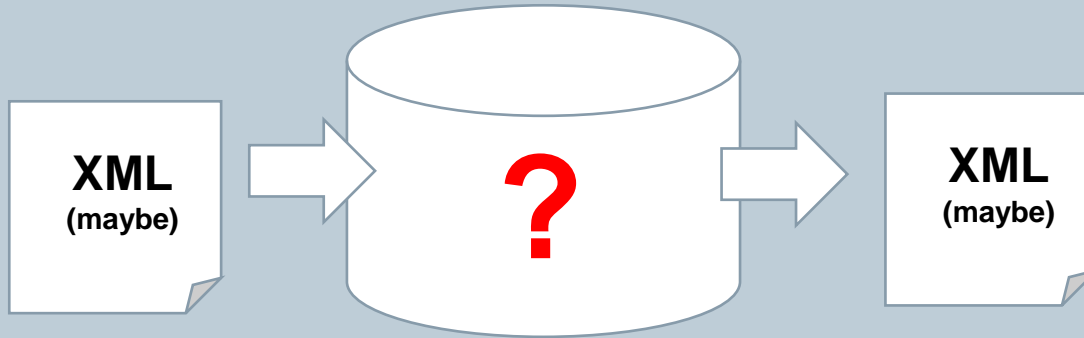


collective-intelligence-framework

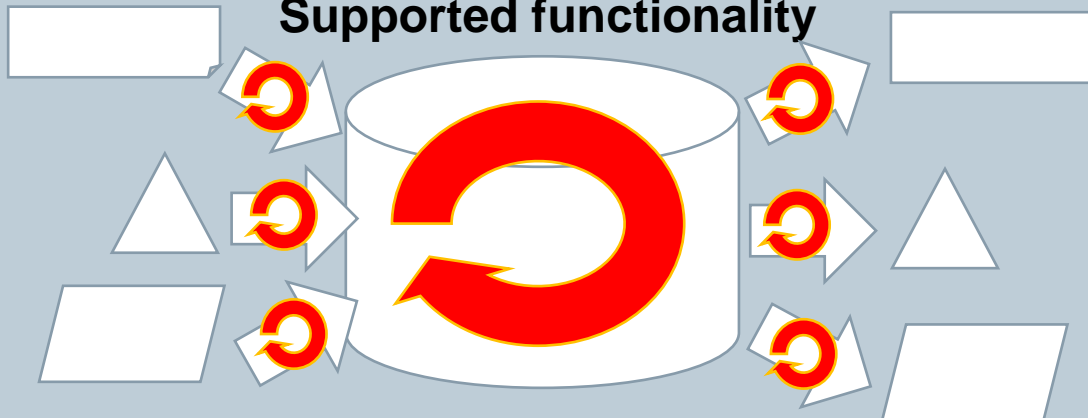
The Intelligence Layer

What are the distinguishing features of a cyber threat intelligence management solution?

Internal data model



Supported functionality



THE basic design decision when implementing a solution for managing cyber threat intelligence: The internal data model

■ **Genesis**

What does your data model look like?

- Home-brew
- Somehow derived from a standard

■ **Distance**

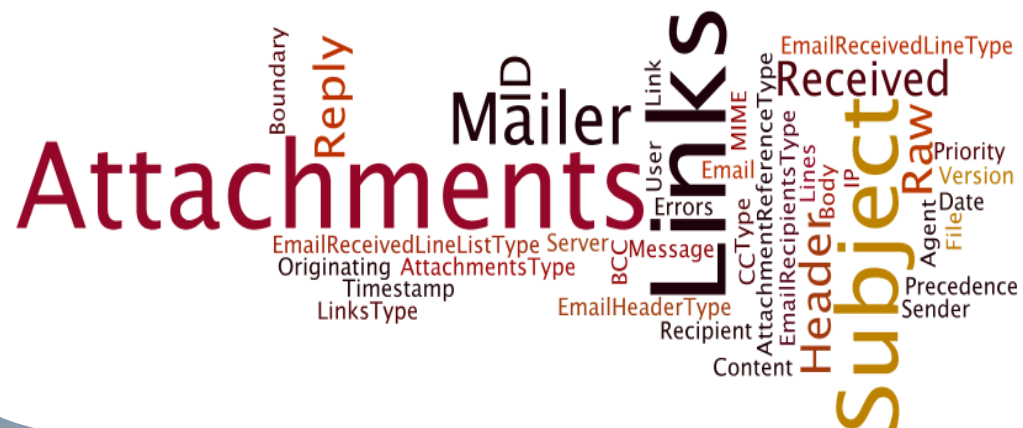
- How close is your data model to the (main) exchange standard(s) you are going to utilize?

■ **Flexibility**

- If the exchange standard allows very flexible usage: does your model, too, or do you narrow things down?
- Can your model cope with moderate revision changes?

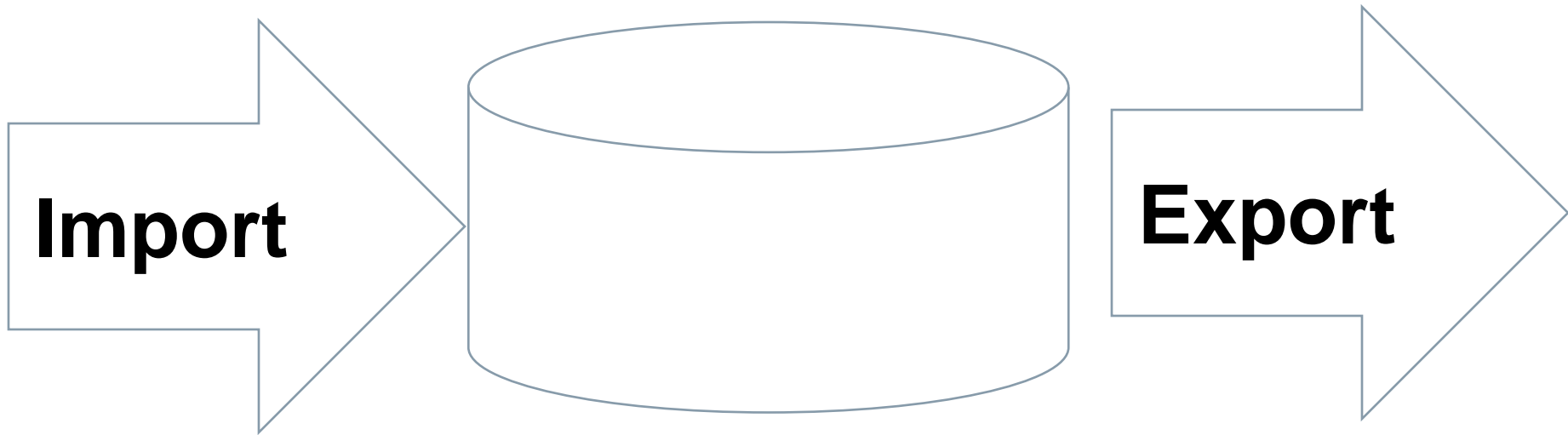
Genesis of the internal data model: Arguments against home-brew models

- Homebrew means re-doing work others have already done (and that probably much more thoroughly than you have time for)



- Homebrew necessarily increases “distance” (see next slide)

Implications of „distance“ between the exchange standard and your data model: Import and Export

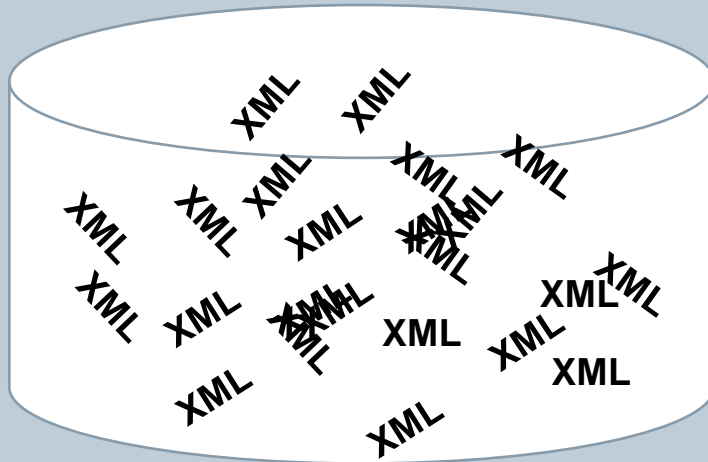


- The further removed your internal data model is, the more you have to work for import and export
- The real problem is the import: what to do with information that cannot be mapped into your internal data model?
 - reject and don't import at all?
 - import partially (as far as it fits your data model?)

Flexibility: two extremes

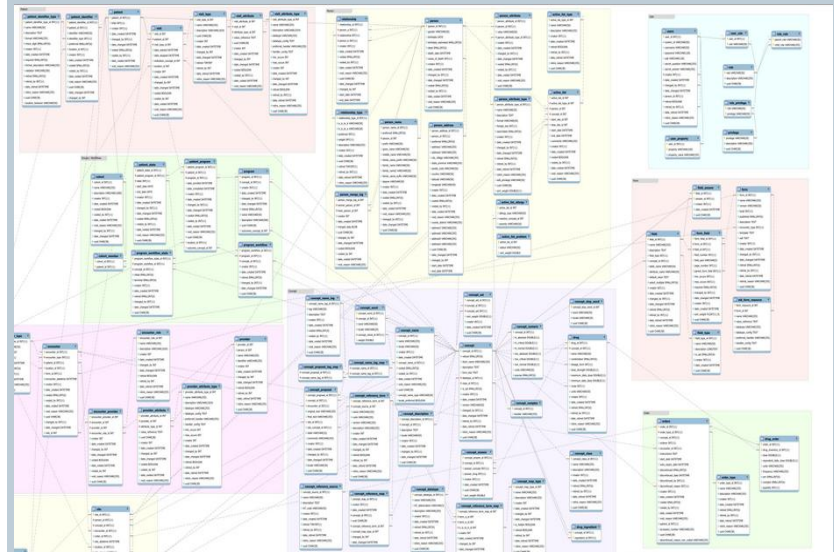
Extremely flexible

- Just dump each file into an XML database (assuming that your main standard is in XML) ...



Rather inflexible

- Create a database model for a given revision of some part of the standard



Implications of flexibility: Processing

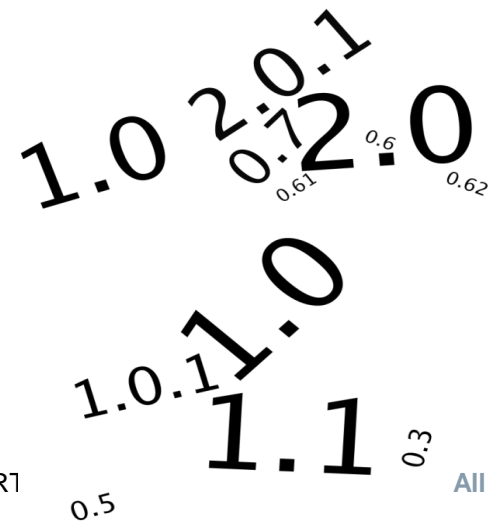
- Flexibility eases import, but makes processing more complicated, since you cannot assume that things always look the same:
 - **automated mechanisms** must be able to deal with different representations of data ... and in all likelihood will fail in some cases
 - **visualization/presentation** to the user becomes more complicated; your users will require a higher level of expertise regarding the data format
 - **export** becomes a challenge: you have imported data in revisions X, Y, and Z of a given standard; to what revision can you export?

Our choices for the MANTIS data model

- **Genesis:** “stand on the shoulders of giants” – the data model mirrors the threat intelligence exchanges standards that are relevant to us
- **Distance:** exchange standards and data model are *very* close (for details see next few slides)
- **Flexibility:**
 - regarding import: the Mantis importer is *very* forgiving and will import,
 - e.g., different revisions of STIX/CybOX in a sensible way with relatively little effort in adapting the importer to revision changes
 - XML that does quite conform to a standard’s XML schema
 - regarding the challenges wrt. processing and export: much of this is still future work ... but following the “crawl, walk, run” approach: we are already able to crawl ...

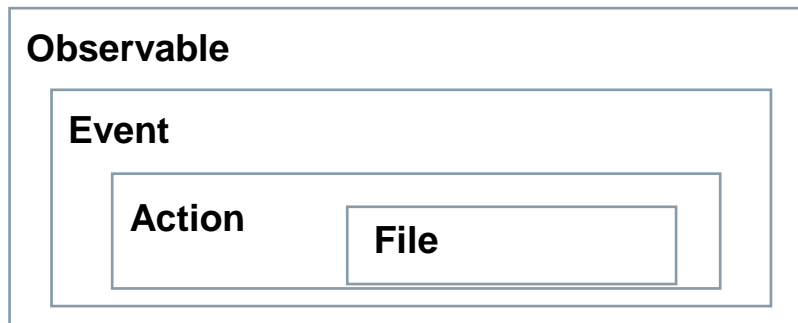
Why do we need maximum tolerance for exchange data formats and their revisions?

- At the moment, we cannot do without OpenIOC, so a STIX/CybOX-exclusive solution will not work. And it looks like we will also start importing the MISP data format ...
 - ➔ need to be able to import several standards
- I bet you that two years, after STIX 3.0 has been released, there will still be persons or tools that keep sending you STIX 1.0.1 ...
 - ➔ need to be able to import different revisions

The logo for OpenIOC, featuring the text "OpenIOC" in white on a dark blue rectangular background.The logo for CybOX, featuring the text "CybOX" in blue with a magnifying glass icon over the letter "o".The logo for STIX, featuring the text "STIX" in bold black letters with a red "X" and a trademark symbol.A collection of version numbers for STIX, including 1.0, 2.0, 1.0.1, 0.61, 0.6, 0.62, 1.0.1, 1.1, 1.1, 0.5, and 0.3, scattered and tilted.

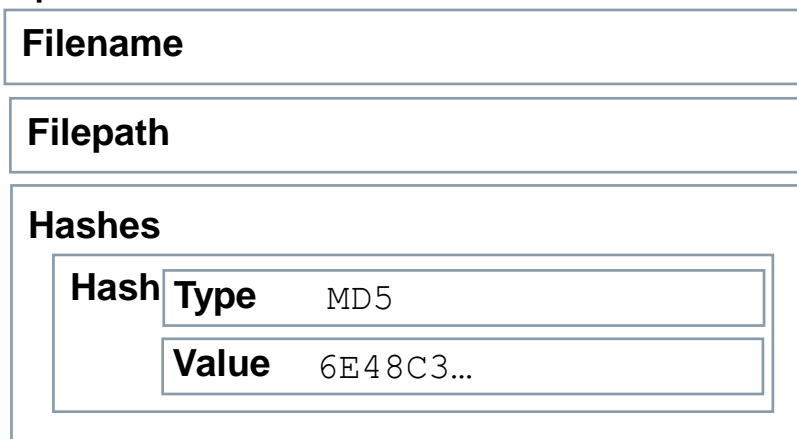
MANTIS's data model: pretty flexible, but a trying to do a bit more than just dumping XMLs or JSONs

- If you look at STIX and CybOX, you see that XML's hierachical structure is used for two different purposes:
 - modelling of containment relations between different objects



This, MANTIS preserves

- description of facts



This, MANTIS flattens into a list of „fact term“-value pairs ... and **deduplicates** these facts

Example: A CybOX Observable XML Source

```
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
  <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
    <cybox:Actions>
      <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1blade75f" action_status="Success"
        context="Host" timestamp="2013-04-08T09:22:00.0Z">
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Create</cybox:Type>
        <cybox:Name xsi:type="cyboxVocabs:ActionNameVocab-1.0">Create File</cybox:Name>
        <cybox:Associated_Objects>
          <cybox:Associated_Object id="example:Object-5ec92e95-a31f-470b-97c4-aa9046189fbb">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:File_Name>foobar.dll</FileObj:File_Name>
              <FileObj:File_Path>C:\Windows\system32</FileObj:File_Path>
              <FileObj:Hashes>
                <cyboxCommon:Hash>
                  <cyboxCommon:Type>MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value datatype="hexBinary">
                    6E48C348D742A931EC2CE90ABD7DAC6A
                  </cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
            <cybox:Association_Type
              xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-1.0">
                Affected</cybox:Association_Type>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>
```

Example: Importing a CybOX 2.0 Observable XML Source: Focusing on objects and facts

```

<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
  <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
    <cybox:Actions>
      <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1blade75f" action_status="Success"
        context="Host" timestamp="2013-04-08T09:22:00.0Z">
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Create</cybox:Type>
        <cybox:Name xsi:type="cyboxVocabs:ActionNameVocab-1.0">Create File</cybox:Name>
        <cybox:Associated_Objects>
          <cybox:Associated_Object id="example:Object-5ec92e95-a31f-470b-97c4-aa9046189fbb">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:File_Name>foobar.dll</FileObj:File_Name>
              <FileObj:File_Path>C:\Windows\system32</FileObj:File_Path>
              <FileObj:Hashes>
                <cyboxCommon:Hash>
                  <cyboxCommon:Type>MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value datatype="hexBinary">
                    6E48C348D742A931EC2CE90ABD7DAC6A
                  </cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
            <cybox:Association_Type
              xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-1.0">
                Affected</cybox:Association_Type>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>

```

Observed event. An action that creates a file with certain file name, file path and hash

Example: A CybOX Observable XML Source

Defining object boundaries

```
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
  <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
    <cybox:Actions>
      <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1blade75f" action_status="Success"
        context="Host" timestamp="2013-04-08T09:22:00.0Z">
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Create</cybox:Type>
        <cybox:Name xsi:type="cyboxVocabs:ActionNameVocab-1.0">Create File</cybox:Name>
        <cybox:Associated_Objects>
          <cybox:Associated_Object id="example:Object-5ec92e95-a31f-470b-97c4-aa9046189fbb">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:File_Name>foobar.dll</FileObj:File_Name>
              <FileObj:File_Path>C:\Windows\system32</FileObj:File_Path>
              <FileObj:Hashes>
                <cyboxCommon:Hash>
                  <cyboxCommon:Type>MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value datatype="hexBinary">
                    6E48C348D742A931EC2CE90ABD7DAC6A
                  </cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
            <cybox:Association_Type
              xsi:type="cyboxVocabs:ActionObjectAssociationTypeVocab-1.0">
                Affected</cybox:Association_Type>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>
```

In the XML, an identifier is provided for each structure that naturally gives rise to an information object of its own.

Example: A CybOX Observable XML Source Extracting „flat“ facts from hierarchical XML

```

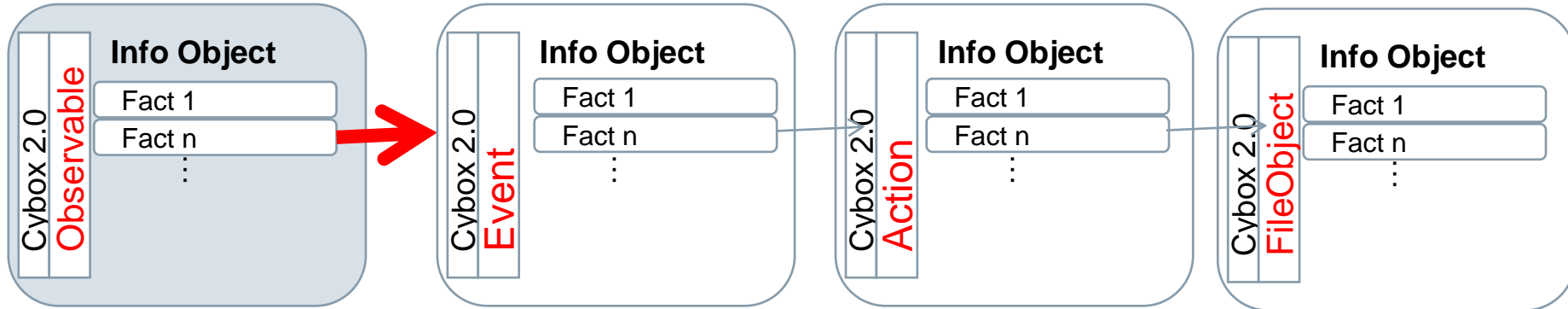
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
  <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
    <cybox:Actions>
      <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1blade75f" action_status="Success"
        context="Host" timestamp="2013-04-08T09:22:00.0Z">
        <cybox:Type xsi:type="cyboxVocabs:ActionTypeVocab-1.0">Create</cybox:Type>
        <cybox:Name xsi:type="cyboxVocabs:ActionNameVocab-1.0">Create File</cybox:Name>
        <cybox:Associated_Objects>
          <cybox:Associated_Object id="example:Object-5ec02e95-a21f-470b-07c4-aa9046189fbb">
            <cybox:Properties xsi:type="FileObj:FileObjectType">
              <FileObj:File_Name>foobar.dll</FileObj:File_Name>
              <FileObj:File_Path>C:\Windows\system32</FileObj:File_Path>
              <FileObj:Hashes>
                <cyboxCommon:Hash>
                  <cyboxCommon:Type>MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value datatype="hexBinary">
                    6E48C34D742A931EC2CE90ABD7DAC6A
                  </cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
          </cybox:Associated_Object>
        </cybox:Associated_Objects>
      </cybox:Action>
    </cybox:Actions>
  </cybox:Event>
</cybox:Observable>

```

The facts we are really interested into about the observed file are:

- Properties/File_Name = foobar.dll
- Properties/File_Path = C:\Windows\system32
- Properties/Hashes/Hash/Type = MD5
- Properties/Hashes/Hash/Simple_Hash_Value = 6E48C34D742A931EC2CE90ABD7DAC6A

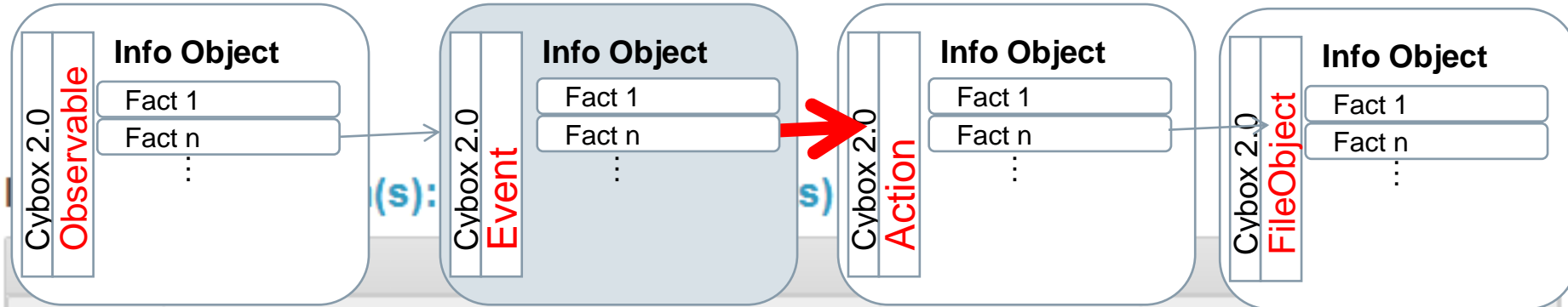
Example: Importing a CybOX 2.0 Observable Resulting Structure



Info Object: **Event: Action(s): Create File (6 facts) ...**

Identifying data			
Identifier	http://example.com:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2	Timestamp	2014-06-19T00:07:21.713707+02:00
Type	cybox.mitre.org:Observable 2 (http://cybox.mitre.org/cybox)	Import Timestamp	2014-06-19T00:07:21.713707+02:00
Facts			
Event	Action(s): Create File (6 facts) ...		

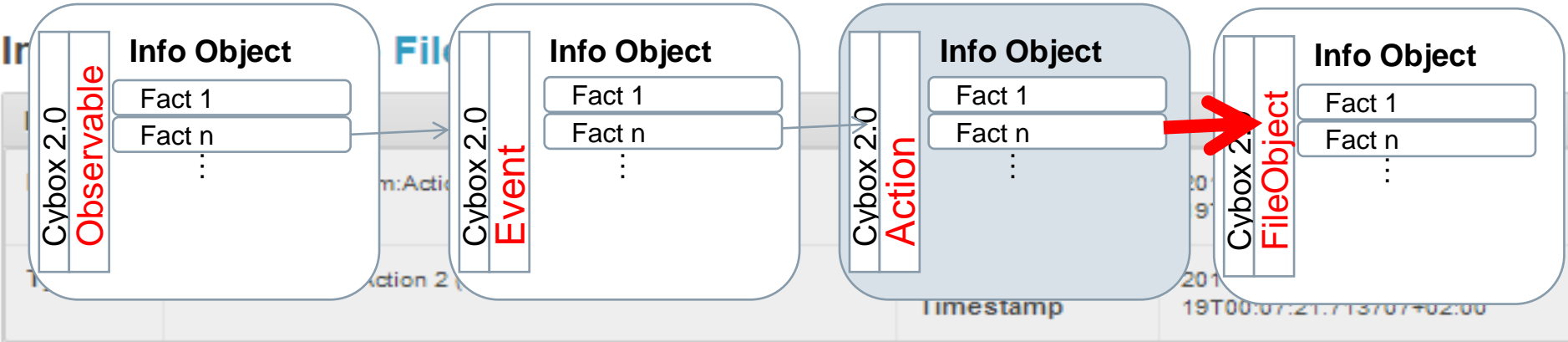
Example: Importing a CybOX 2.0 Observable Resulting Structure



Identifier	http://example.com:Event-44578886-b0c5-4551-84dd-0f1f02f8210f	Timestamp	2014-06-19T00:07:21.713707+02:00
Type	cybox.mitre.org:Event 2 (http://cybox.mitre.org/cybox)	Import Timestamp	2014-06-19T00:07:21.713707+02:00

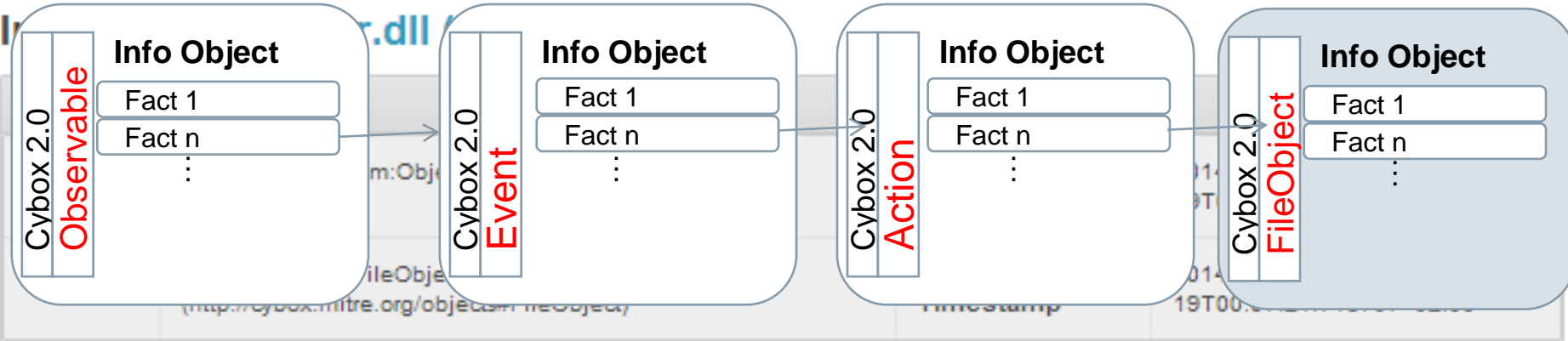
Facts							
Actions	<div style="background-color: red; color: white; padding: 5px; display: flex; align-items: center;"> <input type="text" value="Create File (6 facts)"/> </div> <table border="1" style="margin-top: 5px;"> <tr> <td>@action_status</td> <td>Success</td> </tr> <tr> <td>@context</td> <td>Host</td> </tr> <tr> <td>@timestamp</td> <td>2013-04-08T09:22:00.0Z</td> </tr> </table>	@action_status	Success	@context	Host	@timestamp	2013-04-08T09:22:00.0Z
@action_status	Success						
@context	Host						
@timestamp	2013-04-08T09:22:00.0Z						

Example: Importing a CybOX 2.0 Observable Resulting Structure



Facts	
@action_status	Success
@context	Host
@timestamp	2013-04-08T09:22:00.0Z
Type	Create
Name	Create File
Associated_Objects	Associated_Object foobar.dll (5 facts)

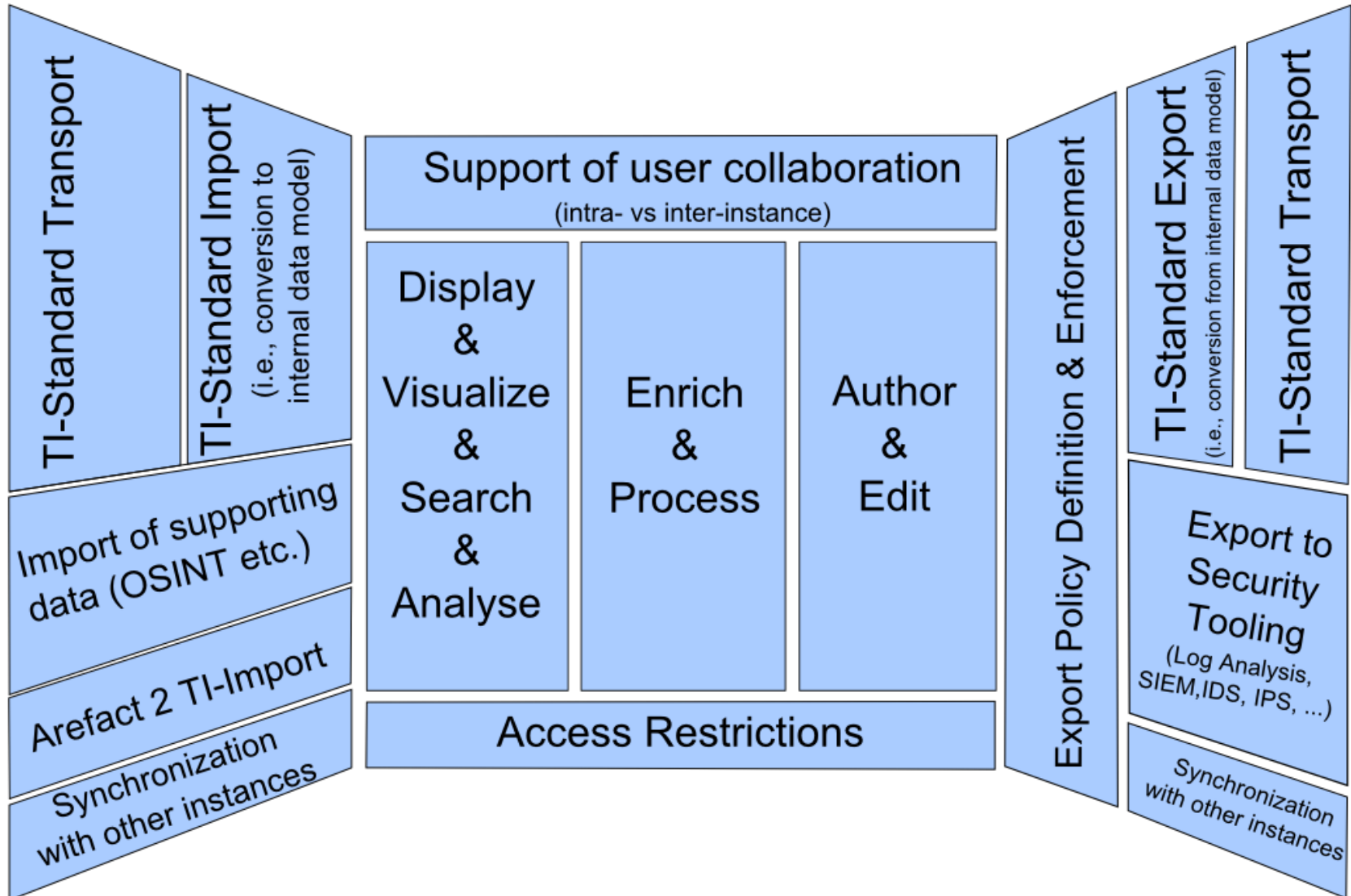
Example: Importing a CybOX 2.0 Observable Resulting Structure



Facts				
Properties	File_ Name	foobar.dll		
	File_ Path	C:\Windows\system32		
	Hashes	Hash	Type	MD5
Simple_ Hash_ Value			6E48C348D742A931EC2CE90ABD7DAC8A	

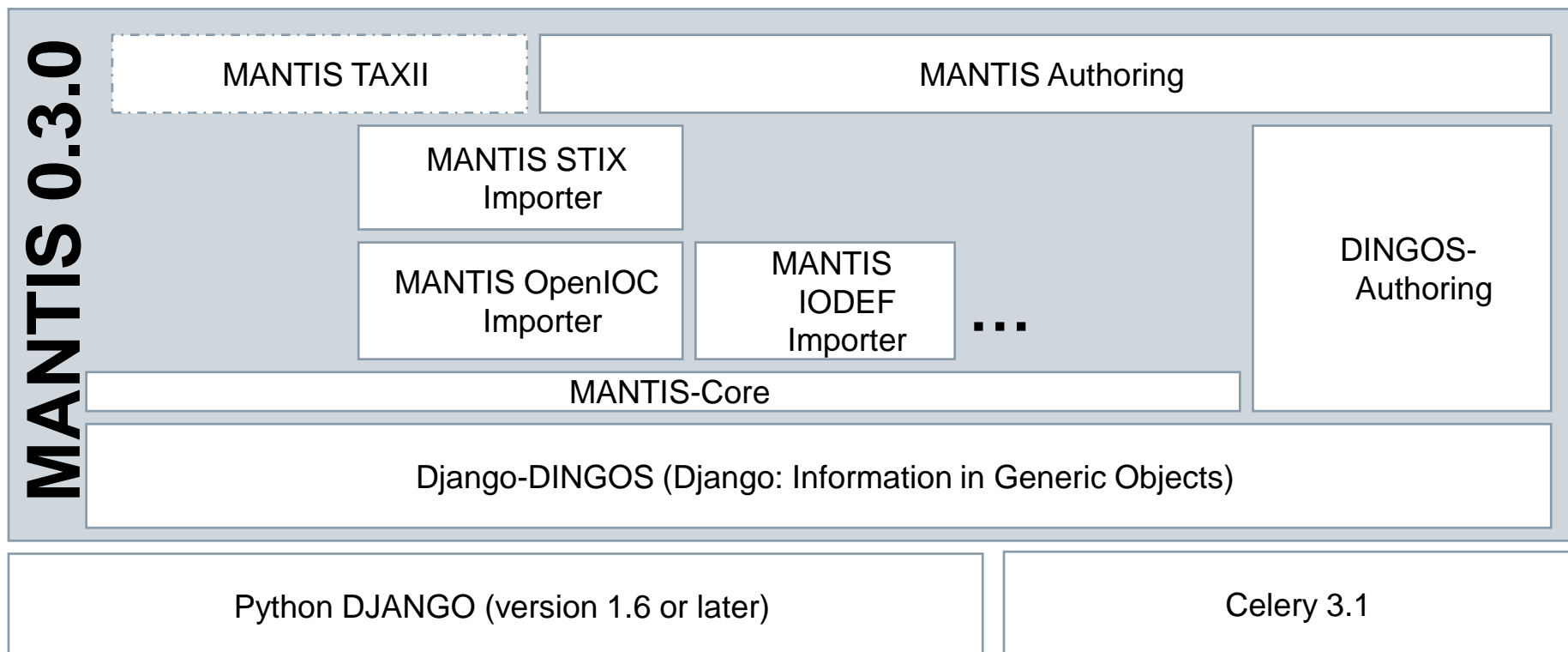
Presentation to user mirrors hierarchical composition of facts, but underlying data model contains flattened „fact terms“

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality

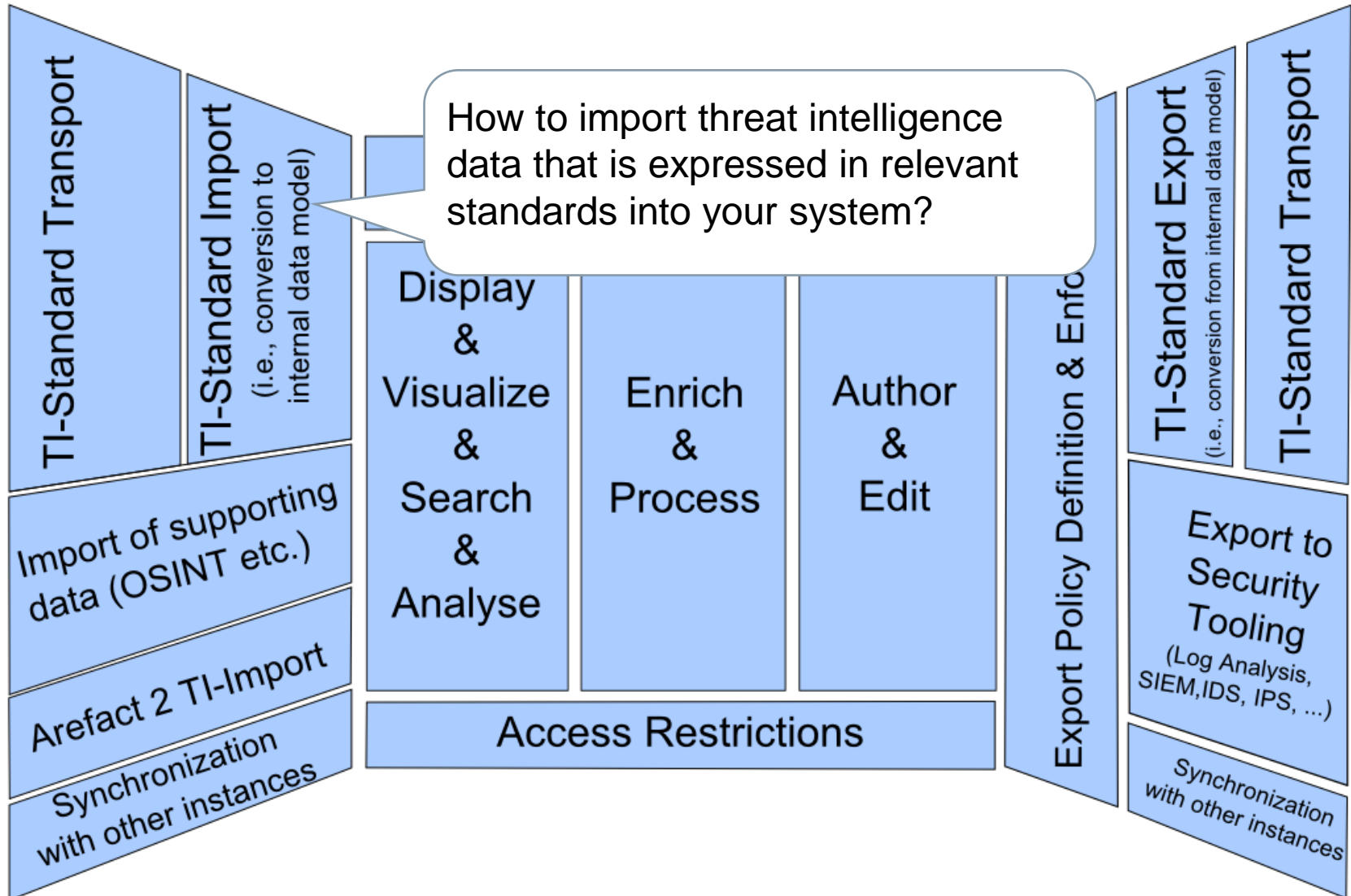


Siemens CERT's MANTIS Framework

- MANTIS is based on Django, the Python-based web application framework.
- The current version of MANTIS contains import modules for STIX/Cybox, OpenIOC, and IODEF, but the architecture of MANTIS is generic and provides for easy generation of additional import modules for other standards.

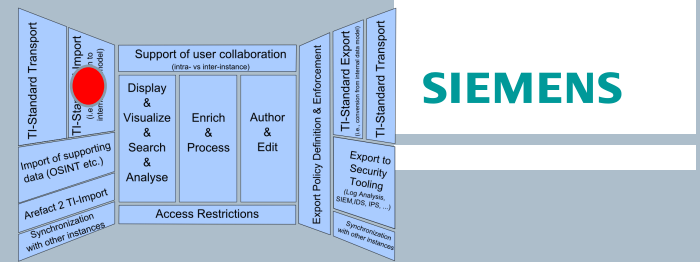


(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

TI-Standard Import

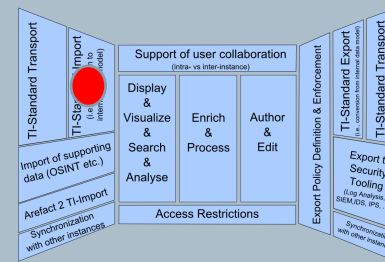


- We have talked about how STIX/CybOX XML is imported into MANTIS
- The MANTIS framework provides a generic importer class that has been customized to import
 - CybOX/STIX
 - OpenIOC indicators
 - IODEF
- Importer function can be triggered
 - programmatically (using Celery for task management)
 - via commandline for scripting
 - via GUI 'XML Import' dialogue
 - via authoring GUI (import OpenIOC into STIX Test Mechanism)

MANTIS

TI-Standard Import

XML-Import via GUI



Name:

Name is displayed in list of imported XML; the name is not used in the import.

Xml:

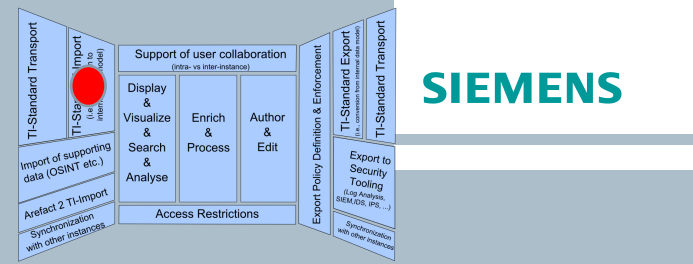
```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation=
    "http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 ../cybox/objects/Domain_Name_Object.xsd"
  id="example:STIXPackage-f61cd874-494d-4194-a3e6-6b487dbb6d6e"
  timestamp="2014-05-08T09:00:00.000000Z"
  version="1.1.1"
>
<stix:STIX_Header>
  <stix:Title>Example watchlist that contains domain information.</stix:Title>
  <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-
```

ATTENTION: Make sure that the identifier namespaces occurring in the XML are contained in your allowed namespaces (see display on right-hand side)!!! Otherwise, the created objects will be moved into a temporary namespace!!!

Import

MANTIS

Import of OpenIOC as part of STIX Authoring



STIX Package Campaign Info Indicator Pool **IOC** Observable Pool Observable Relations

Test Mechanisms

cert_my_organization:Test_Mechanism-6d2a1b03-b216-4cd8-9a9e-8827af6ebf93

loc title: zeus_openioc.xml

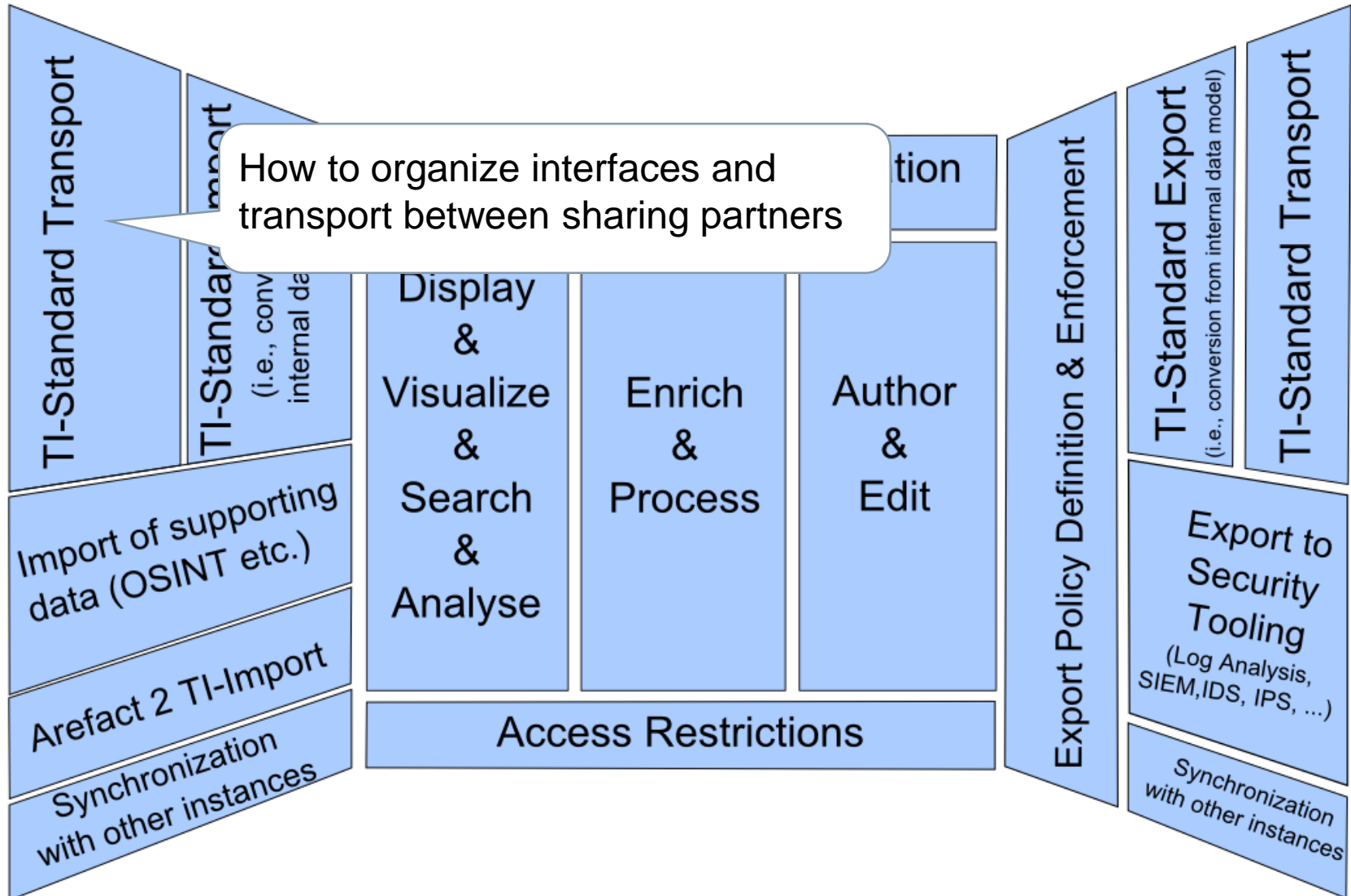
loc description:

File Dropzone



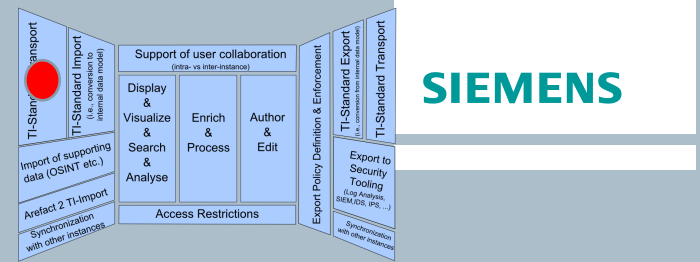
Drag & Drop

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

TI-Standard Import

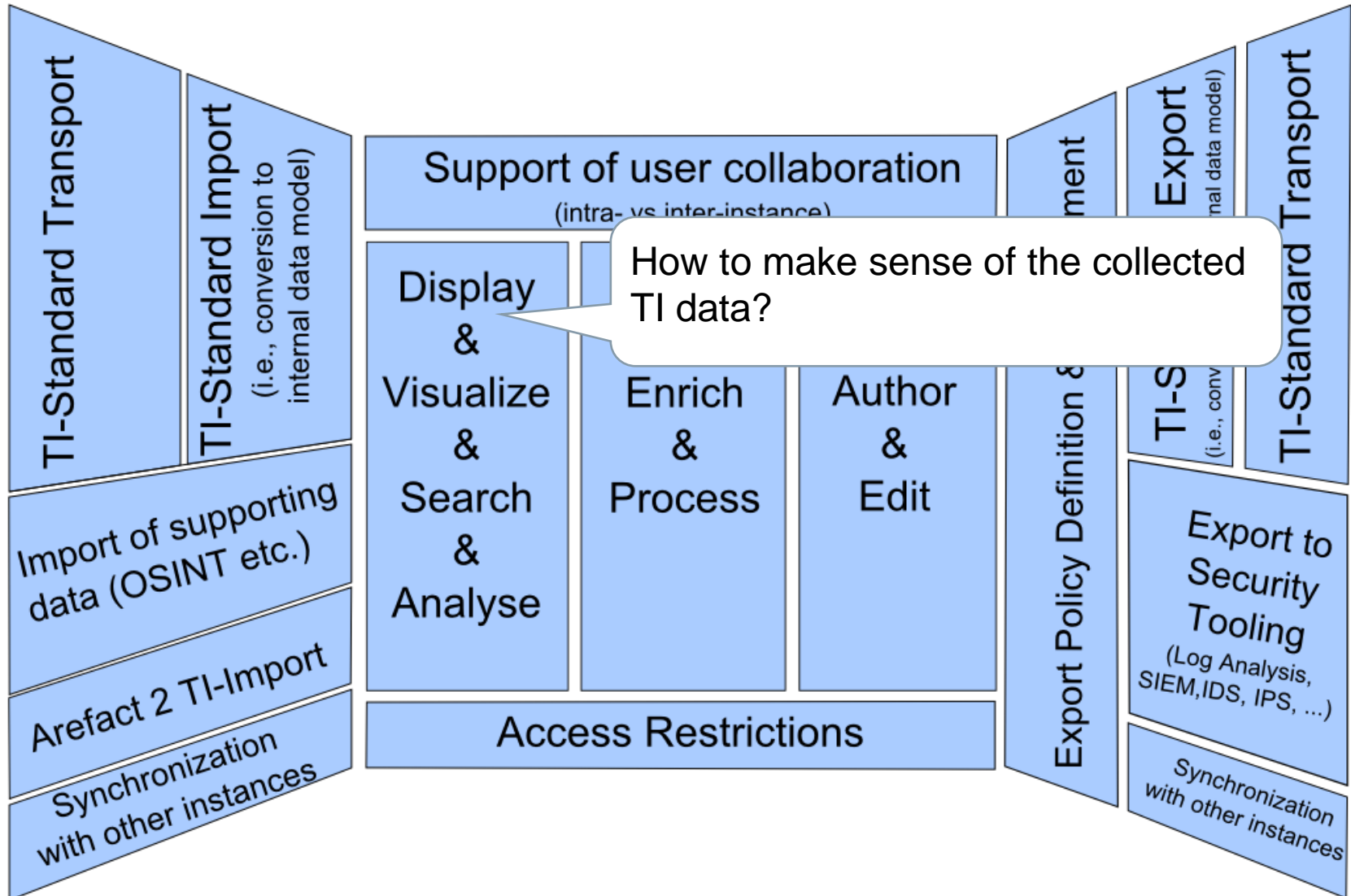


- For organizing interfaces for import from external sharing partners, we plan to leverage



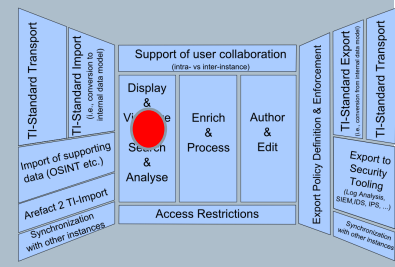
- Luckily, MITRE's TAXII proof-of-concept implementation YETI is also running on top of Django
- Imports registered by YETI can be made to trigger a import task in MANTIS (using Celery for asynchronous processing)

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

Filtering by Object Property



Filter Parameters

InfoObject Type:	-----
Object Type matches:	
InfoObject Family:	----- ▾
Name contains:	
ID Namespace:	----- ▾
ID contains:	
Object Creation Timestamp:	Any date ▾
Import Timestamp:	Any date ▾
Marking ID contains:	

Submit Query Save Search

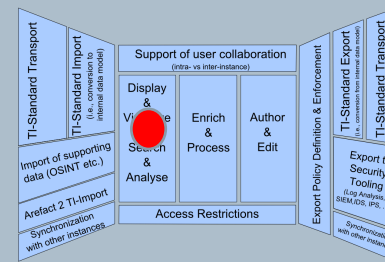
Filter Parameters

InfoObject type:	stix.mitre.org:STIX_Package ▾
Object Type matches:	<ul style="list-style-type: none"> cybox.mitre.org:Observable cybox.mitre.org:ProcessObject cybox.mitre.org:URIObject cybox.mitre.org:WinDriverObject cybox.mitre.org:WinExecutableFileObject cybox.mitre.org:WinProcessObject cybox.mitre.org:WinRegistryKeyObject cybox.mitre.org:WinServiceObject data-marking.mitre.org:Marking ioc.mandiant.com:DriverItem ioc.mandiant.com:FileItem ioc.mandiant.com:ioc ioc.mandiant.com:ProcessItem ioc.mandiant.com:RegistryItem ioc.mandiant.com:ServiceItem ioc.mandiant.com:UrlHistoryItem stix.mitre.org:Indicator stix.mitre.org:Kill_Chain stix.mitre.org:Kill_Chain_Phase stix.mitre.org:STIX_Package
Object Type matches:	
InfoObject Family:	
Name contains:	
ID Namespace:	
ID contains:	
Object Creation Timestamp:	
Import Timestamp:	
Marking ID contains:	

Submit Query Save Search

MANTIS

Filtering by Fact Property

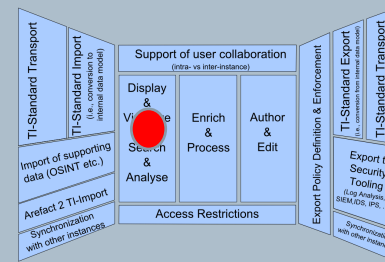


Filter Parameters

Fact term (w/o attribute) matches:	<input type="text" value="Hashes/Hash/SimpleHashValue"/>
Attribute matches:	<input type="text"/>
Value contains:	<input type="text"/>
Object name contains:	<input type="text"/>
Object Timestamp:	<input type="text" value="Any date"/> ▼
Import Timestamp:	<input type="text" value="Any date"/> ▼
ID Namespace:	<input type="text" value="-----"/> ▼
InfoObject Type:	<input type="text" value="-----"/> ▼
Object Type name contains:	<input type="text"/>
Marking ID contains:	<input type="text"/>

MANTIS

Displaying Information Objects



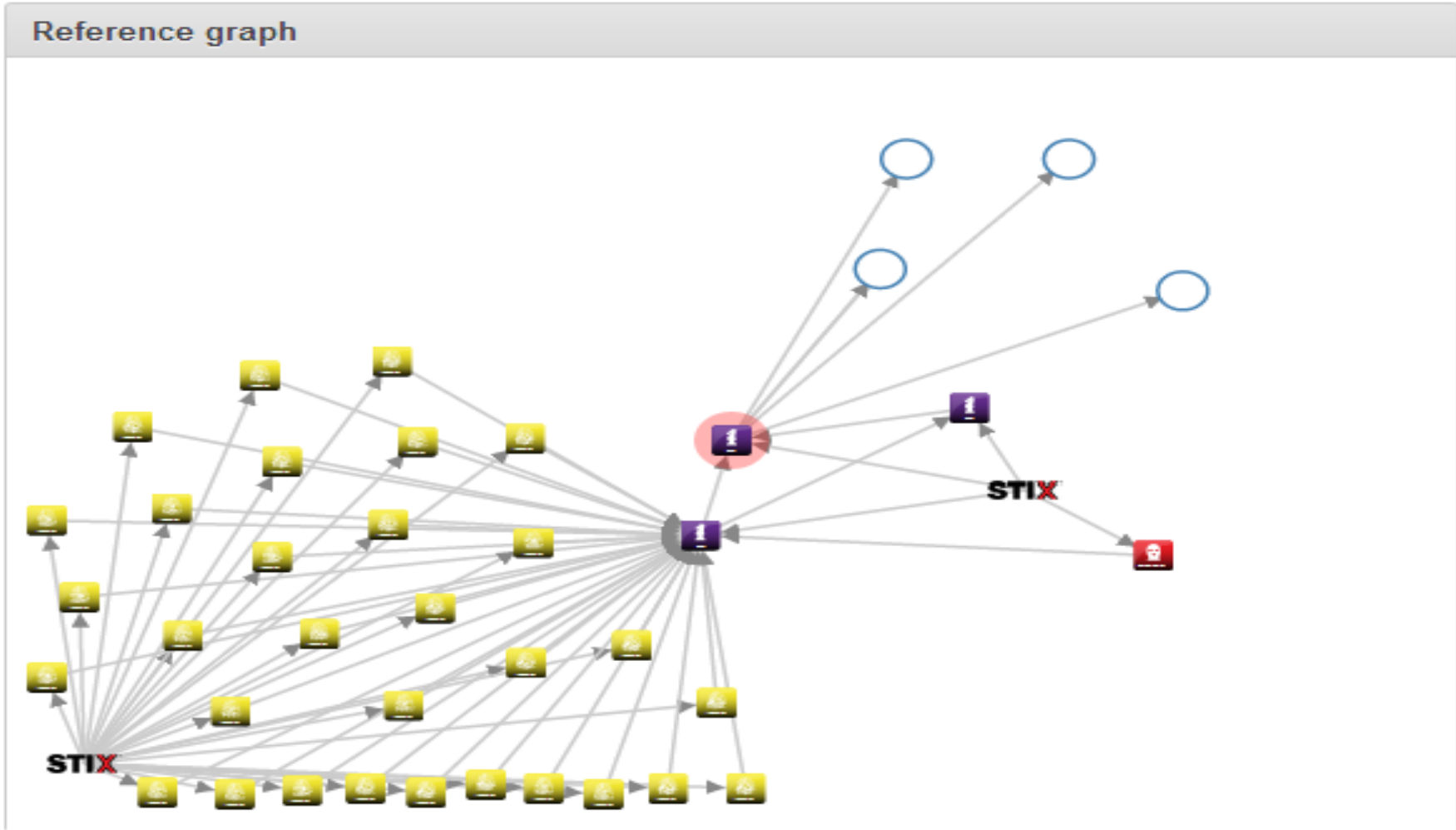
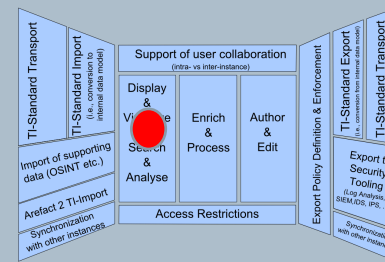
Identifying data			
Identifier	http://www.mandiant.com:ttp-33159b98-3264-4e10-a968-d67975b6272f	Timestamp	2013-02-19T01:00:02+01:00
Type	stix.mitre.org:TTP 1 (http://stix.mitre.org/TTP)	Import Timestamp	2014-06-18T13:29:09.473642+02:00

Facts				
@xsi:type	TTPType			
Title	HTRAN Malware C2			
Behavior	Malware	Malware_Instance	Type	Relay
			Name	HUC Packet Transmit Tool (HTRAN)
			Description	<!DOCTYPE html> <html> <body> <p> When APT1 attackers are not using WERC2, they require a

Resources	Infrastructure	Type	Leveraged IP Blocks			
		Observable_Characterization	Observable	Object	🔍	143.89.255.255 (condition InclusiveBetween) (4 facts)
			Observable	Object	🔍	143.89.255.255 (condition InclusiveBetween) (4 facts)

MANTIS

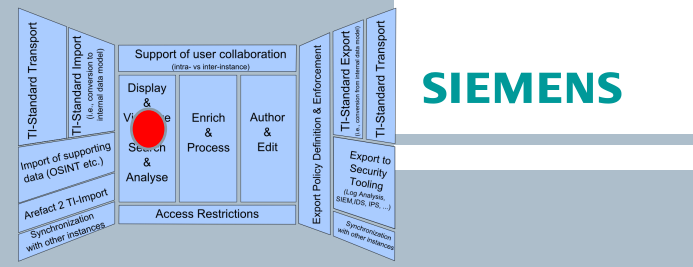
Visualizing Object Relations



MANTIS

Searching Objects and Facts

What we can search for



Object Properties

Info Object: **APT1 Tactics, Techniques and Procedures**

Identifying data			
Identifier	http://www.mandiant.com/ttp-c63f31ac-871b-4846-aa25-de1926f4f3c8	Timestamp	2013-02-19T01:00:02+01:00
Type	stix.mitre.org:TTP 1 (http://stix.mitre.org/TTP)	Import Timestamp	2014-04-10T12:54:35.800000000Z

2 markings

[your.organization.com:WHITE](http://www.mandiant.com/APT1: Exposing One of China's Cyber Espionage Units (the)

Markings

Facts			
	Value		
@xsi:type	TTPType		ttp
Intended_Effect	Description	<!DOCTYPE html> <html><body> <p> Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership. We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed. </P> </body></html>	String
Intended_Effect	Description	@structuring_format HTML5	String
Intended_Effect	Value	Advantage - Economic	IntendedEffectVocab-1.0

Current revision of 1 revision

Embedded in 2 objects

People's Liberation Army

<http://www.mandiant.com/threat-actor-8dff0344-0c82-4079-8d04-6f3e4d9bd1df>

2013-02-19T01:00:02+01:00

Referenced revision: Latest revision

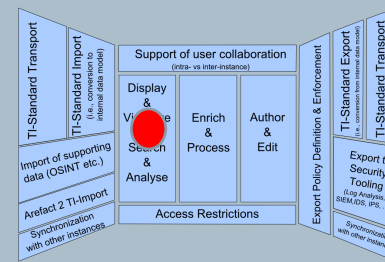
as Observed_TTPs/Observed_TTP/TTP

APT1: Exposing One of China's Cyber Espionage Units

Fact Terms and Fact Values

MANTIS

Search Interface for Facts



Filter Parameters

```
fact: [Properties/Value] regexp "business"  
| object: identifier.namespace contains 'mandiant.com'  
  && object_type.name contains 'URIObject'  
| marked_by: (fact: [Marking_Structure/Statement] contains 'APT1')
```

Paginate by

50

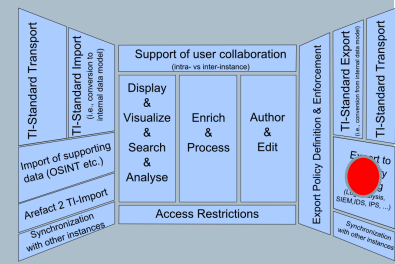


Execute query

Save Search

MANTIS

Editing saved searches



SIEMENS

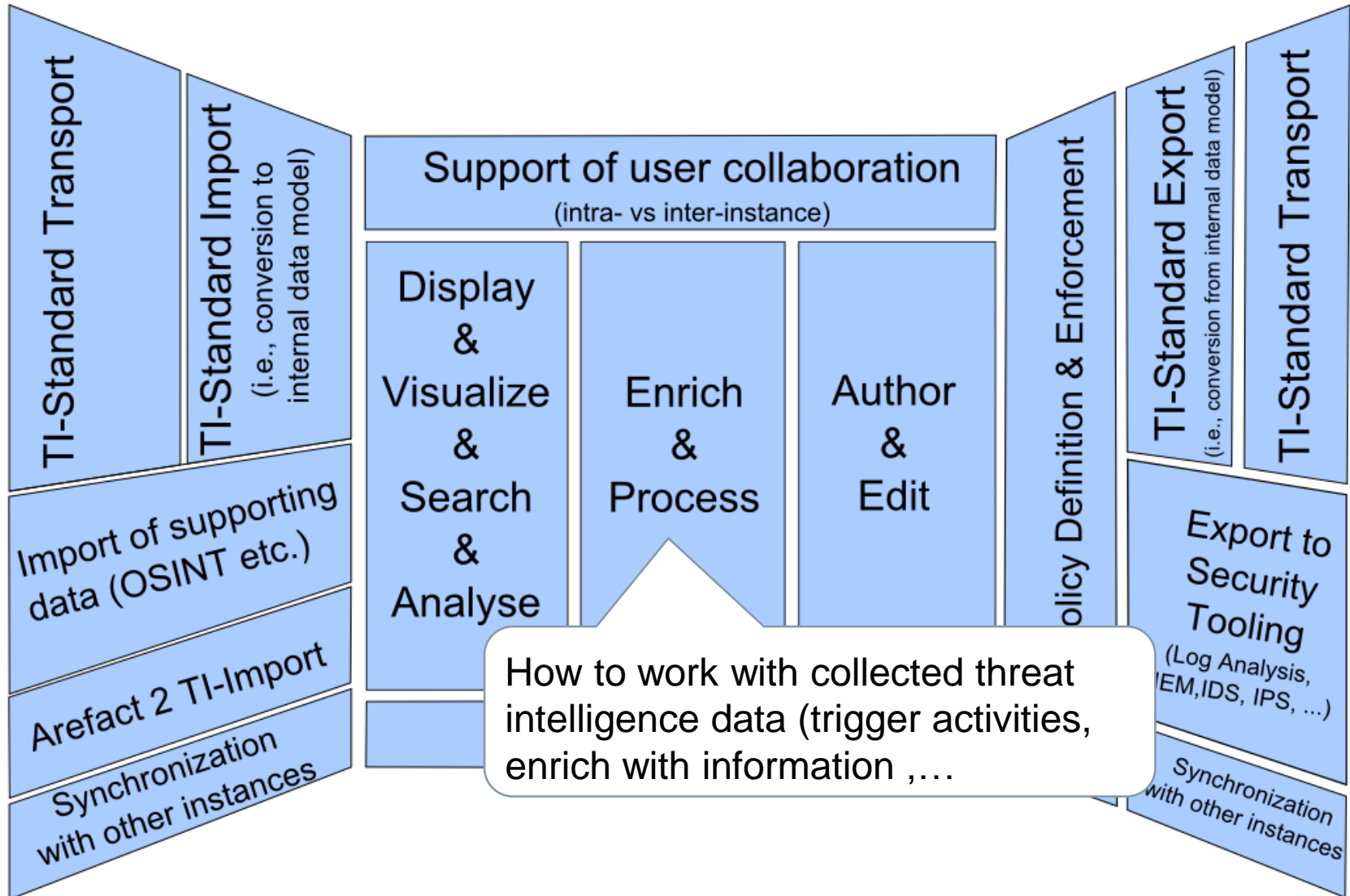
Saved searches for user John Doe

Available searches				
Name	Link	Custom Query	Parameters	Actions
<input type="text" value="Filter for STIX Packages"/>	/mantis/View/InfoObject	<code>{}</code>	<input type="text" value="iobject_type=72"/>	
<input type="text" value="Filter for OpenIOC Indicator"/>	/mantis/View/InfoObject	<code>{}</code>	<input type="text" value="iobject_type=71"/>	
<input type="text" value="Network Indicators of past two days"/>	/mantis/Search/CustomFactSearch	<code>fact: fact_term regexp 'URI Domain_Name Properties/Value\$ Properties/Address_Value' && attribute != 'condition' && @[condition] = 'Equals'</code>	<input type="text" value="paginate_by=50"/>	
<input type="text" value=""/>	/mantis/View/InfoObject	<code>{}</code>	<input type="text" value="iobject_type=157"/>	

This is a temporary entry and won't be persisted unless you give it a name and press save.

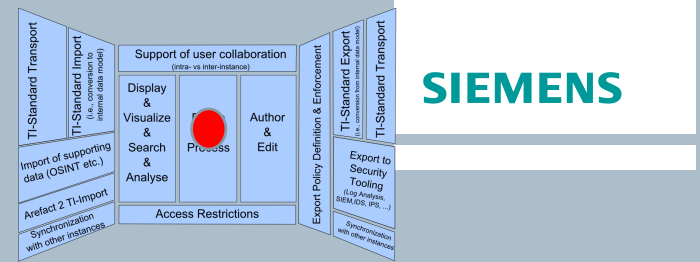
Save

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



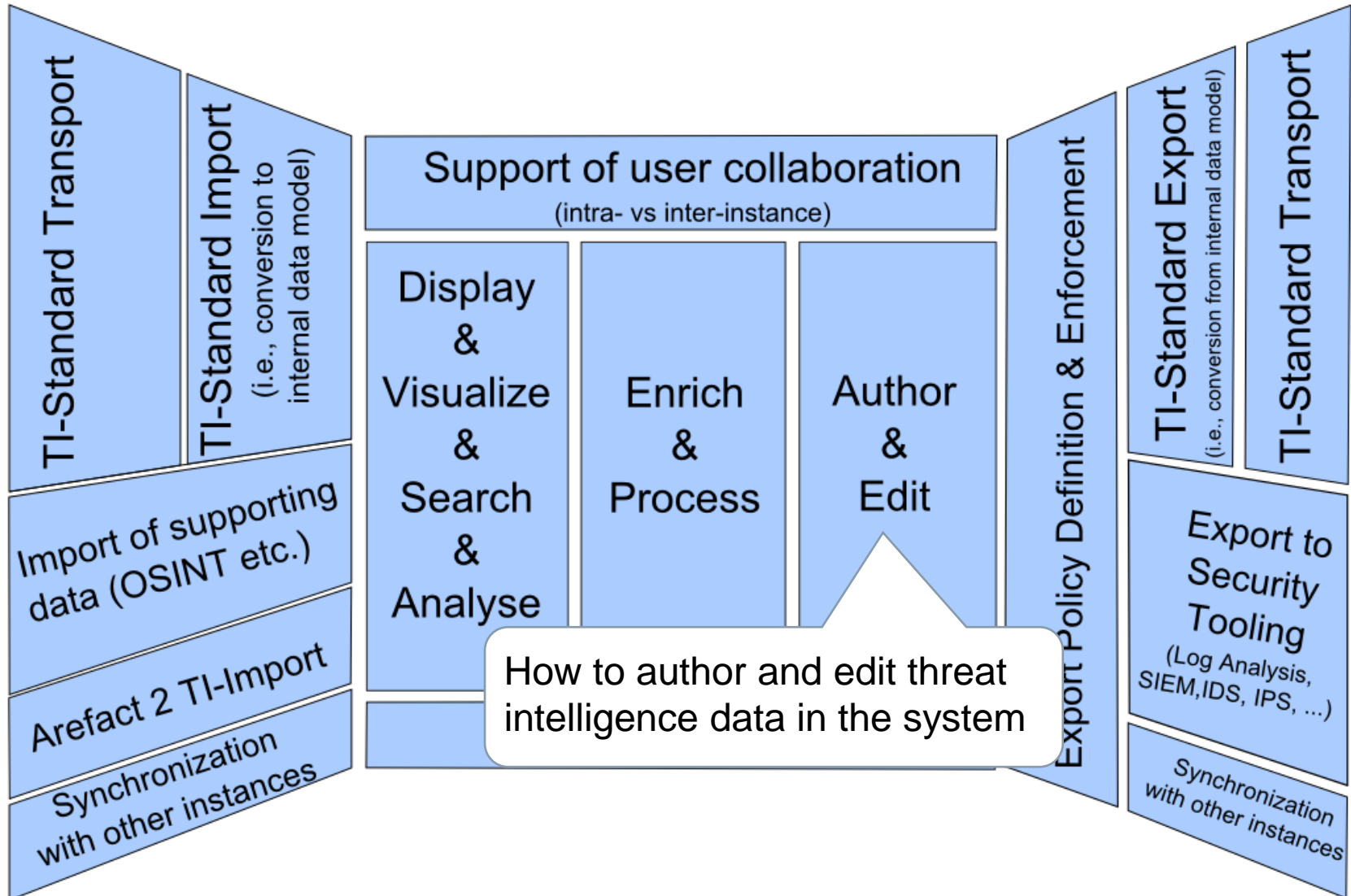
MANTIS

Processing & Enrichment of Data

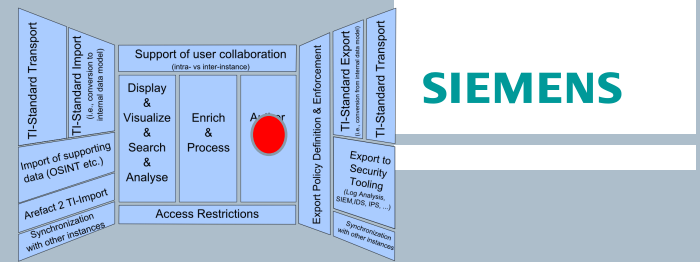


- MANTIS 0.3.0 does not offer standard methods for processing and enriching data
- In our internal instance customized for our use, we employ base classes offered by the MANTIS framework to implement
 - actions on objects
 - marking of objects with additional information
- First standard processing/enrichment method likely to be implemented by the next MANTIS release will be object tagging (i.e., marking of objects with relatively restricted markings)

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality

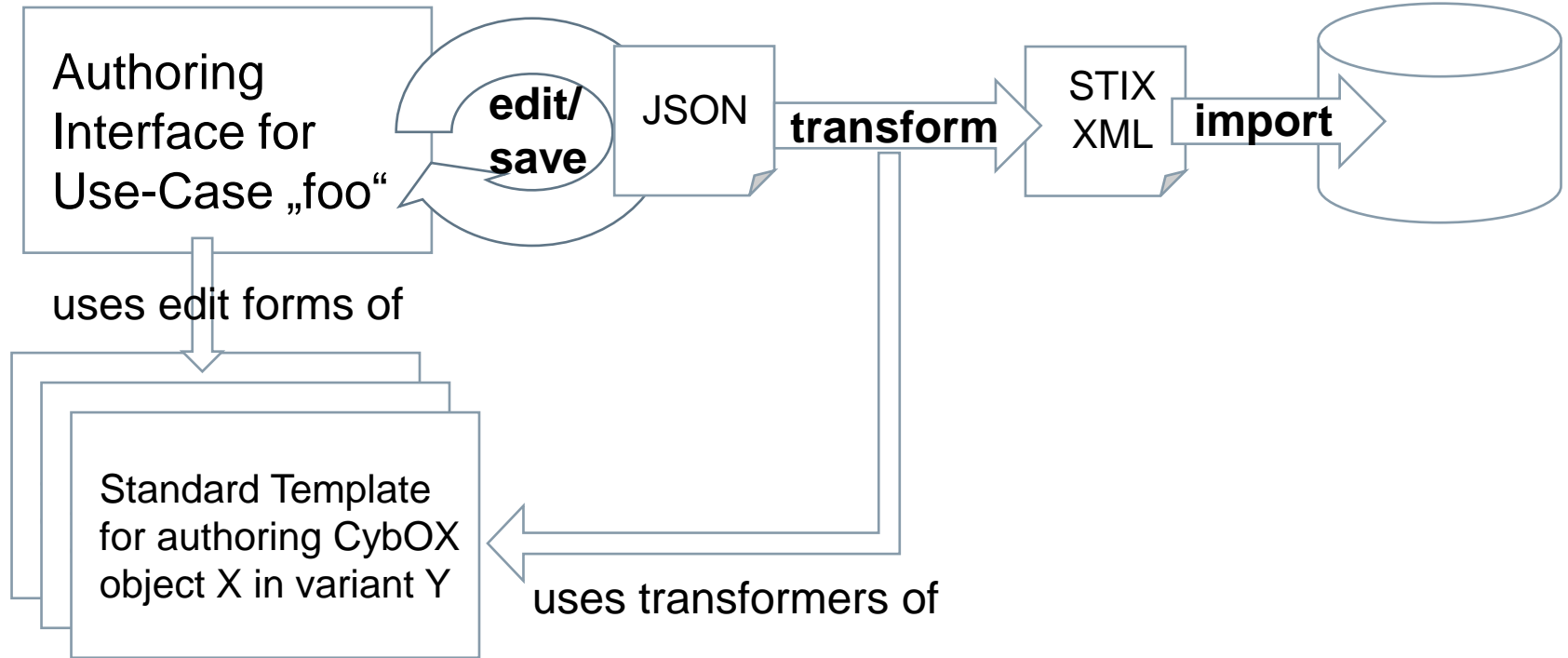
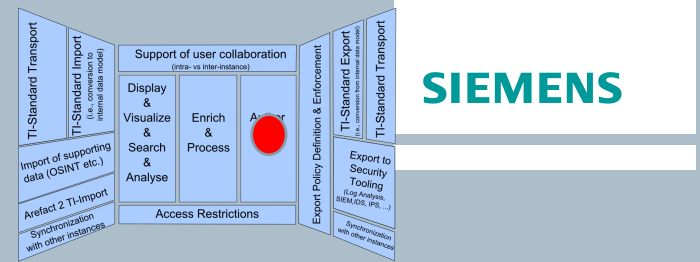


Interlude: The problem of authoring STIX and CyboX



- STIX and CyboX are complex, ...really, really complex
- The STIX/CyboX community is in the process of working out the intended usage of STIX/CyboX for standard use-cases (just last week, a discussion of how to communicate sightings of a given indicator got started on the mailing list)
- There will be organization/company-specific specializations of standard use-cases.
- Your tool needs a way to codify standard use cases such that the user can concentrate on entering the right data, while the tool takes care of generating STIX/CyboX that follows the intended usage for the particular use-case

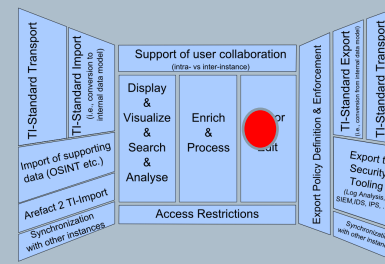
MANTIS's approach to authoring and editing threat intelligence



Objects originating from imported reports maintain a relationship with the defining JSON structure; the report can be modified by re-opening the JSON, editing it and carrying out another import: existing objects are then overwritten with the newly created version.

MANTIS

Authoring Campaign and Threat Actor



STIX Package	Campaign Info	Indicator Pool	IOC	Observable Pool	Observable Relations
--------------	---------------	----------------	-----	-----------------	----------------------

Campaign Information

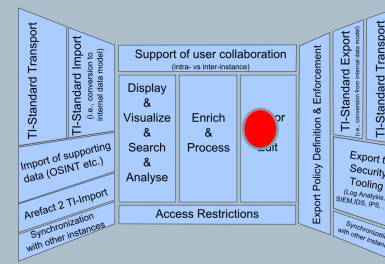
Name:	Campaign 0815 <small>*required</small>
Title:	First observed campaign against HR Department with aim of tax fraud carried out by Robin H00d
Description:	This is the first time we observe a campaign by adversary Robin H00d against our HR department with the obvious aim of stealing data that can be used to file tax returns in the name of our employees.
Status:	Ongoing
Activity timestamp from:	
Activity timestamp to:	
Confidence:	High

Threat Actor Information

Identity name:	R
Identity aliases:	<ul style="list-style-type: none"> stix.mitre.org:ThreatActor threat-actor-f1ce5a9e-0fb7-465b-acb9-e7f75098eee9 Comment threat-actor-5abb4d96-e3f2-4a1a-b025-c5b63ec6eb0b Comment Group threat-actor-d5b62b58-df7c-46b1-a435-4d01945fe21d Communist Part of China threat-actor-b5d1d28c-d824-49c0-80b6-9179202e297b GSD 3rd Department threat-actor-94624865-2709-443f-9b4c-2891985fd69b GSD 3rd Department / 2nd Bureau threat-actor-8dff0344-0c82-4079-8d04-6f3e4d9bd1df People's Liberation Army threat-actor-5ac0fd8e-5804-4849-a170-4ec0d15a5e8b PLA General Staff threat-actor-d9619c21-9d4f-414e-9471-36bb8fc42bbe
Title:	
Description:	
Confidence:	

MANTIS

Authoring Indicator Information



STIX Package

Campaign Info

Indicator Pool

IOC

Observable Pool

Observable Relations

Indicator Configuration

cert_my_organization:Indicator-4775a6c3-58cf-3dee-91f1-349568260f0f

Indicator producer:

Indicator title:

Indicator description:

Indicator confidence:

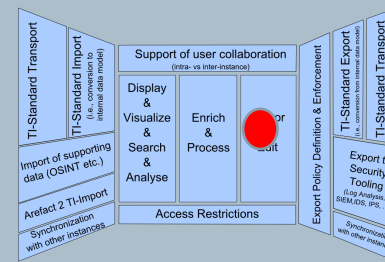
Robin H00d's RAT

The RAT used by Robin H00d is disguised as file "

High ▼

MANTIS

Authoring File Object via Drag & Drop



STIX Package Campaign Info Indicator Pool IOC Observable Pool **Observable Relations**

Pool Toggle All

File
super_cool_game.exe (58880 Bytes)

Observable Title

Observable Description

File name:

File path:

File size:

Md5:

Sha1:

Sha256:

File Dropzone

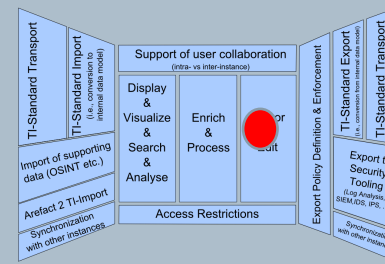
Observable Template

- Address
- Artifact
- DNS Record
- Email Message (De)
- File
- HTTP Session
- Port
- Gene
- Service

super_cool_game.exe

MANTIS

Authoring Generic URI Object



STIX Package Campaign Info Indicator Pool IOC Observable Pool **Observable Relations**

Pool Toggle All

Generic URI
super.evil.com (4 facts) 🗑️ 🔍

Domain contacted by Robin H00d's RAT.

Observable Description

Type : Domain Name ▾

Value: super.evil.com

File
super_cool_game.exe (58880 Bytes) 🗑️ 🔍

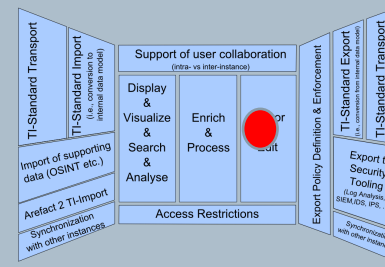
File Dropzone

Observable Templates

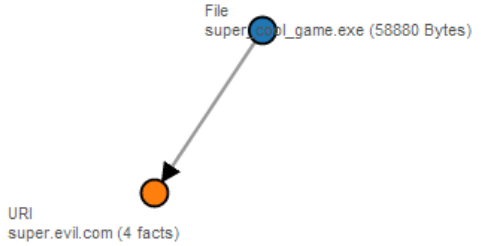
- Address 🗑️ 🔍
- Artifact 🗑️ 🔍
- DNS Record 🗑️ 🔍
- Email Message (Default) 🗑️ 🔍
- File 🗑️ 🔍
- HTTP Session 🗑️ 🔍
- Port 🗑️ 🔍
- Generic URI 🗑️ 🔍
- Windows Service 🗑️ 🔍

MANTIS

Authoring Object Relationships



- STIX Package
- Campaign Info
- Indicator Pool
- IOC
- Observable Pool
- Observable Relations

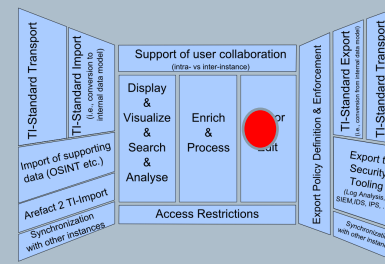


Relation Type

- Characterizes**
Specifies that this object describes the properties of the related object. This is most applicable in cases where the related object is an Artifact Object and this object is a non-Artifact Object.
- Closed**
Specifies that this object closed the related object.
- Connected_To**
Specifies that this object connected to the related object.
- Contains**
Specifies that this object contains the related object.
- Copied**
Specifies that this object copied the related object.
- Created**
Specifies that this object created the related object.
- Deleted**
Specifies that this object deleted the related object.
- Downloaded**
Specifies that this object downloaded the related object.
- Downloaded_From**
Specifies that this object was downloaded from the related object.
- Dropped**
Specifies that this object dropped the related object.
- Extracted_From**
Specifies that this object was extracted from the related object.
- FQDN_Of**
Specifies that this object is an FQDN of the related object.
- Installed**
Specifies that this object installed the related object.
- Installed**
Specifies that this object installed the related object.
- Moved**
Specifies that this object moved the related object.
- Opened**
Specifies that this object opened the related object.
- Read_From**

MANTIS

Putting together the STIX Package



STIX Package | Campaign Info | Indicator Pool | IOC | Observable Pool | Observable Relations

Package Contents

Robin Hood's RAT

- super_cool_game.exe (58880 Bytes)
- Generic URI
super.evill.com (4 facts)

Drop here to create new indicator

Package Meta

Test STIX Package

This is a test of Mantis Authoring

White

Save Draft | Save & Release | Import to MANTIS

Load Draft

Show JSON | Show STIX

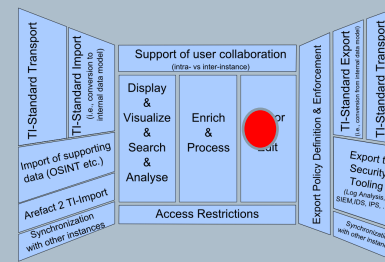
Observables

- File
super_cool_game.exe (58880 Bytes)
- Generic URI
super.evill.com (4 facts)

Test Mechanisms

MANTIS

Viewing the resulting XML

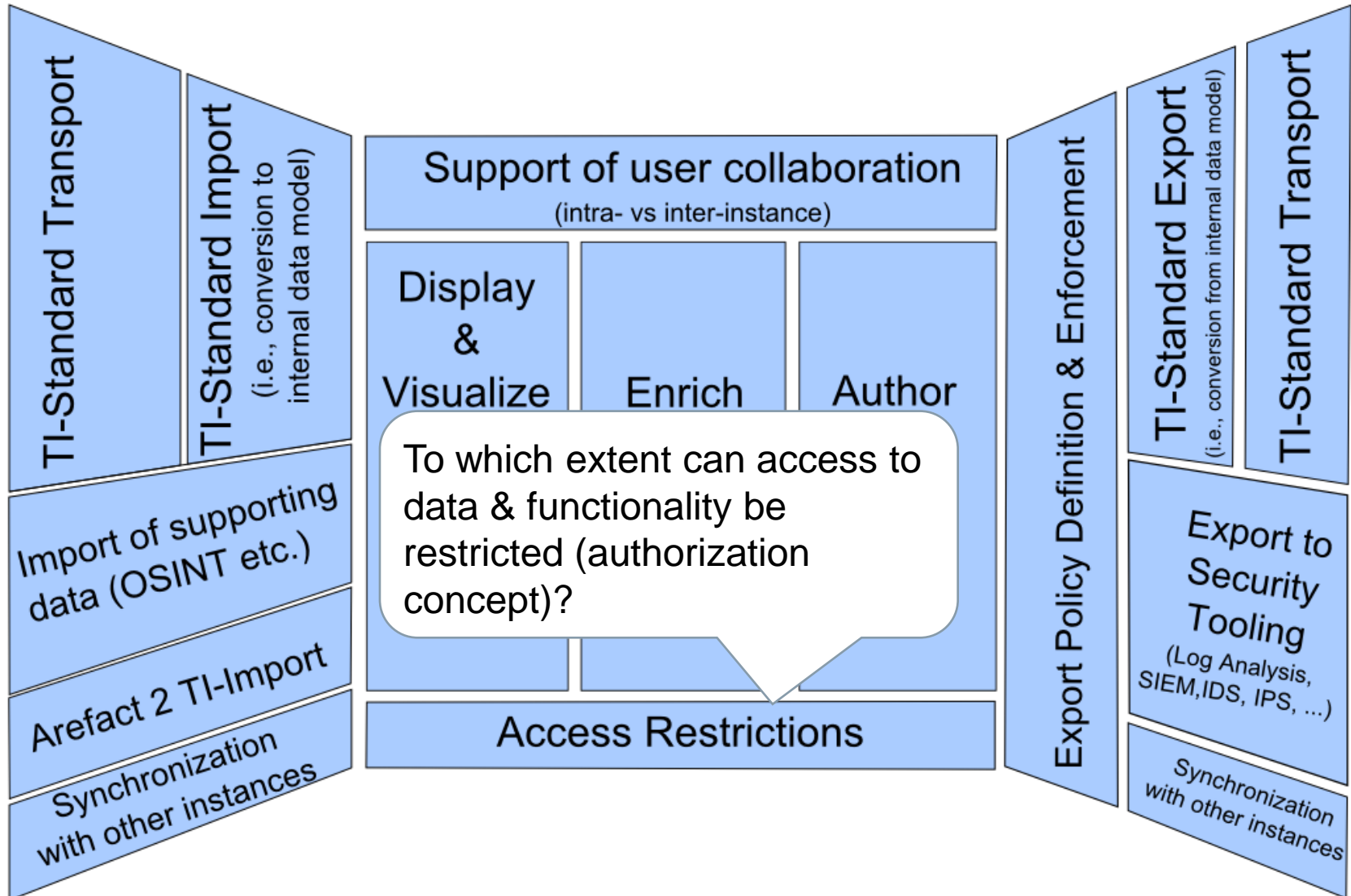


SIEMENS

STIX Package Output

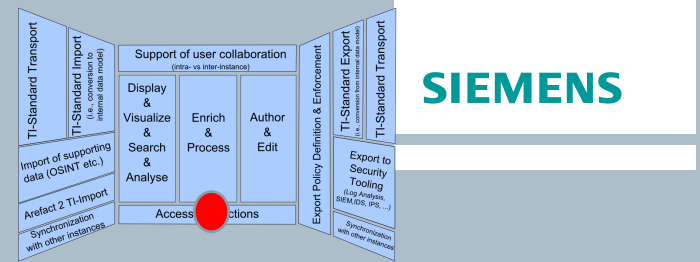
```
11 xmlns:incident="http://stix.mitre.org/incident-1"
12 xmlns:indicator="http://stix.mitre.org/Indicator-2"
13 xmlns:ta="http://stix.mitre.org/ThreatActor-1"
14 xmlns:stixCommon="http://stix.mitre.org/common-1"
15 xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
16 xmlns:stix="http://stix.mitre.org/stix-1"
17 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
18 xsi:schemaLocation="
19 http://cybox.mitre.org/common-2 http://cybox.mitre.org/XMLSchema/common/2.1/cybox_common.xsd
20 http://cybox.mitre.org/cybox-2 http://cybox.mitre.org/XMLSchema/core/2.1/cybox_core.xsd
21 http://cybox.mitre.org/default_vocabularies-2 http://cybox.mitre.org/XMLSchema/default_vocabularies/2.1/cybox_default_vocabularies.xsd
22 http://cybox.mitre.org/objects#FileObject-2 http://cybox.mitre.org/XMLSchema/objects/File/2.1/File_Object.xsd
23 http://cybox.mitre.org/objects#URIObject-2 http://cybox.mitre.org/XMLSchema/objects/URI/2.1/URI_Object.xsd
24 http://data-marking.mitre.org/Marking-1 http://stix.mitre.org/XMLSchema/data_marking/1.1.1/data_marking.xsd
25 http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1 http://stix.mitre.org/XMLSchema/extensions/marking/tlp/1.1.1/tlp_marking.xsd
26 http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.1.1/campaign.xsd
27 http://stix.mitre.org/Incident-1 http://stix.mitre.org/XMLSchema/incident/1.1.1/incident.xsd
28 http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.1.1/indicator.xsd
29 http://stix.mitre.org/ThreatActor-1 http://stix.mitre.org/XMLSchema/threat_actor/1.1.1/threat_actor.xsd
30 http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
31 http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/default_vocabularies/1.1.1/stix_default_vocabularies.xsd
32 http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.1.1/stix_core.xsd" id="cert_my_organization:package-cf116b10-3acc-f926-01ca-f902e8414d0e" version="1.1.1" timestamp="2014-06-18T22:39:31.945781+02:00"
33 <stix:STIX_Header>
34 <stix:Title>Test STIX Package</stix:Title>
35 <stix:Description>This is a test of Mantis Authoring</stix:Description>
36 <stix:Handling>
37 <stix:Marking:Marking>
38 <stix:Marking:Controlled_Structure>
39 </stix:Marking:Marking>
40 </stix:Handling>
41 <stix:Information_Source>
42 <stixCommon:Time>
43 <cyboxCommon:Produced_Time>2014-06-18T22:39:31.945781+02:00</cyboxCommon:Produced_Time>
44 </stixCommon:Time>
45 <stixCommon:Tools>
46 <cyboxCommon:Tool>
47 <cyboxCommon:Name>Mantis Authoring GUI</cyboxCommon:Name>
48 <cyboxCommon:Vendor>Siemens CERT</cyboxCommon:Vendor>
49 </cyboxCommon:Tool>
50 </stixCommon:Tools>
51 </stix:Information_Source>
52 </stix:STIX_Header>
53 <stix:Observables cybox_major_version="2" cybox_minor_version="1" cybox_update_version="0">
54 <cybox:Observable id="cert_my_organization:Observable-667ae0a8-d43a-be9d-ffa9-f32e2db60fc4">
55 <cybox:Title></cybox:Title>
56 <cybox:Description/>
57 <cybox:Object id="cert_my_organization:File-c2281518-854d-4378-9c80-fe7fea8c6a0e">
58 <cybox:Properties xsi:type="FileObj:FileObjectType">
59 <FileObj:File_Name>super_cool_game.exe</FileObj:File_Name>
60 <FileObj:File_Extension>exe</FileObj:File_Extension>
61 <FileObj:Size_In_Bytes>58880</FileObj:Size_In_Bytes>
62 <FileObj:Hashes>
63 <cyboxCommon:Hash>
64 <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5</cyboxCommon:Type>
65 <cyboxCommon:Simple_Hash_Value condition="Equals">2c4ae5cf18d6688a75582a7d5d67bb48</cyboxCommon:Simple_Hash_Value>
66 </cyboxCommon:Hash>
```

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

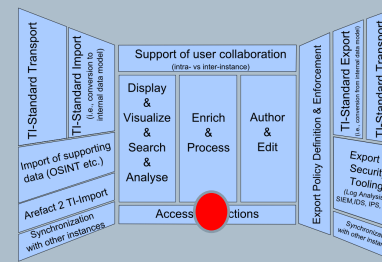
Authoring Groups restrict authoring & editing



- A user can be member of one or more groups (standard mechanism offered by Django)
- By associating a group with identifier namespace information, it becomes an *Authoring Group*
- Namespace information contains
 - **default namespace:** objects created via authoring interface are created in identifier namespace as specified by *default namespace*
 - **allowed namespace:** objects created by user e.g., via XML Import interface, may only carry identifiers with an allowed identifier namespace
- A user can only access the author interface for reports created within an authoring group of which he is a member

MANTIS

Authoring Groups restrict authoring & editing



SIEMENS

Authoring Group: CERT Team

Default Namespace

cert.my-organization.com

Allowed Namespaces

cert.my-organization.com

Name: Import of XML via GUI

Name is displayed in list of imported XML; the name is not used in the import.

Xml:

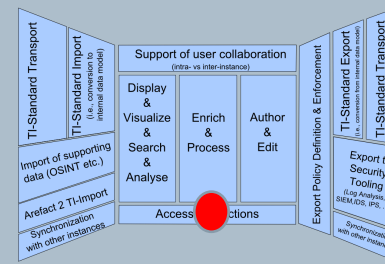
```
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObj-1"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation=
    "http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 ../cybox/objects/Domain_Name_Object.xsd"
  id="example:STIXPackage-f61cd874-494d-4194-a3e6-6b487dbb6d6e"
  timestamp="2014-05-08T09:00:00.000000Z"
  version="1.1.1"
>
<stix:STIX_Header>
  <stix:Title>Example watchlist that contains domain information.</stix:Title>
  <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-
```

ATTENTION: Make sure that the identifier namespaces occurring in the XML are contained in your allowed namespaces (see display on right-hand side)!!! Otherwise, the created objects will be moved into a temporary namespace!!!

Import

MANTIS

Authoring Groups restrict authoring & editing



MANTIS Cyber Threat Info Management [List, Filter & Search](#) [Saved Filters/Searches](#) **Doe, John**

[Edit user config](#)

[Edit saved searches](#)

[Switch Authoring Group](#)

[Log out](#)

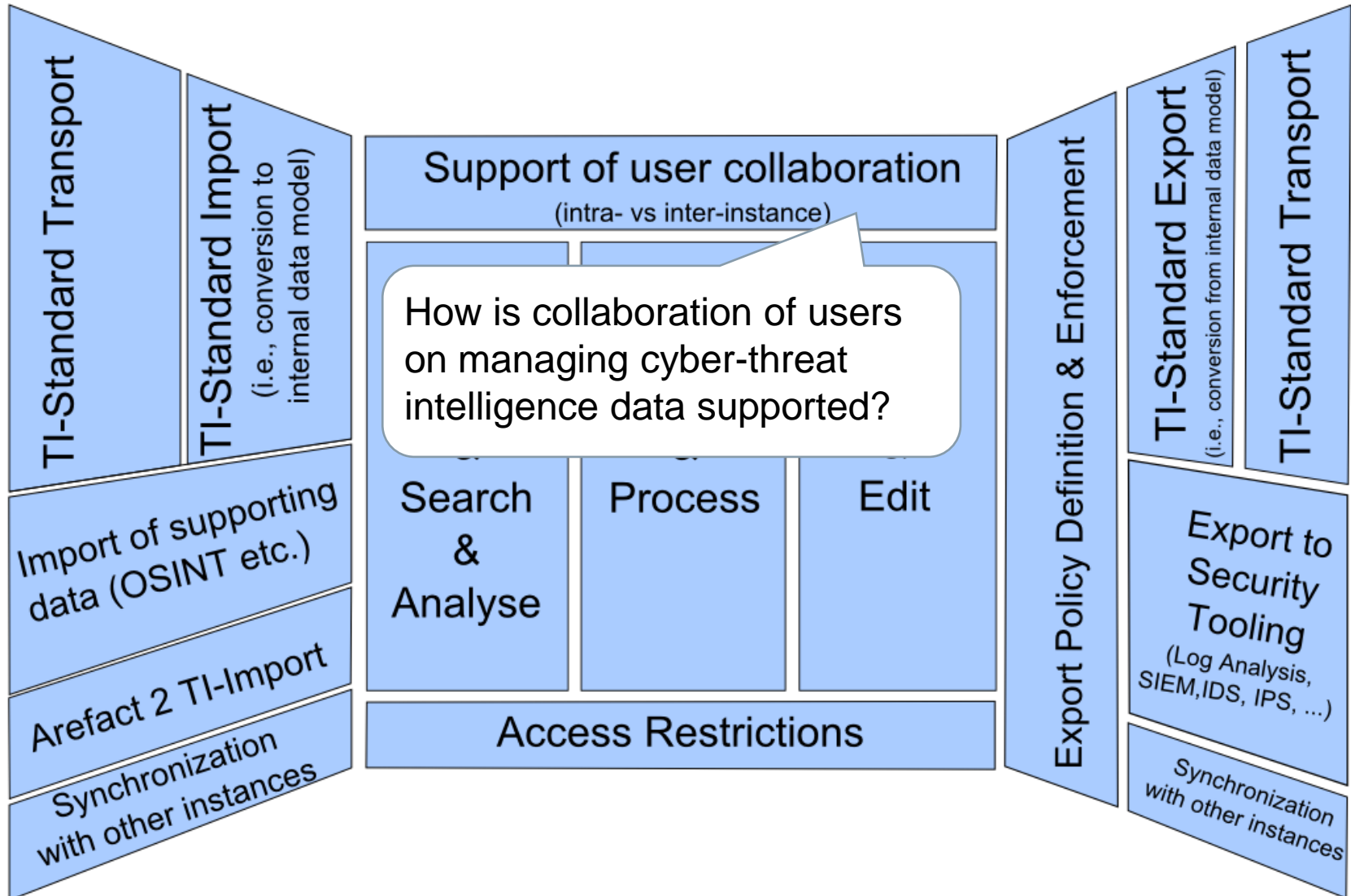
Switch Authoring Group

Chose active authoring group:

Authoring Group: None

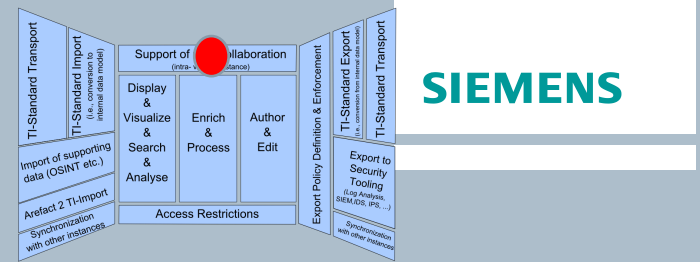
Please select an authoring group!

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

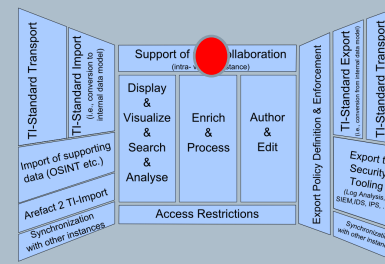
Users can cooperate on reports within authoring groups



- A user can access via the authoring interface authored within his authoring group(s)
- Reports may have an owner: as long as an owner holds the report, no other user may edit the report
- A report can be released by its owner; importing the report into MANTIS releases the report automatically
- Users can take ownership of a report currently owned by another user (to be used with care!)

MANTIS

Viewing, editing and taking reports within own authoring group



Drafts and Imports of Authoring Group CERT Team

Saved Drafts						
	Owner	Name	Status	Timestamp		
<input checked="" type="checkbox"/>	Erika Mustermann	Erika's First Report	Update (not yet imported)	June 18, 2014, 11:07 p.m.	View History	
<input type="checkbox"/>		Test STIX Package	Imported	June 18, 2014, 11:07 p.m.	View History	EDIT

Filter Parameters

Import Timestamp:

Name contains:

Status:

User:

[Submit Query](#) [Save Search](#)

Authoring Group: CERT Team

Default Namespace

cert.my-organization.com

Allowed Namespaces

cert.my-organization.com

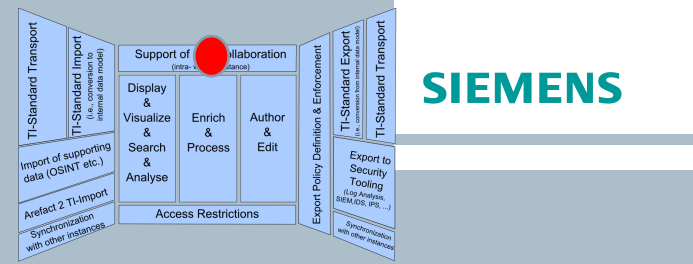
Take from owner

Take from owner ▾ 1 of 2 selected

[Submit](#)

MANTIS

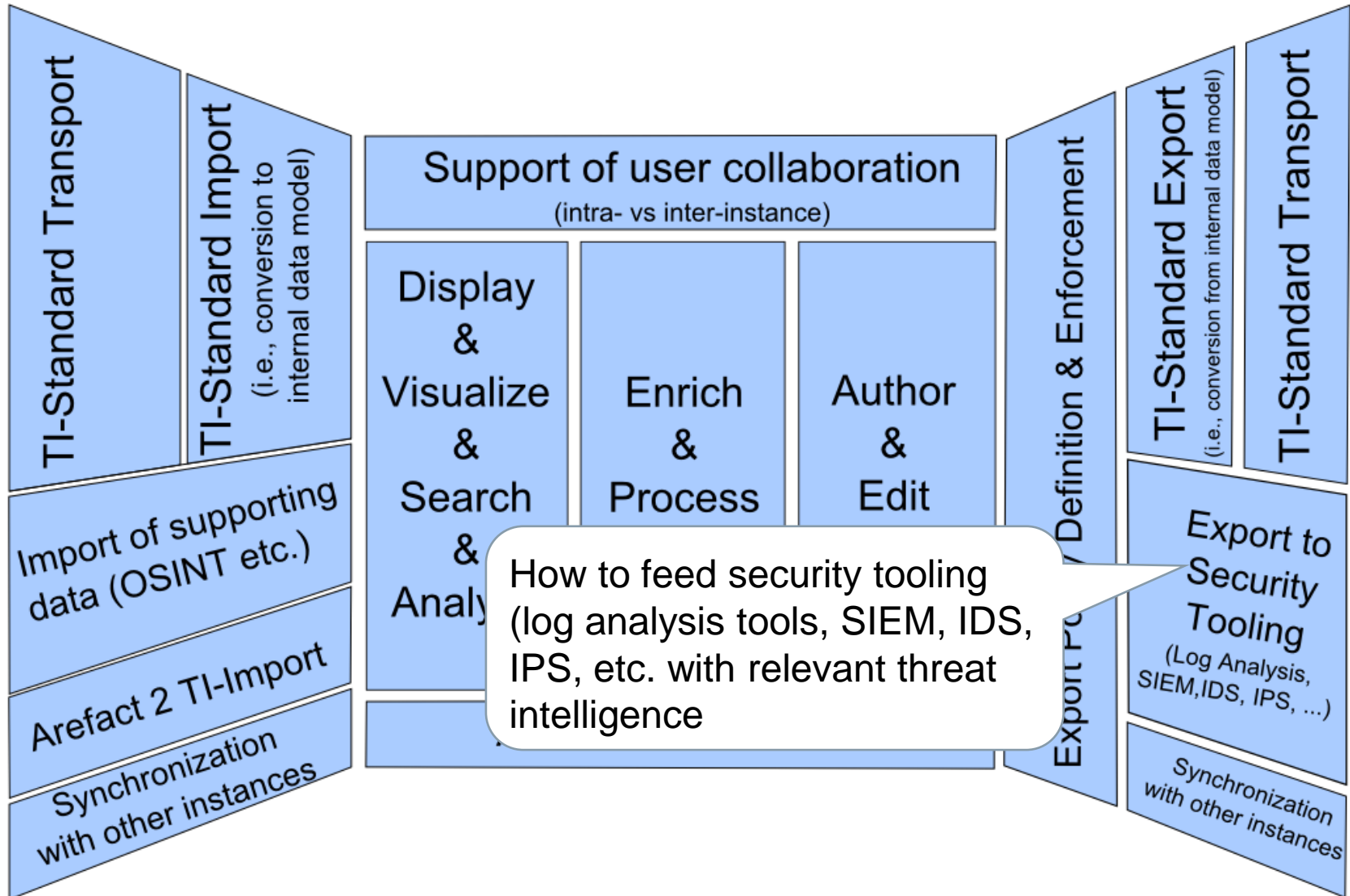
Viewing the history of a report



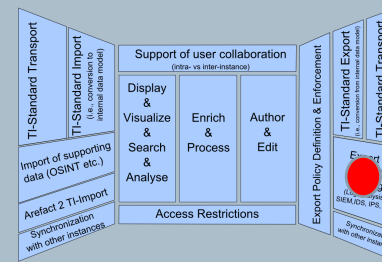
History of 'Test STIX Package'

Owner	Status	Kind	Timestamp	
	Imported	JSON (Dingos Authoring)	June 18, 2014, 10:55 p.m.	EDIT
John Doe	Imported	XML	June 18, 2014, 10:55 p.m.	
John Doe	Draft	JSON (Dingos Authoring)	June 18, 2014, 10:55 p.m.	
John Doe	Draft	JSON (Dingos Authoring)	June 18, 2014, 10:43 p.m.	
John Doe	Draft	JSON (Dingos Authoring)	June 18, 2014, 10:42 p.m.	

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



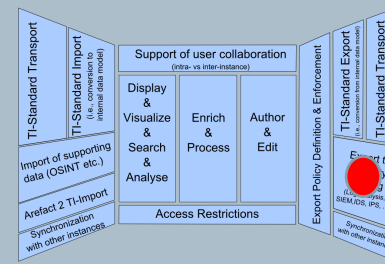
Feeding security tools with threat intelligence via saved searches



- Custom searches
 - can be saved
 - can return results as CSV, simple JSON, etc.
- Concept for feeding security tools with simple indicator lists:
 - Generate a saved search that pulls relevant data out of the system
 - Allow tools access to saved searches via REST interface

MANTIS

Providing search results as csv



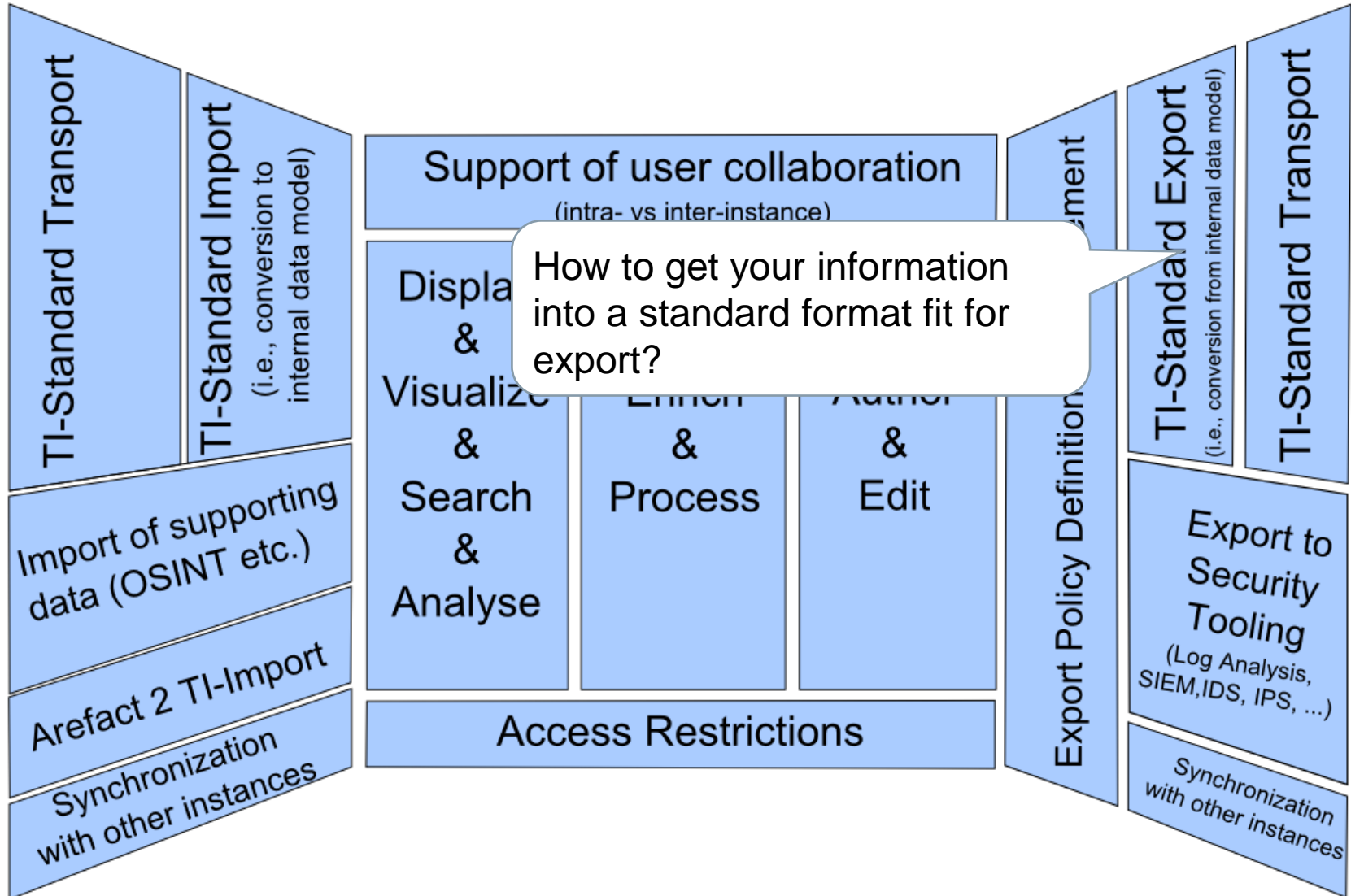
Filter Parameters

```
fact: [Properties/Value] regexp "business"  
| object: identifier.namespace contains 'mandiant.com' && object_type.name contains  
'URIObject'  
| marked_by: (fact: [Marking_Structure/Statement] contains 'APT1')  
[F> csv('Object Type:object.object_type.name','Fact  
Term:fact_term_with_attribute','Value:value')]
```

Paginate by

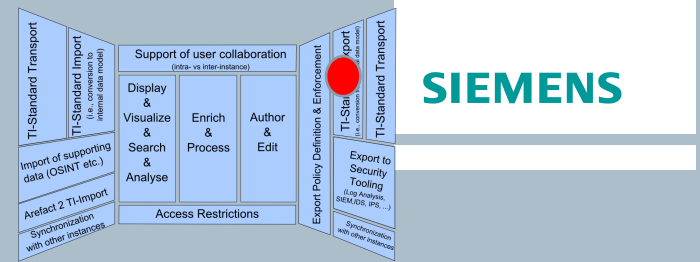
```
IO-Type, Fact Term, Value  
cybox.mitre.org:URIObject, Properties/Value, xmer.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, www-ctr.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, www-049.businessformars.com  
cybox.mitre.org:URIObject, Properties/Value, www.businessformars.com  
cybox.mitre.org:URIObject, Properties/Value, www.advanbusiness.com  
cybox.mitre.org:URIObject, Properties/Value, wtom.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wrim.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wpm.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wptex.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wpot.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wpcs.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, world.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wopm.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wopec.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, woil.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wnew.businessconsults.net  
cybox.mitre.org:URIObject, Properties/Value, wned.businessconsults.net
```

(Cyber)Threat Intelligence Tooling: A reference frame regarding functionality



MANTIS

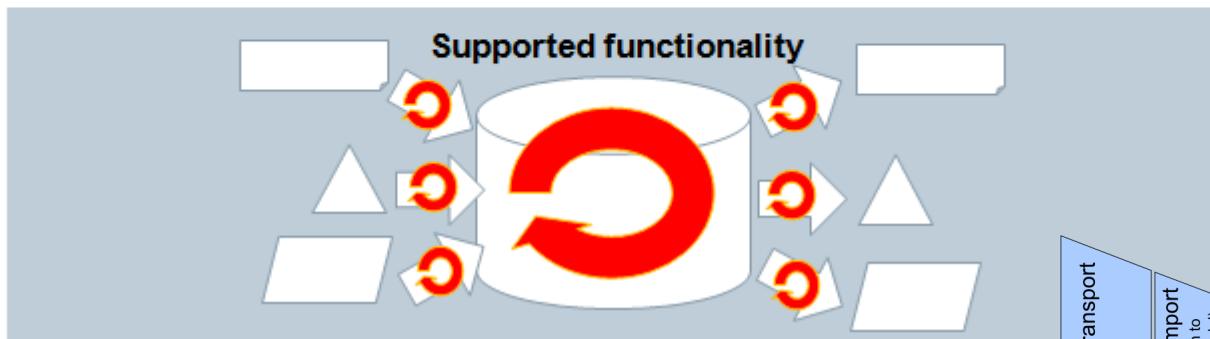
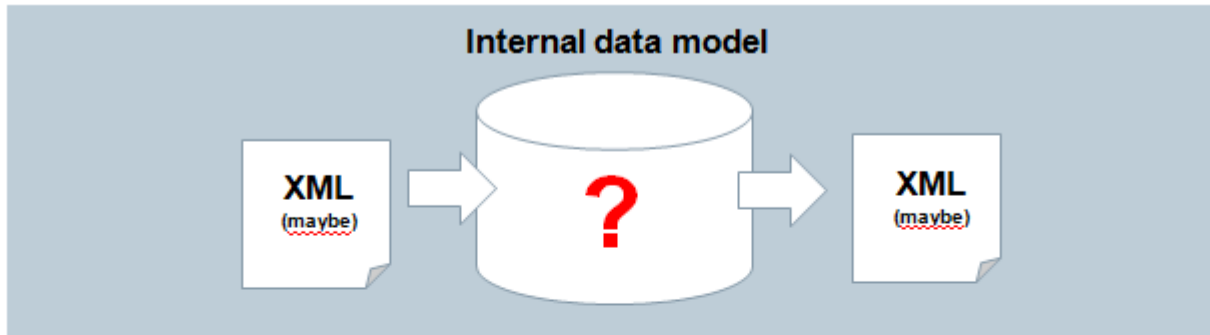
Towards exporting data



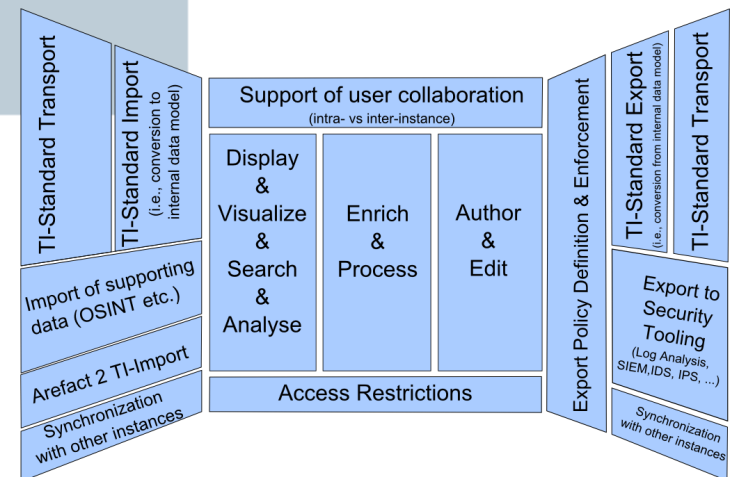
- As discussed above when talking about the flexible data model: flexible import makes export challenging
 - Possible concepts:
 - always export to a given revision of the standard; for data imported in older revisions, some data may be lost or misrepresented
 - always export to the revision that was imported (but for this we would need to have STIX/CybOX python bindings in different revisions in parallel
 - ...?
 - **But:** for our main use case of exporting self-authored data, we are all set for always exporting to the latest revision:
 - Upgrade transformers to new revision
 - Regenerate STIX/CybOX for all reports

Take away #1

Distinguishing features of Threat Intelligence Management Systems



- **Genesis?**
- **Distance?**
- **Flexibility?**



Caveat: What MANTIS is and isn't

- MANTIS **is** an *alpha/early beta implementation* of a framework for managing cyber threat intelligence expressed in standards such as STIX, CybOX, OpenIOC, IODEF, etc.
- Our aims of providing MANTIS as open source are:
 - To aide discussions about tooling for emerging standards such as STIX, CybOX et al.
 - To lower the entrance barrier for organizations and teams (esp. CERT teams) in using emerging standards for cyber-threat intelligence management and exchange.
 - To provide a platform on the basis of which research and community-driven development in the area of cyber-threat intelligence management can occur.
- MANTIS **isn't** a finished tool or project: we like to think that it provides a solid basis on which cyber-threat intelligence management can be built up upon, but if you expect something that out of the box covers all aspects of cyber-threat intelligence management or are unable/unwilling to dive into Django and Python code and fix/modify according to your requirements, MANTIS isn't for you. This may change sometime in the future when Mantis reaches version 1.0.0 ... but currently, we are at 0.3.0...
- MANTIS (currently) **isn't** a tool fit for importing *huge* datasets or huge numbers of datasets. This situation may change at some point of time with more stream-lined importers, but MANTIS is really not intended to deal with very big data the way log management solutions are.

Where to get MANTIS?

Access to the Mantis source code for installation:

- Either via git clone from the Mantis Github Repository (<https://github.com/siemens/django-mantis.git>) (recommended):
`git clone https://github.com/siemens/django-mantis.git`
- Or via download as zip package from <https://github.com/siemens/django-mantis/archive/master.zip>

There is a mailing list for dicussions, questions, etc.:

- Subscribe to the mailing list by sending a mail to Mantis-ti-discussion-join@lists.trusted-introducer.org.
- The archives of the mailing list are available via Nabble (<http://mantis-threat-intelligence-management-framework-discussion-list.57317.x6.nabble.com/>)

Many thanks to the TF-CSIRT Trusted Introducer for their support in hosting the list!

All issues regarding Mantis and its components are tracked on the Mantis Issue Tracker (<https://github.com/siemens/django-mantis/issues?state=open>)

Documentation: the full documentation is at <http://django-mantis.readthedocs.org>.