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

The MANTIS Framework
Cyber-Threat Intelligence Mgmt. for CERTs

Open Source solutions for Managing Cyber Threat Intelligence Fall 2012

Open Source solutions for
Managing Cyber Threat Intelligence
Fall 2012

CIF ticks quite a few boxes, but is very much geared towards automated processing of a restricted part of threat intelligence data. **Very** useful to have, but not general enough as a Cyber Threat Intelligence Management Solution.

collective-intelligence-framework

The Intelligence Layer

Open Source solutions for Managing Cyber Threat Intelligence Now

SIEMENS

CRITS

MISP

MANTIS

AVALANCHE

One person's incident is everyone's defense

(upcoming fall 2014)

{P} collective-intelligence-framework

The Intelligence Layer

Had we known in fall 2012 that MISP, CRITS or Avalanche would become available, would we still have started development of Mantis?

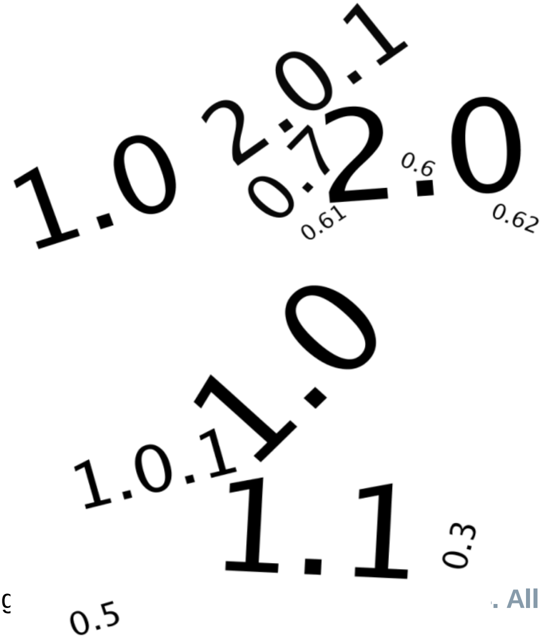
- Yes.
- Don’t get me wrong: from what I have seen of the mentioned tools: those are *really* great tools!!!
- But none of them fits quite our use-case:

  A central repository of all Cyber Threat Intelligence information created by ourselves or provided to us by partners with *maximum* tolerance for data formats and evolution of data formats, yet sensible structuring of information
- Let me explain …

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

Basic assumptions:

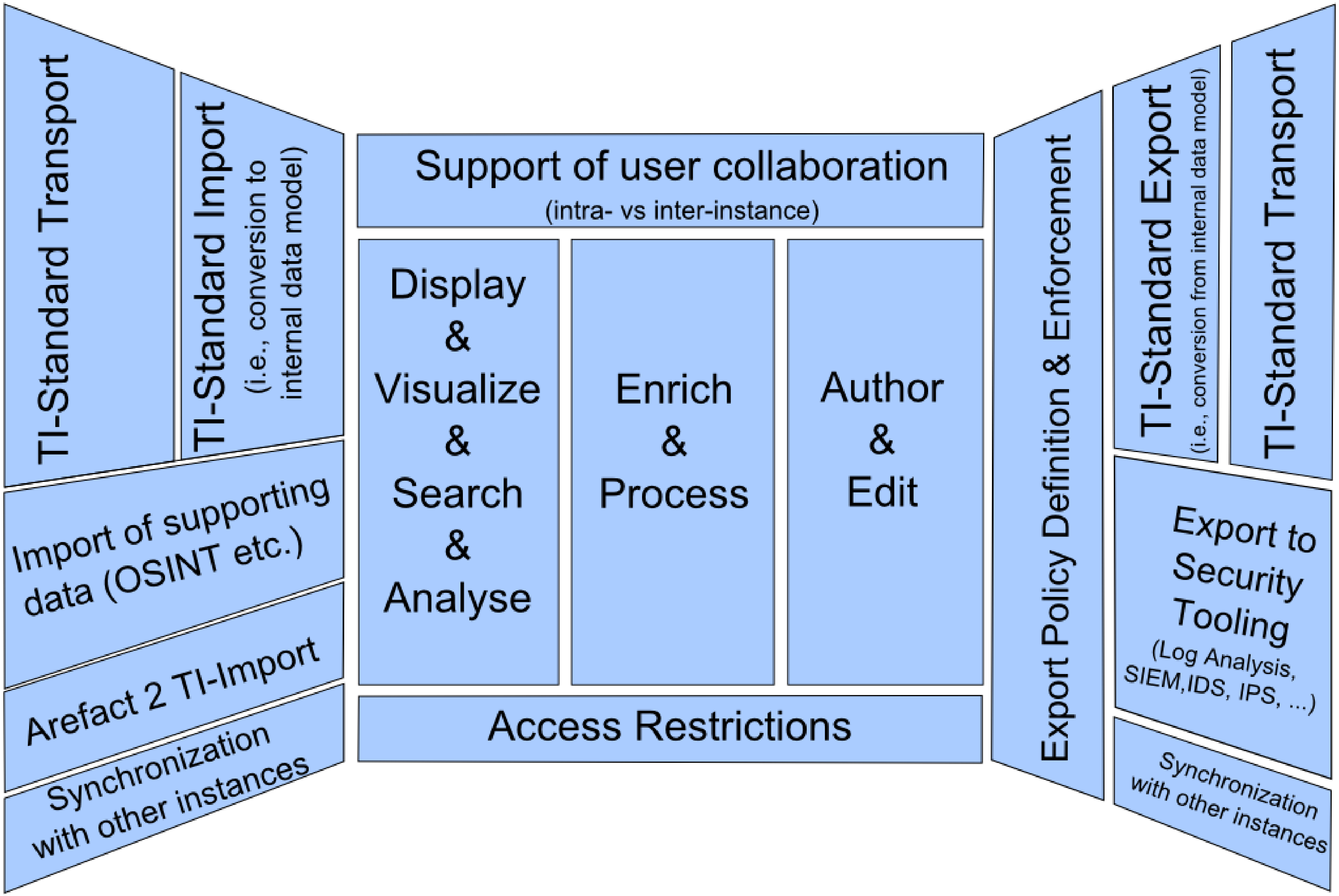
- At the moment, we cannot do without OpenIOC, so a STIX/CybOX-exclusive solution will not work
- I bet you that two years, after STIX 3.0 has been released, there will still be persons or tools that keep sending you STIX 1.0.1 …



The remainder of this talk

- Functionality of Cyber Threat Intelligence Management Solutions: an overview
- THE fundamental design decision when creating a Cyber Threat Intelligence Management Solution and its consequences
  (Hint: this has to do with tolerance for different formats and revisions)
- -> Thus, we arrive at the beginnings of a reference frame for talking about cyber threat intelligence management solutions
- Where does MANTIS sit in this frame?

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



TI-Standard Transport

TI-Standard Import (i.e., conversion to internal data model)

Import of supporting data (OSINT etc.)

Arefact 2 TI-Import

Synchronization with other instances

Support of user collaboration (intra- vs inter-instance)

Display & Visualize & Search & Analyse

Enrich & Process

Author & Edit

Access Restrictions

Export Policy Definition & Enforcement

TI-Standard Export (i.e., conversion from internal data model)

TI-Standard Transport

Export to Security Tooling (Log Analysis, SIEM,IDS, IPS, ...)

Synchronization with other instances

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

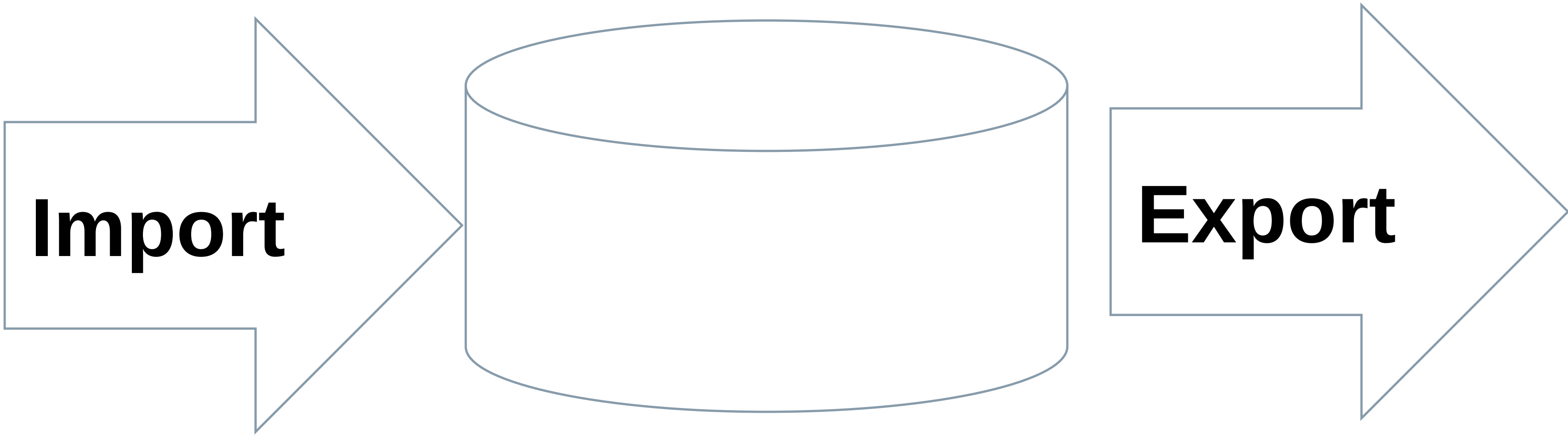
- What does your data model look like?
  - Home-brew
  - Somehow derived from a standard

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

- How flexible is your data model?
  - If the exchange standard allows very flexible usage: does your model, too, or have you narrowed things down?
  - can your model cope with moderate revision changes?

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

SIEMENS



Import

Export

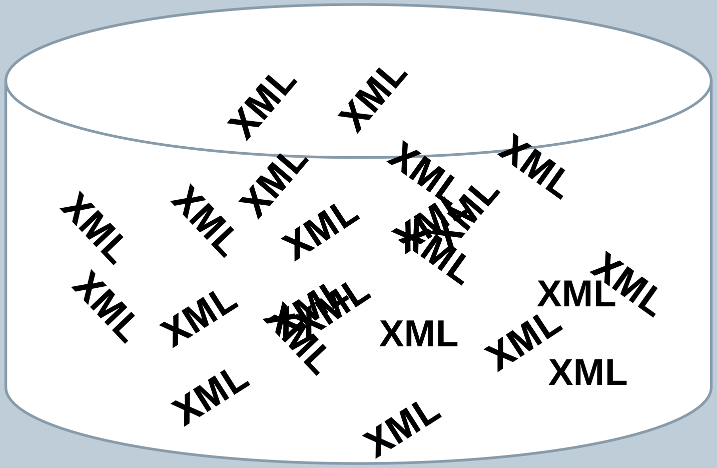
- The further removed your internal data model is, the more you have to work for import and export

- The real problem is the import: what to do with information that cannot be mapped into your internal data model?

Flexibility: two extremes

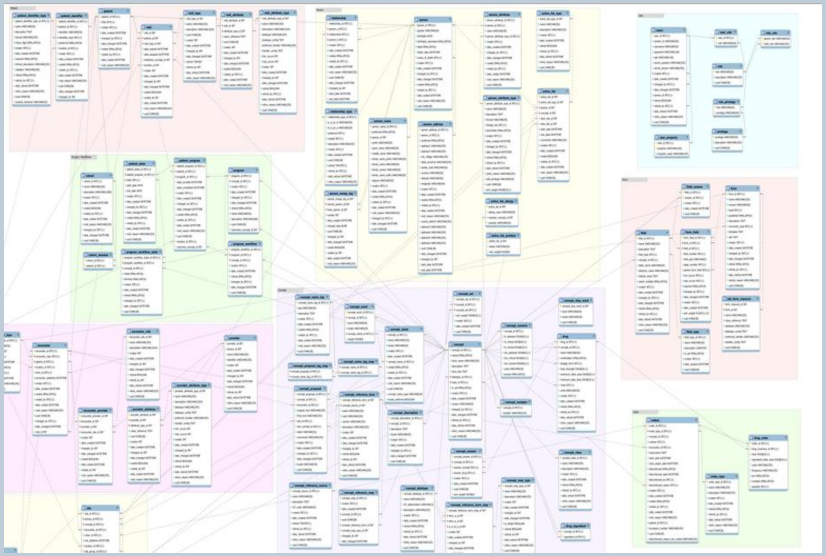
Extremely flexible

- Just dump each file into an XML database …

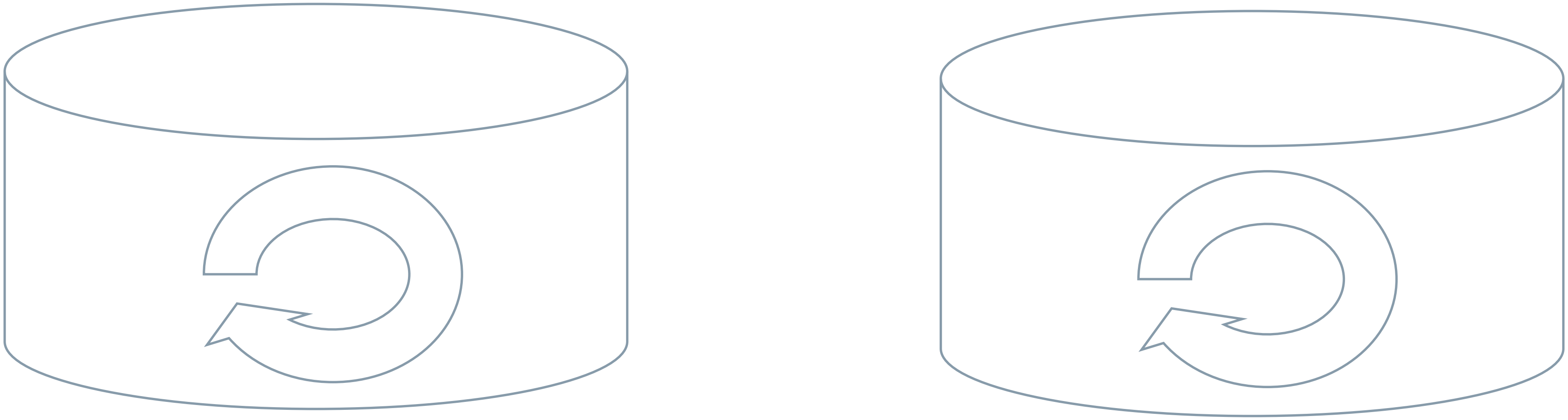


Rather inflexible

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



Implications of flexibility: Processing

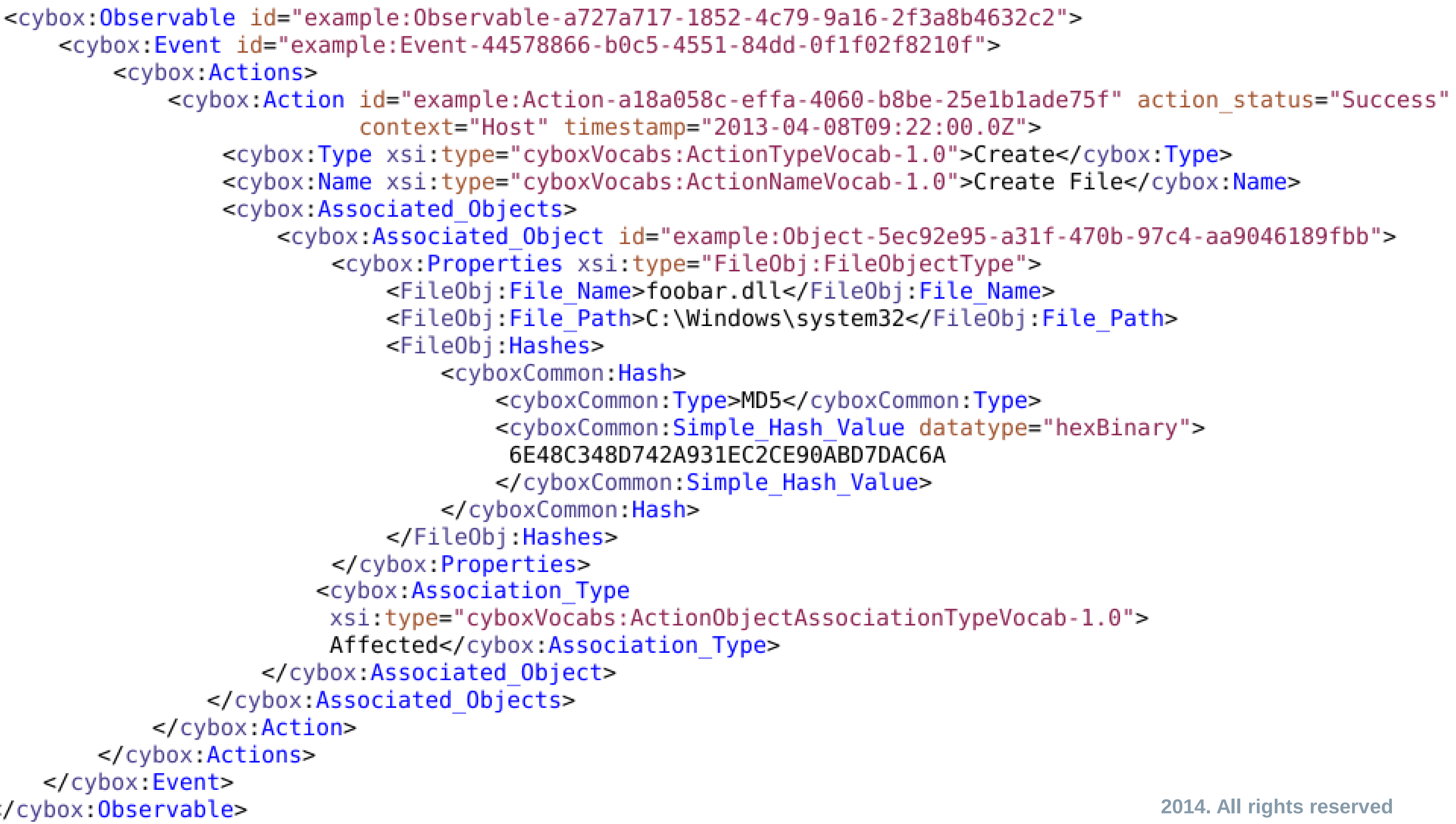


- Flexibility eases import, but makes processing more complicated, since you cannot assume that things always look the same
- A highly relevant problem when dealing with STIX and CybOX: the same thing can be expressed in a hundred different ways…

MANTIS‘s data model: pretty flexible, but a lot smarter than just dumping XMLs or JSONs

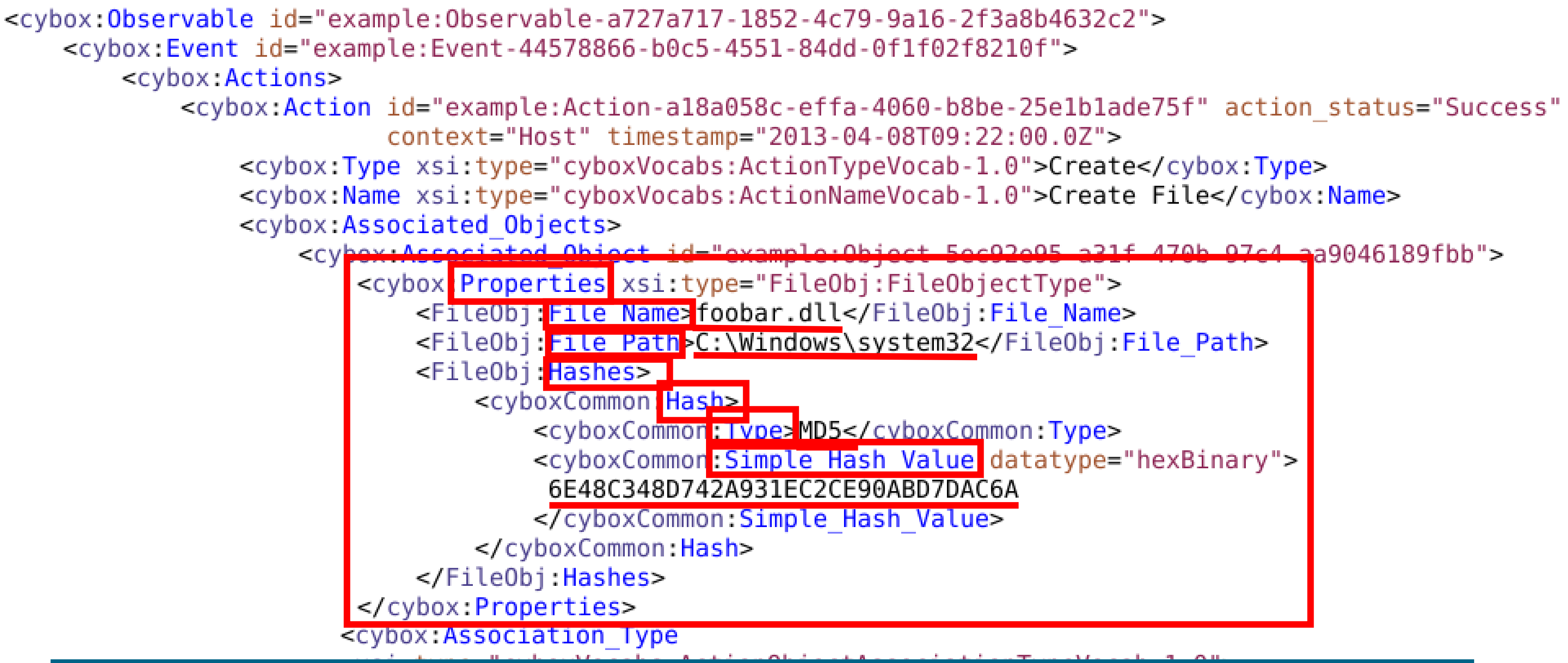
SIEMENS

Example: A CybOX 2.0 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-25e1b1ade75f" 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: A CybOX 2.0 Observable XML Source
Extracting „flat“ facts from hierarchical XML



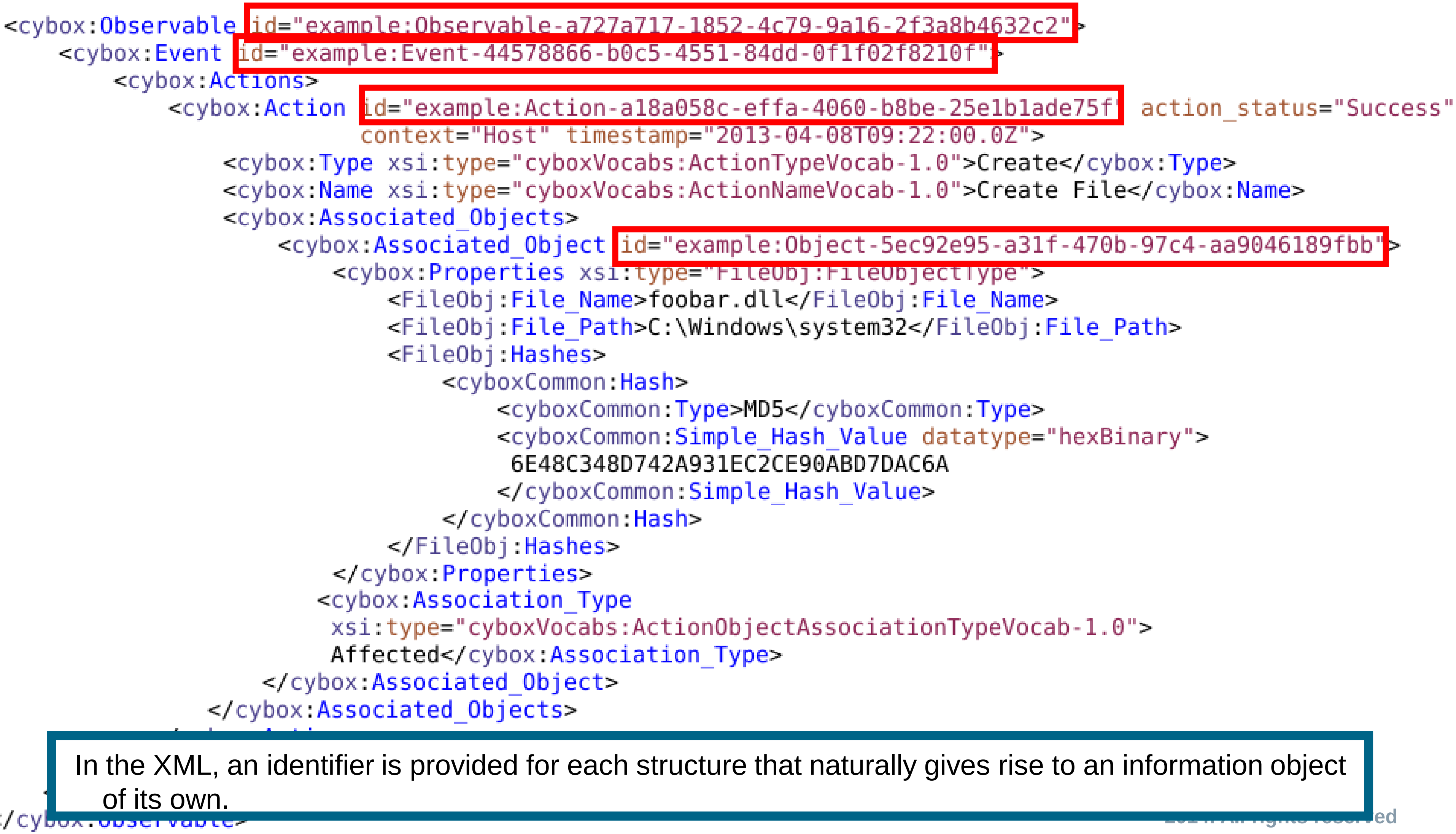
```
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
    <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
        <cybox:Actions>
            <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1b1ade75f" action_status="Success"
                          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
```

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 = 6E48C34(D742A931EC2CE90ABD7DAC6a*

```
</cybox:Observable>
```

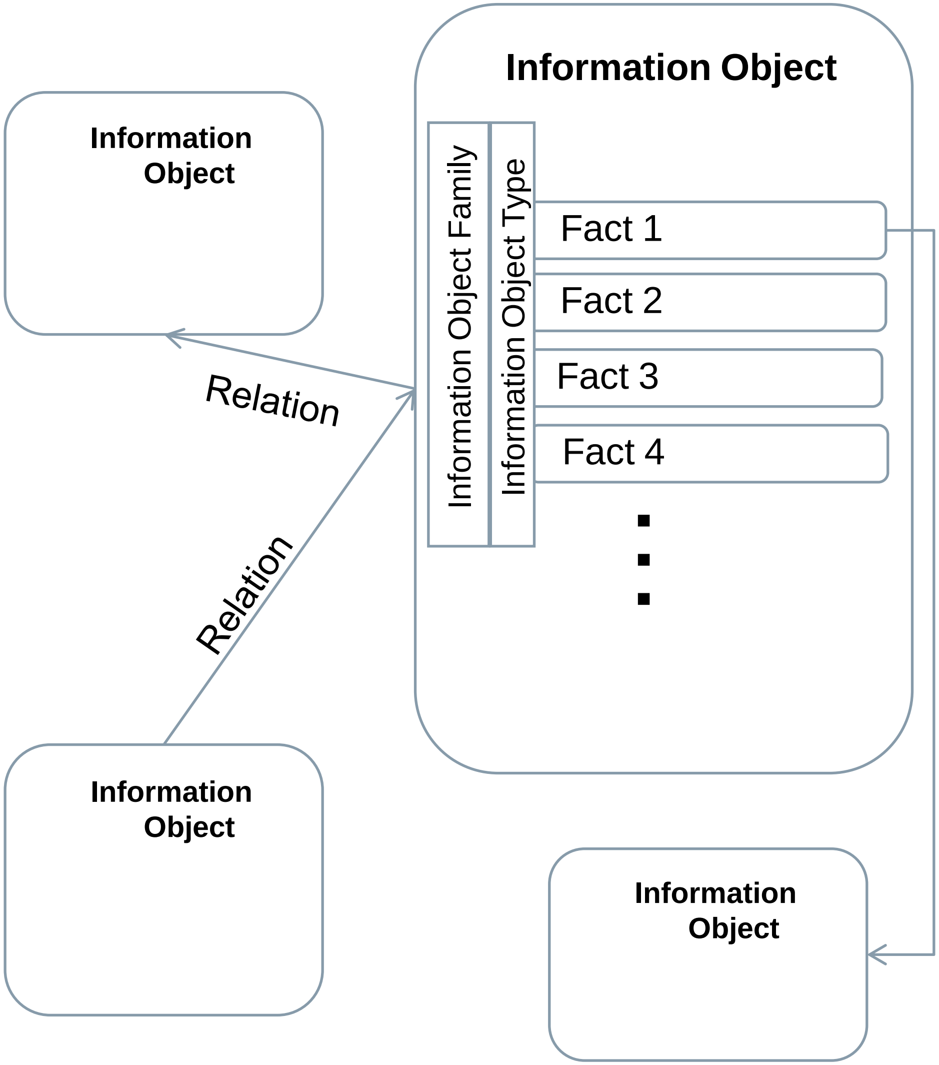
Example: A CybOX 2.0 Observable XML Source XML Defining object boundaries



```
<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-25e1b1ade75f" 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:Observable>
```

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

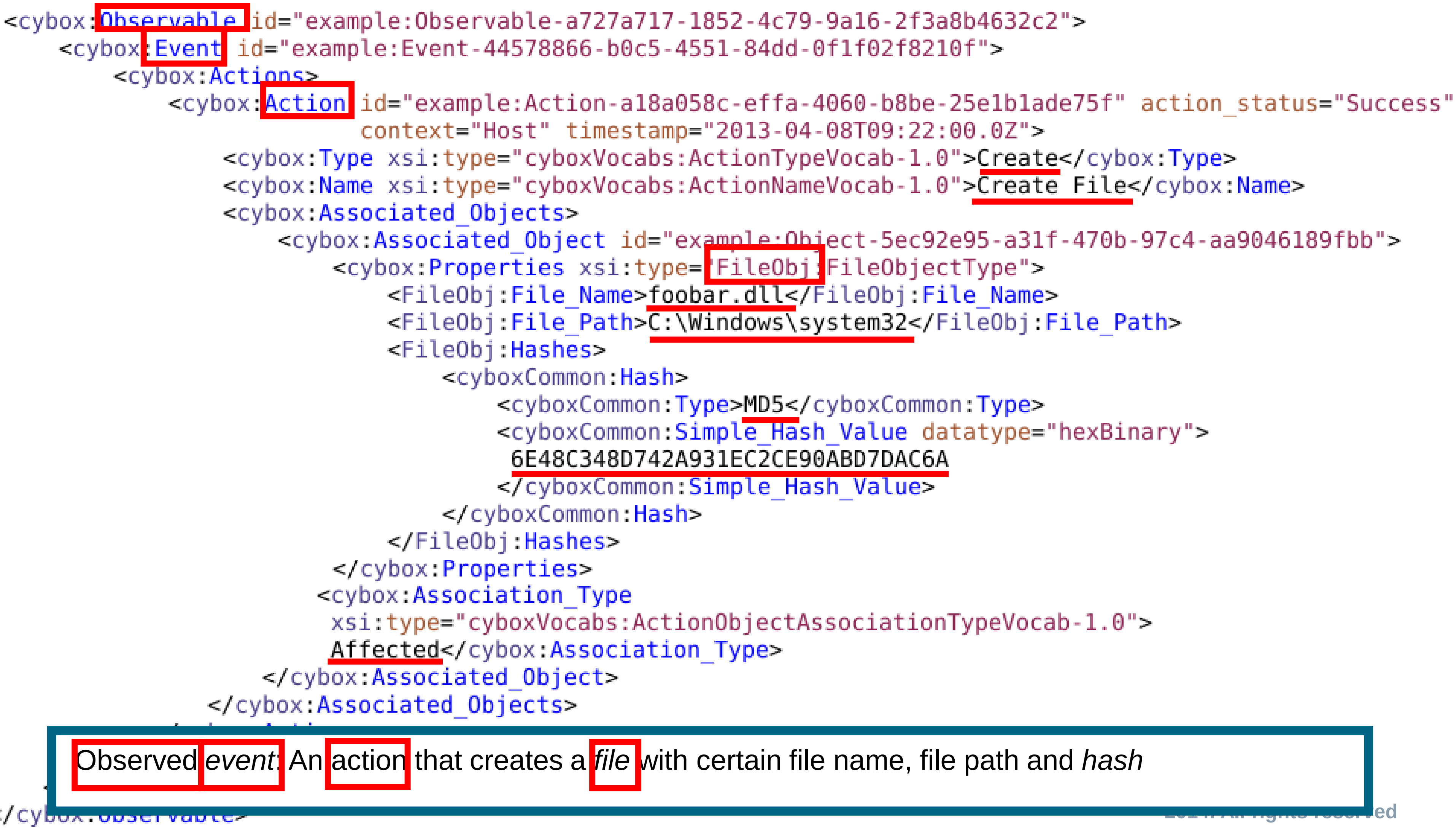
MANTIS-DINGOS
Fundamental Concepts



Information Objects

- *Information Objects*
  - *Information Objects* serve as top-level structure
  - Each *Information Object* has a *family* (e.g., “STIX” or “CybOX) and a type (e.g. “Indicator” or “FileObject”).
  - *Information Objects* contain *facts*
  - *Relations/Links between Information Objects*
    - An *information object* can be related to other information objects
    - A *fact* can reference an *information object*

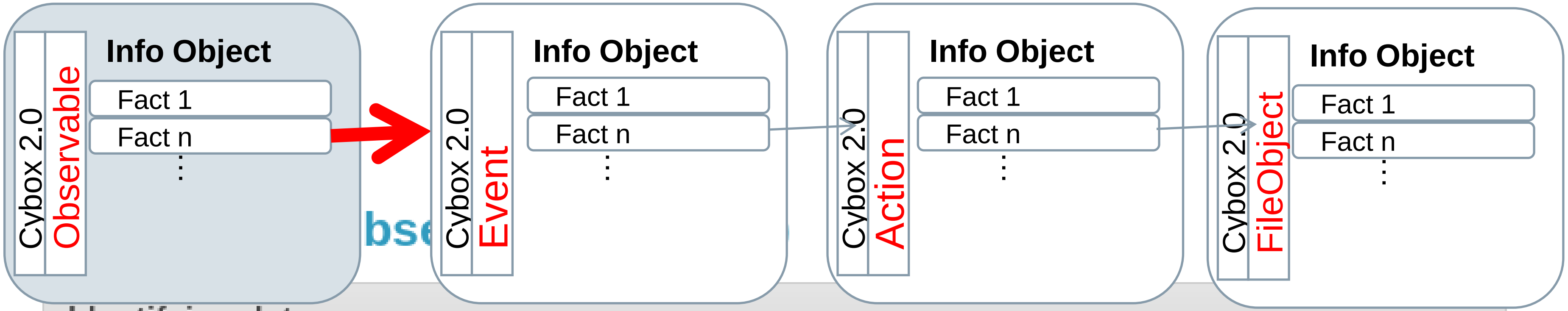
Example: Importing a CybOX 2.0 Observable XML Source: Focusing on objects and facts

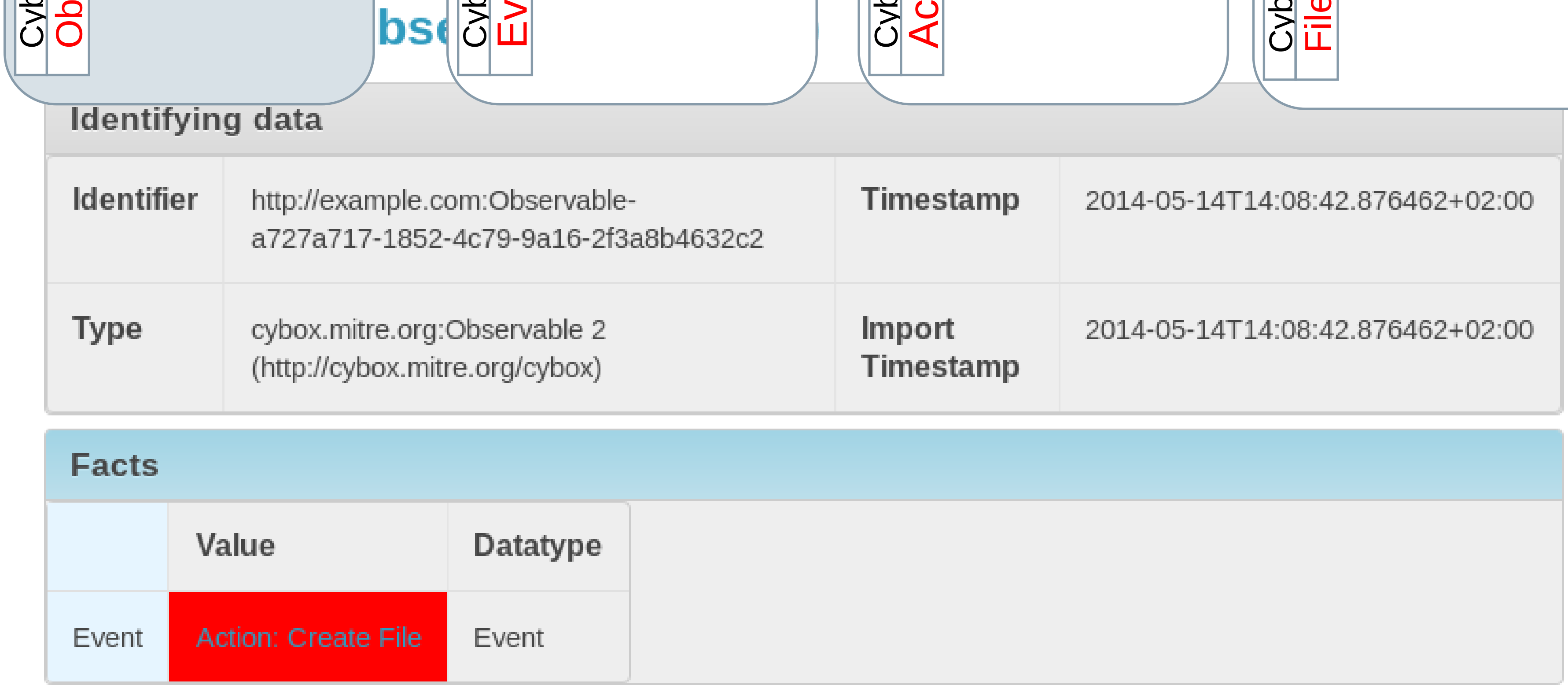


```
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
    <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
        <cybox:Actions>
            <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1b1ade75f" action_status="Success"
                          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:Observable>
```

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

Example: Importing a CybOX 2.0 Observable Resulting Structure





bse

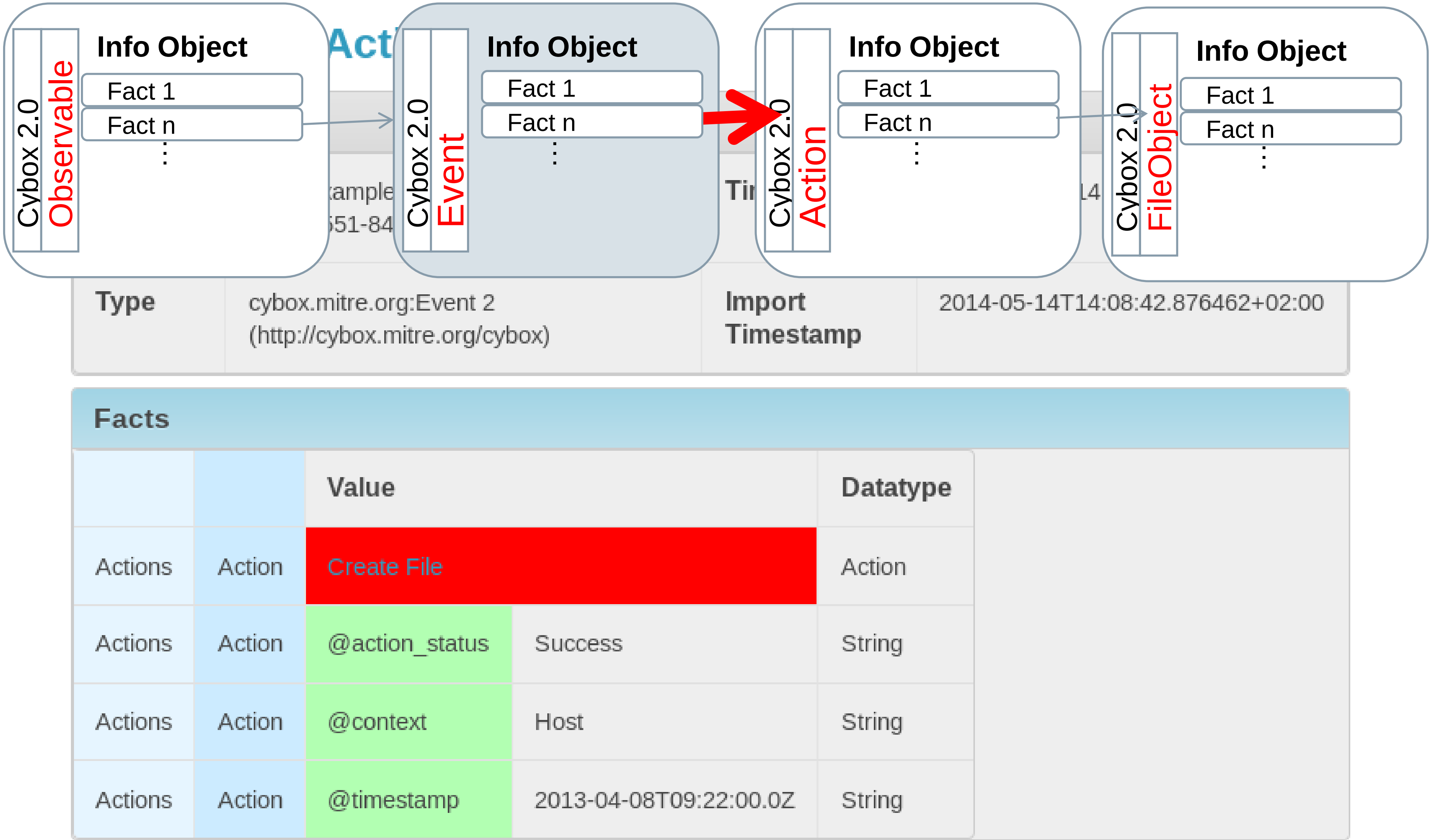
Identifying data

Identifier	http://example.com:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2	**Timestamp**	2014-05-14T14:08:42.876462+02:00
Type	cybox.mitre.org:Observable 2 (http://cybox.mitre.org/cybox)	**Import Timestamp**	2014-05-14T14:08:42.876462+02:00

Facts

	Value	Datatype
Event	Action: Create File	Event

Example: Importing a CybOX 2.0 Observable Resulting Structure

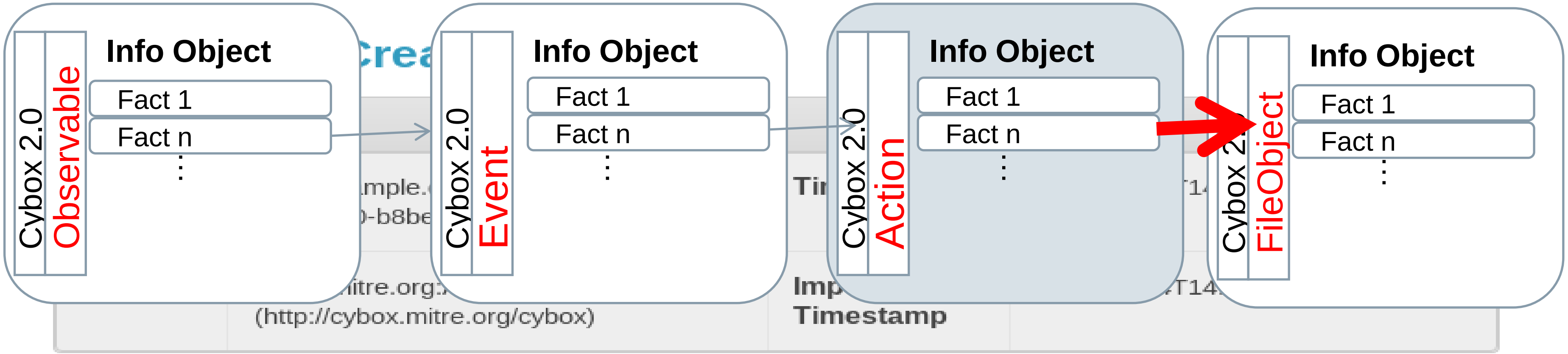


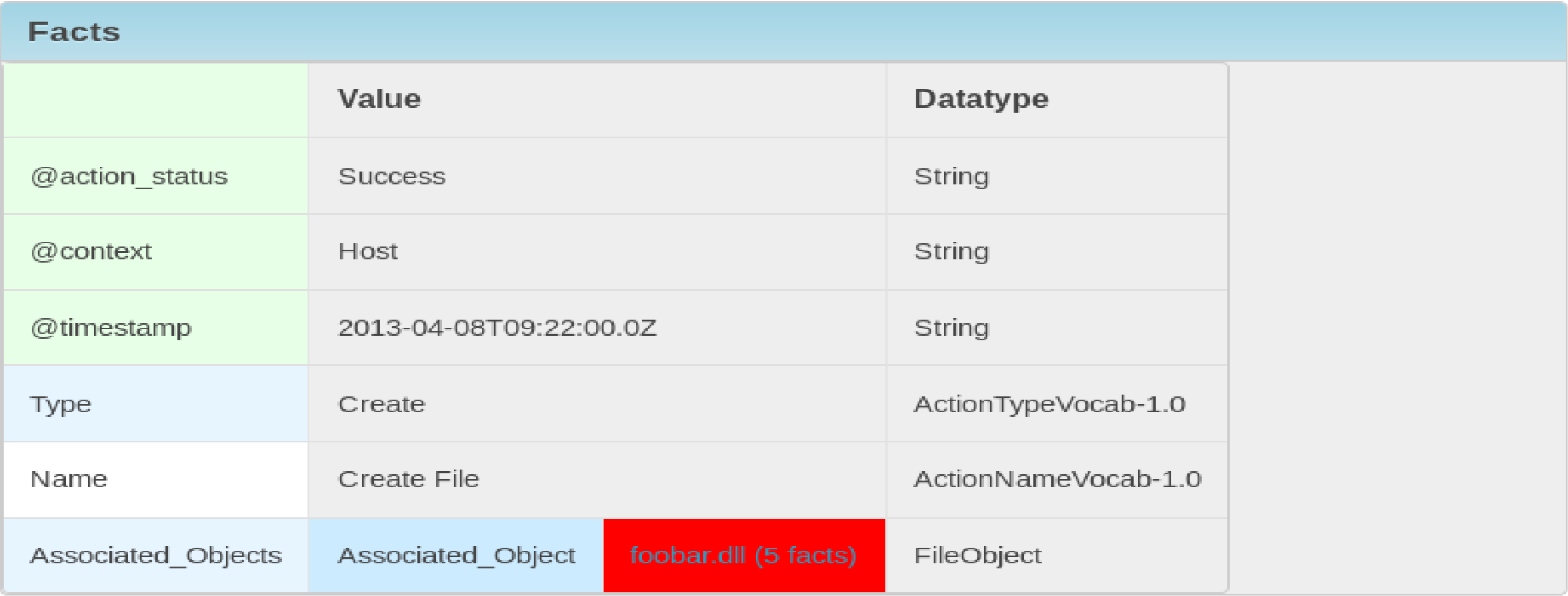
Type	cybox.mitre.org:Event 2 (http://cybox.mitre.org/cybox)	**Import Timestamp**	2014-05-14T14:08:42.876462+02:00

Facts

		Value		Datatype
Actions	Action	Create File		Action
Actions	Action	@action_status	Success	String
Actions	Action	@context	Host	String
Actions	Action	@timestamp	2013-04-08T09:22:00.0Z	String

Example: Importing a CybOX 2.0 Observable
Resulting Structure

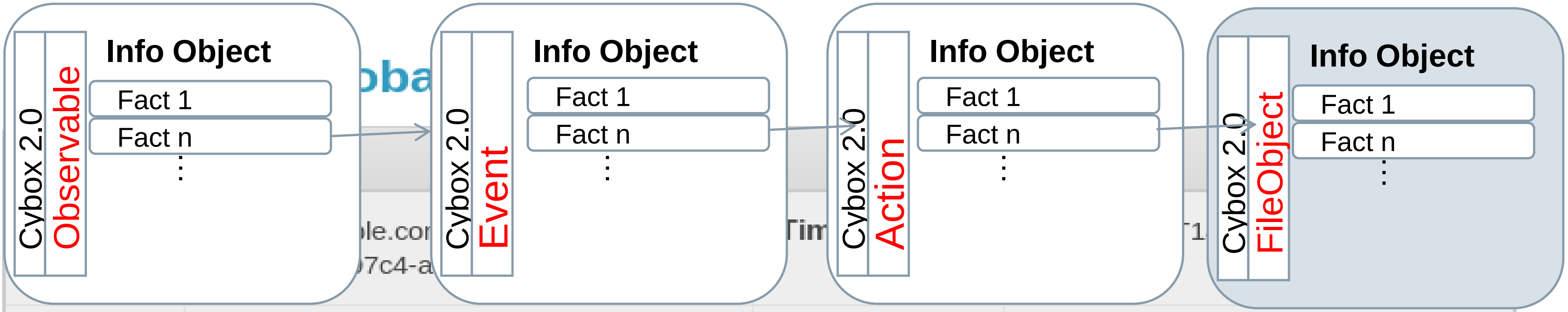


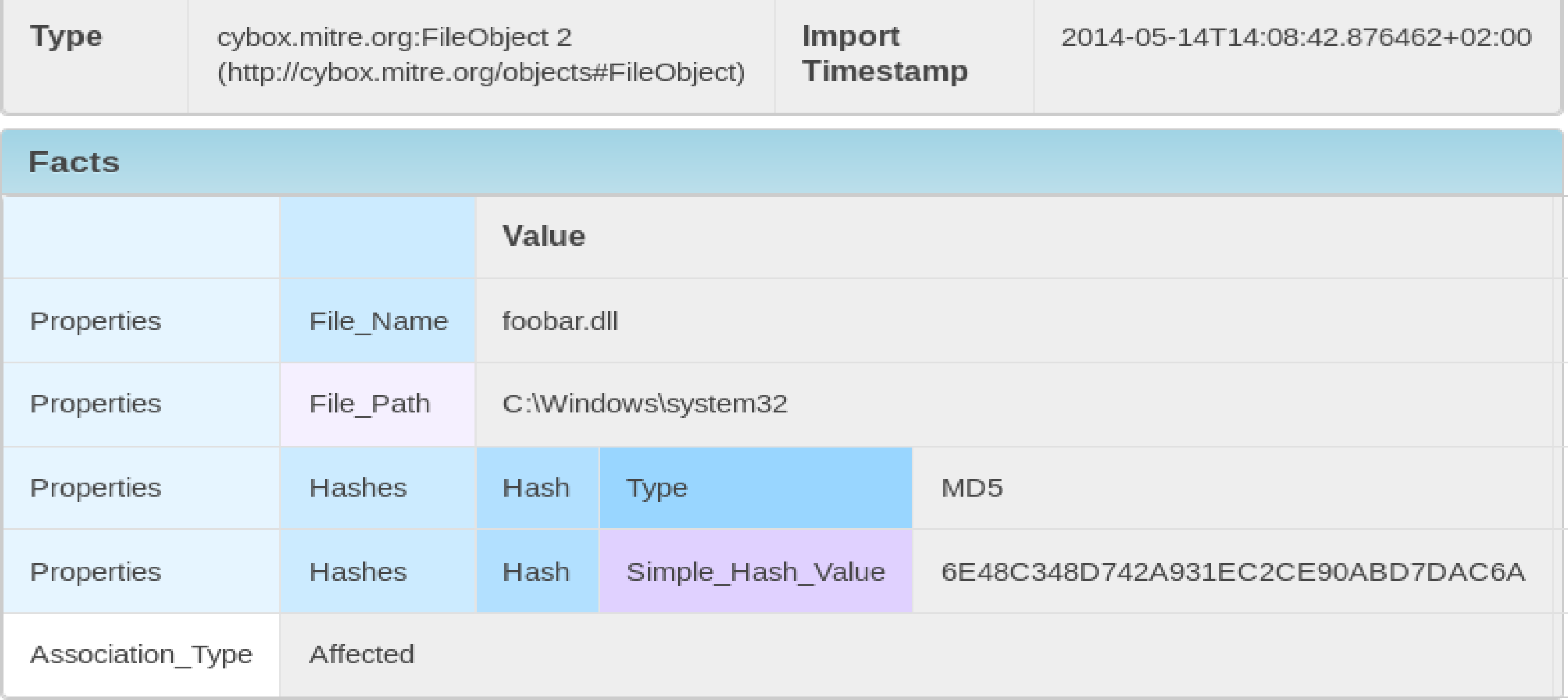


Facts

	Value	Datatype
@action_status	Success	String
@context	Host	String
@timestamp	2013-04-08T09:22:00.0Z	String
Type	Create	ActionTypeVocab-1.0
Name	Create File	ActionNameVocab-1.0
Associated_Objects	Associated_Object foobar.dll (5 facts)	FileObject

Example: Importing a CybOX 2.0 Observable
Resulting Structure





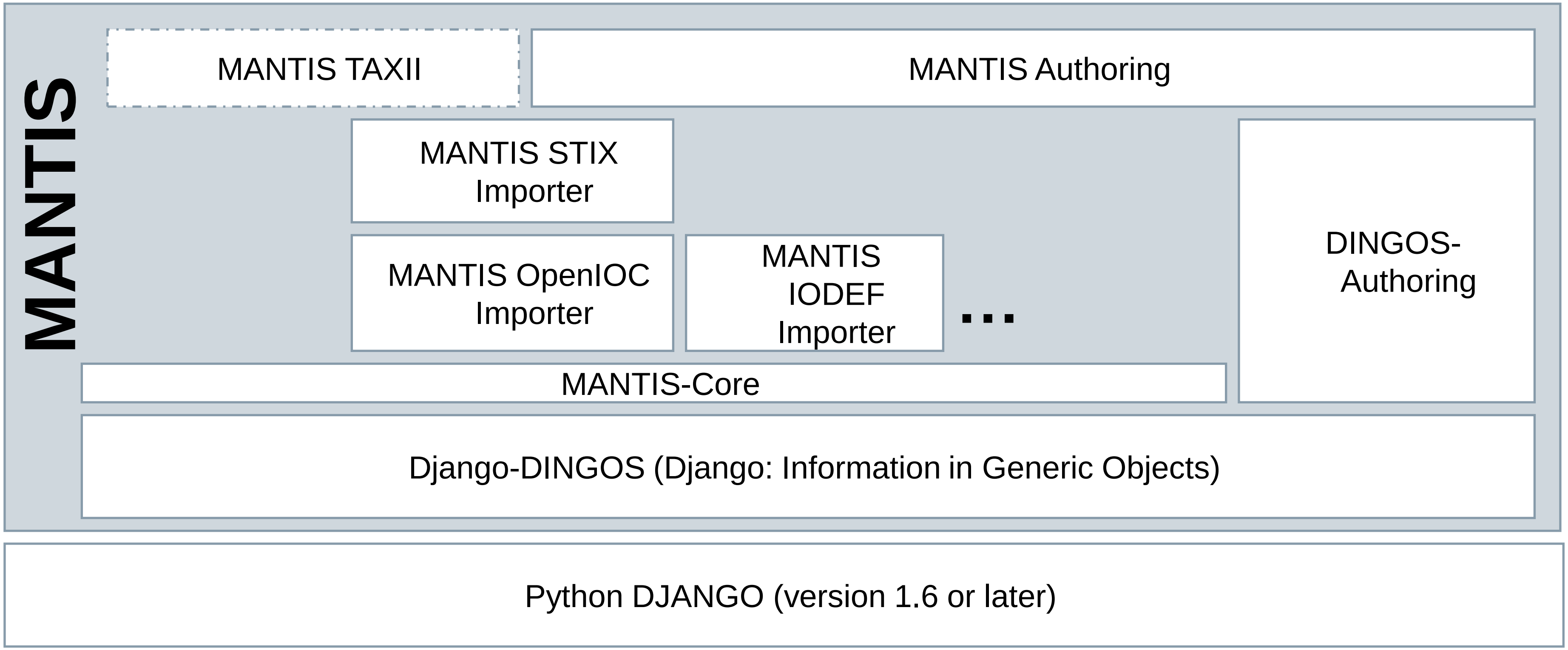
Type	cybox.mitre.org:FileObject 2 (http://cybox.mitre.org/objects#FileObject)	**Import Timestamp**	2014-05-14T14:08:42.876462+02:00

Facts

		Value		
Properties	File_Name	foobar.dll		
Properties	File_Path	C:\Windows\system32		
Properties	Hashes	Hash	Type	MD5
Properties	Hashes	Hash	Simple_Hash_Value	6E48C348D742A931EC2CE90ABD7DAC6A
Association_Type	Affected			

Siemens CERT‘s MANTIS Framework

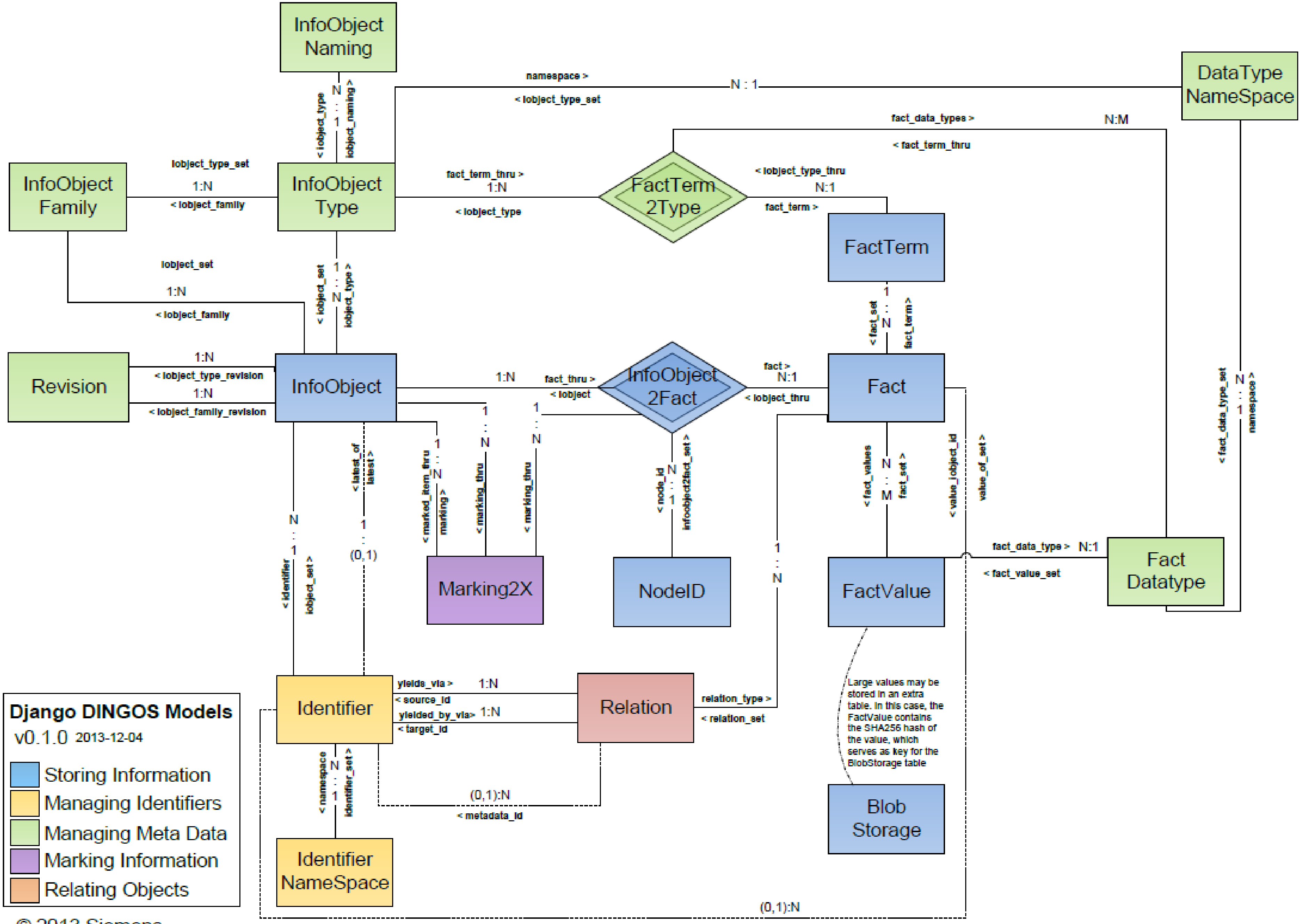
- **MANTIS is based on Django, the Python-based web application framework.**
- **The current version of MANTIS contains import modules for STIX/CybOX, OpenIOC, and IODEF, but the architecture is of MANTIS is generic and provides for easy generation of additional import modules for other standards.**



What MANTIS is and isn‘t

- MANTIS **is** a *PoC implementation* of a framework for managing cyber threat intelligence expressed in standards such as STIX, CybOX, IODEF, etc.
- The aims of providing such an example implementation 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.

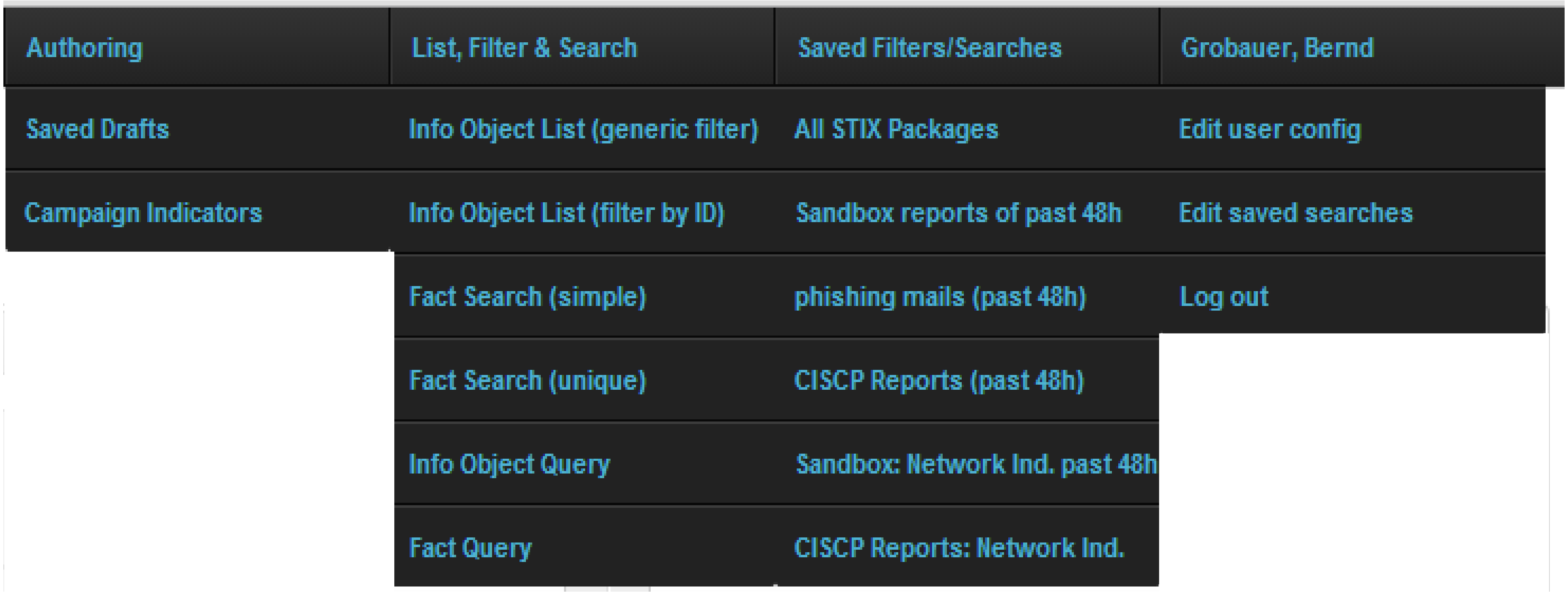


Django DINGOS Models

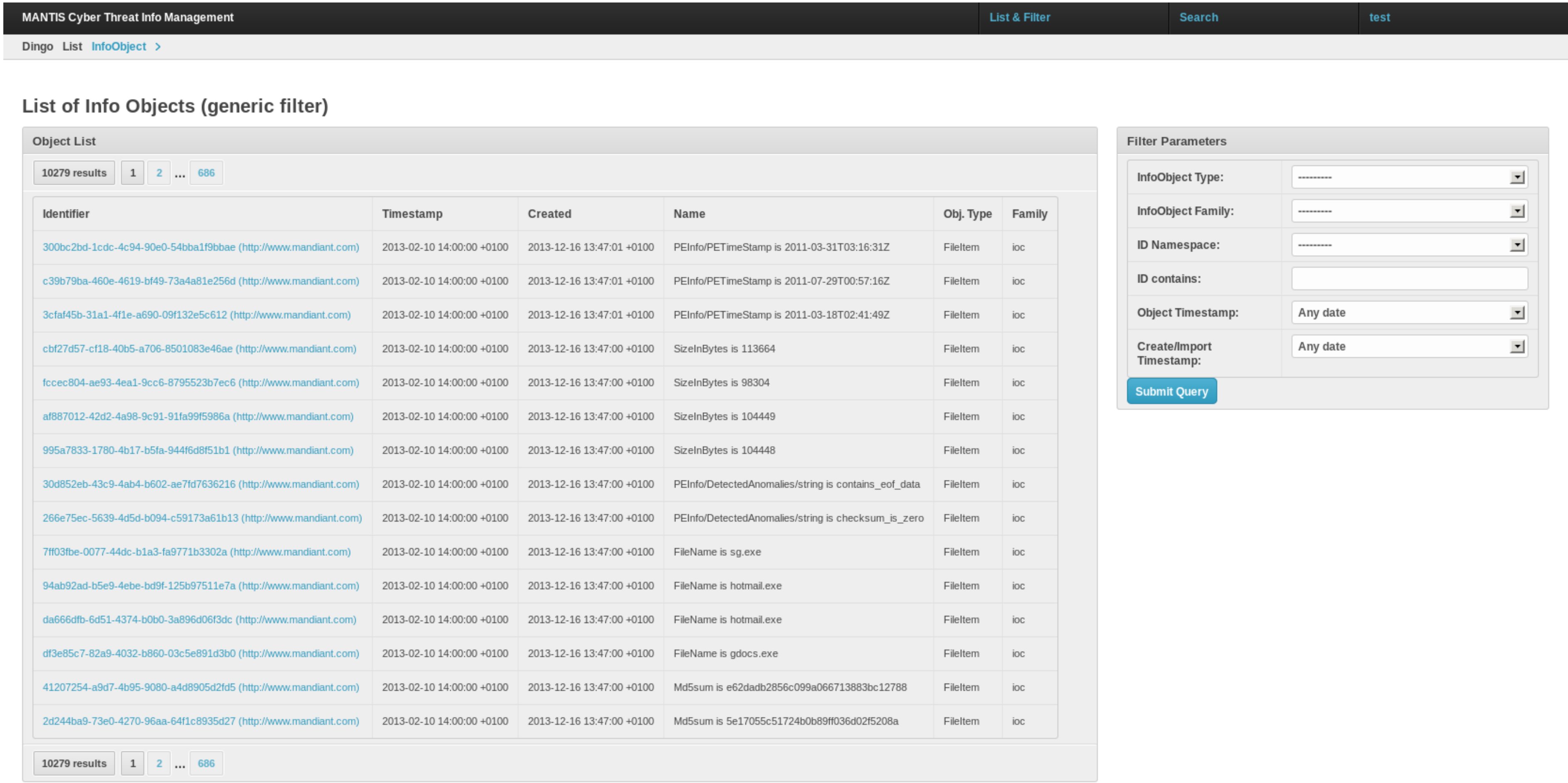
v0.1.0 2013-12-04

- 🟦 Storing Information
- 🟨 Managing Identifiers
- 🟩 Managing Meta Data
- 🟪 Marking Information
- 🟧 Relating Objects

Screenshots
Menubar



Viewing imported InfoObjects



MANTIS Cyber Threat Info Management | List & Filter | Search | test

Dingo List InfoObject >

List of Info Objects (generic filter)

Object List

10279 results 1 2 ... 686

Identifier	Timestamp	Created	Name	Obj. Type	Family
300bc2bd-1cdc-4c94-90e0-54bba1f9bbae (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:01 +0100	PEInfo/PETimeStamp is 2011-03-31T03:16:31Z	FileItem	ioc
c39b79ba-460e-4619-bf49-73a4a81e256d (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:01 +0100	PEInfo/PETimeStamp is 2011-07-29T00:57:16Z	FileItem	ioc
3cfaf45b-31a1-4f1e-a690-09f132e5c612 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:01 +0100	PEInfo/PETimeStamp is 2011-03-18T02:41:49Z	FileItem	ioc
cbf27d57-cf18-40b5-a706-8501083e46ae (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	SizeInBytes is 113664	FileItem	ioc
fccec804-ae93-4ea1-9cc6-8795523b7ec6 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	SizeInBytes is 98304	FileItem	ioc
af887012-42d2-4a98-9c91-91fa99f5986a (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	SizeInBytes is 104449	FileItem	ioc
995a7833-1780-4b17-b5fa-944f6d8f51b1 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	SizeInBytes is 104448	FileItem	ioc
30d852eb-43c9-4ab4-b602-ae7fd7636216 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	PEInfo/DetectedAnomalies/string is contains_eof_data	FileItem	ioc
266e75ec-5639-4d5d-b094-c59173a61b13 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	PEInfo/DetectedAnomalies/string is checksum_is_zero	FileItem	ioc
7ff03fbe-0077-44dc-b1a3-fa9771b3302a (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	FileName is sg.exe	FileItem	ioc
94ab92ad-b5e9-4ebe-bd9f-125b97511e7a (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	FileName is hotmail.exe	FileItem	ioc
da666dfb-6d51-4374-b0b0-3a896d06f3dc (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	FileName is hotmail.exe	FileItem	ioc
df3e85c7-82a9-4032-b860-03c5e891d3b0 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	FileName is gdocs.exe	FileItem	ioc
41207254-a9d7-4b95-9080-a4d8905d2fd5 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	Md5sum is e62dadb2856c099a066713883bc12788	FileItem	ioc
2d244ba9-73e0-4270-96aa-64f1c8935d27 (http://www.mandiant.com)	2013-02-10 14:00:00 +0100	2013-12-16 13:47:00 +0100	Md5sum is 5e17055c51724b0b89ff036d02f5208a	FileItem	ioc

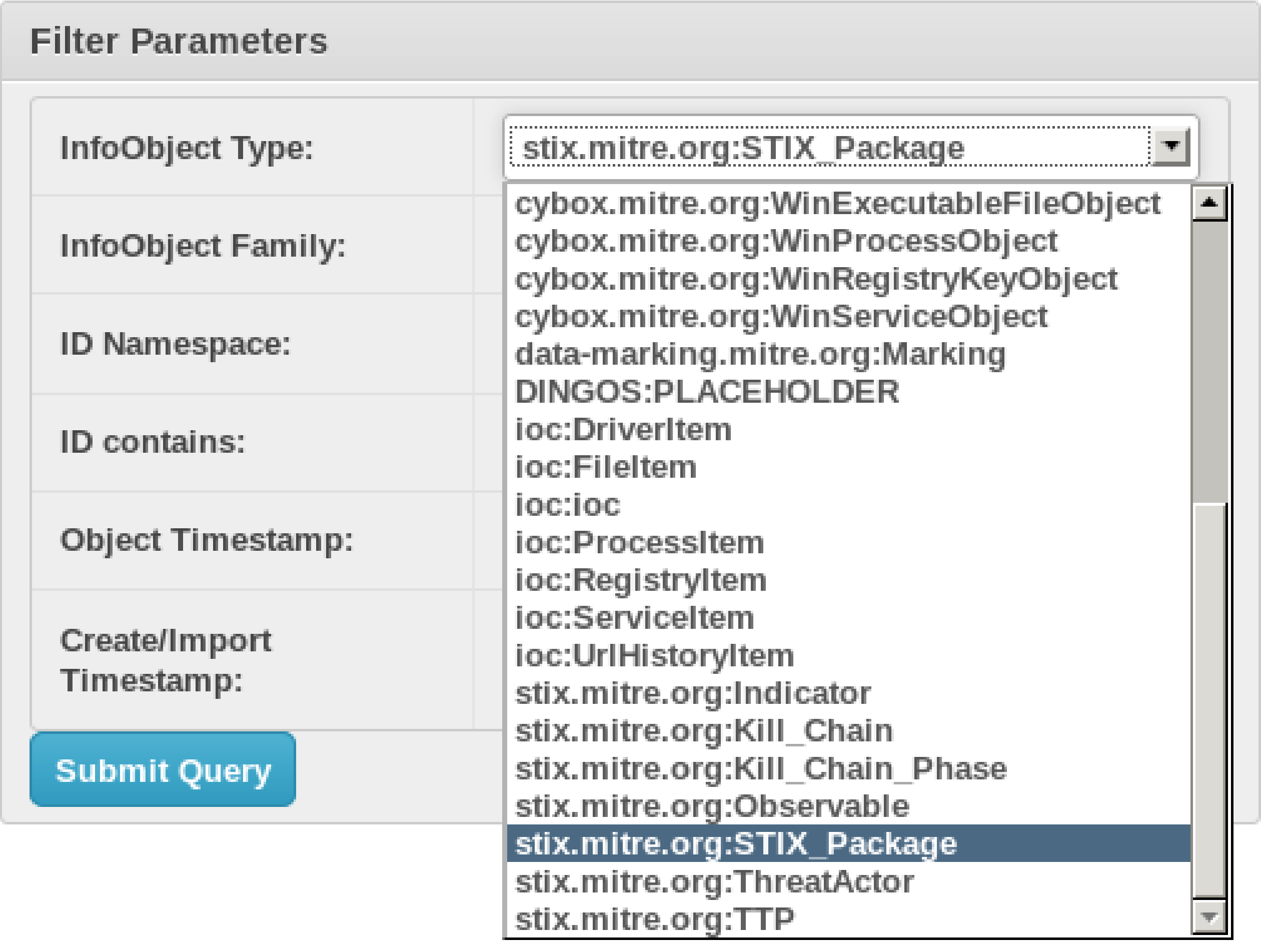
10279 results 1 2 ... 686

Filter Parameters

InfoObject Type:	---------
InfoObject Family:	---------
ID Namespace:	---------
ID contains:	
Object Timestamp:	Any date
Create/Import Timestamp:	Any date

Submit Query

Filtering InfoObjects

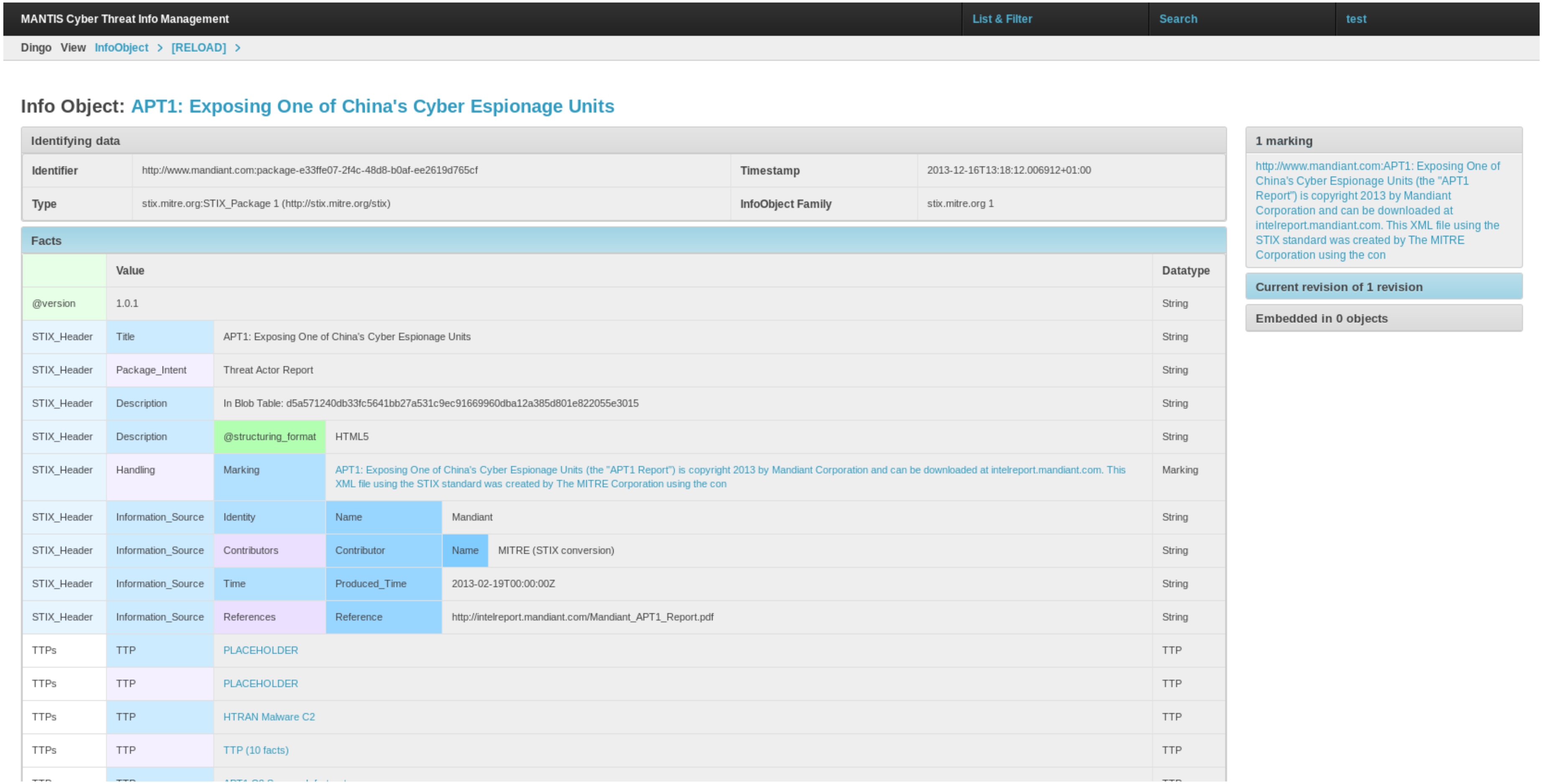


Filter Parameters

InfoObject Type:	stix.mitre.org:STIX_Package
InfoObject Family:	
ID Namespace:	
ID contains:	
Object Timestamp:	
Create/Import Timestamp:	

cybox.mitre.org:WinExecutableFileObject
cybox.mitre.org:WinProcessObject
cybox.mitre.org:WinRegistryKeyObject
cybox.mitre.org:WinServiceObject
data-marking.mitre.org:Marking
DINGOS:PLACEHOLDER
ioc:DriverItem
ioc:FileItem
ioc:ioc
ioc:ProcessItem
ioc:RegistryItem
ioc:ServiceItem
ioc:UrlHistoryItem
stix.mitre.org:Indicator
stix.mitre.org:Kill_Chain
stix.mitre.org:Kill_Chain_Phase
stix.mitre.org:Observable
stix.mitre.org:STIX_Package
stix.mitre.org:ThreatActor
stix.mitre.org:TTP

Viewing an InfoObject



MANTIS Cyber Threat Info Management | List & Filter | Search | test

Dingo View InfoObject > [RELOAD] >

Info Object: APT1: Exposing One of China's Cyber Espionage Units

Identifying data

Identifier	http://www.mandiant.com:package-e33ffe07-2f4c-48d8-b0af-ee2619d765cf	**Timestamp**	2013-12-16T13:18:12.006912+01:00
Type	stix.mitre.org:STIX_Package 1 (http://stix.mitre.org/stix)	**InfoObject Family**	stix.mitre.org 1

Facts

	Value					Datatype
@version	1.0.1					String
STIX_Header	Title	APT1: Exposing One of China's Cyber Espionage Units				String
STIX_Header	Package_Intent	Threat Actor Report				String
STIX_Header	Description	In Blob Table: d5a571240db33fc5641bb27a531c9ec91669960dba12a385d801e822055e3015				String
STIX_Header	Description	@structuring_format	HTML5			String
STIX_Header	Handling	Marking	APT1: Exposing One of China's Cyber Espionage Units (the "APT1 Report") is copyright 2013 by Mandiant Corporation and can be downloaded at intelreport.mandiant.com. This XML file using the STIX standard was created by The MITRE Corporation using the con			Marking
STIX_Header	Information_Source	Identity	Name	Mandiant		String
STIX_Header	Information_Source	Contributors	Contributor	Name	MITRE (STIX conversion)	String
STIX_Header	Information_Source	Time	Produced_Time	2013-02-19T00:00:00Z		String
STIX_Header	Information_Source	References	Reference	http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf		String
TTPs	TTP	PLACEHOLDER				TTP
TTPs	TTP	PLACEHOLDER				TTP
TTPs	TTP	HTRAN Malware C2				TTP
TTPs	TTP	TTP (10 facts)				TTP

1 marking

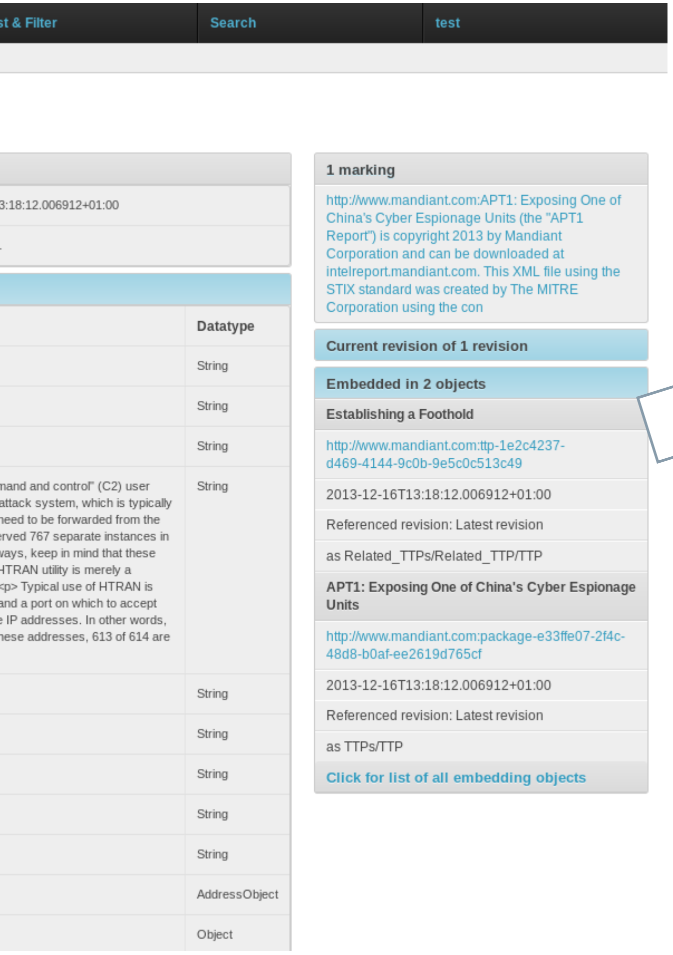
http://www.mandiant.com:APT1: Exposing One of China's Cyber Espionage Units (the "APT1 Report") is copyright 2013 by Mandiant Corporation and can be downloaded at intelreport.mandiant.com. This XML file using the STIX standard was created by The MITRE Corporation using the con

Current revision of 1 revision

Embedded in 0 objects

Viewing another InfoObject

The widget on the right-hand side (bottom) shows, in which InfoObjects the given InfoObject is embedded.



3:18:12.006912+01:00

	Datatype
	String
	String
	String
mand and control" (C2) user attack system, which is typically need to be forwarded from the erved 767 separate instances in ways, keep in mind that these HTRAN utility is merely a <p> Typical use of HTRAN is and a port on which to accept e IP addresses. In other words, hese addresses, 613 of 614 are	String
	String
	String
	String
	String
	String
	AddressObject
	Object

1 marking

http://www.mandiant.com:APT1: Exposing One of China's Cyber Espionage Units (the "APT1 Report") is copyright 2013 by Mandiant Corporation and can be downloaded at intelreport.mandiant.com. This XML file using the STIX standard was created by The MITRE Corporation using the con

Current revision of 1 revision

Embedded in 2 objects

Establishing a Foothold

http://www.mandiant.com:ttp-1e2c4237-d469-4144-9c0b-9e5c0c513c49

2013-12-16T13:18:12.006912+01:00

Referenced revision: Latest revision

as Related_TTPs/Related_TTP/TTP

APT1: Exposing One of China's Cyber Espionage Units

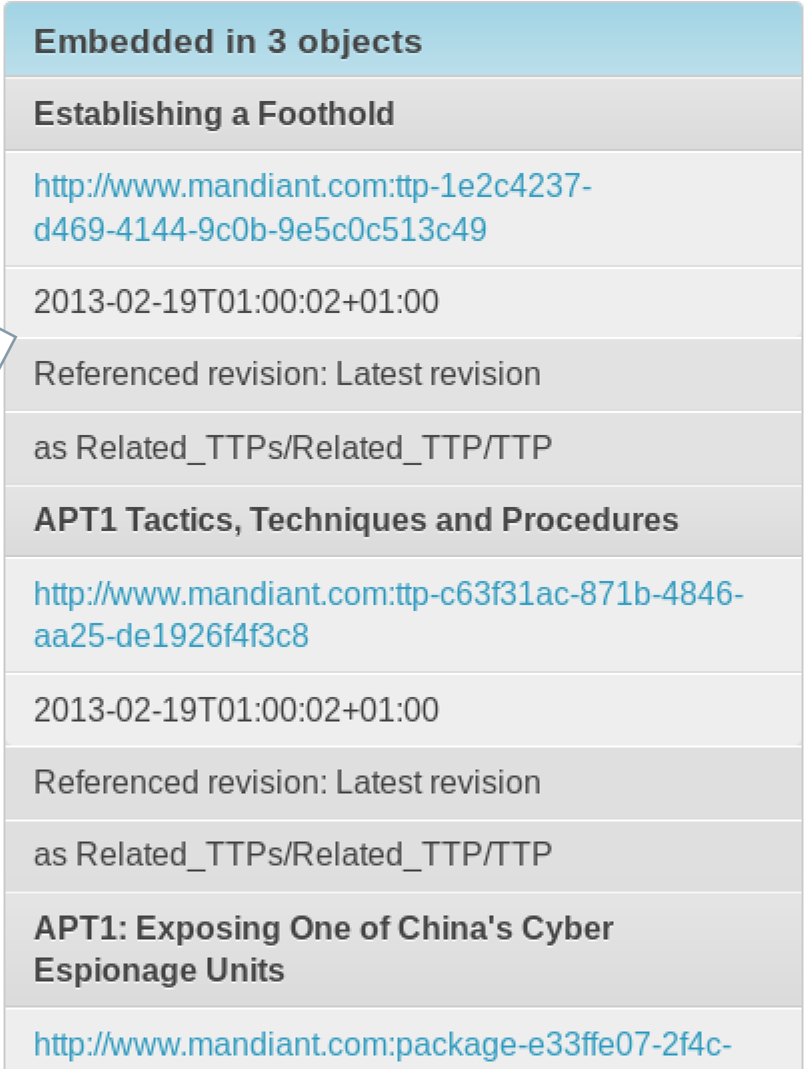
http://www.mandiant.com:package-e33ffe07-2f4c-48d8-b0af-ee2619d765cf

2013-12-16T13:18:12.006912+01:00

Referenced revision: Latest revision

as TTPs/TTP

Click for list of all embedding objects



Embedded in 3 objects

Establishing a Foothold

http://www.mandiant.com:ttp-1e2c4237-d469-4144-9c0b-9e5c0c513c49

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

Referenced revision: Latest revision

as Related_TTPs/Related_TTP/TTP

APT1 Tactics, Techniques and Procedures

http://www.mandiant.com:ttp-c63f31ac-871b-4846-aa25-de1926f4f3c8

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

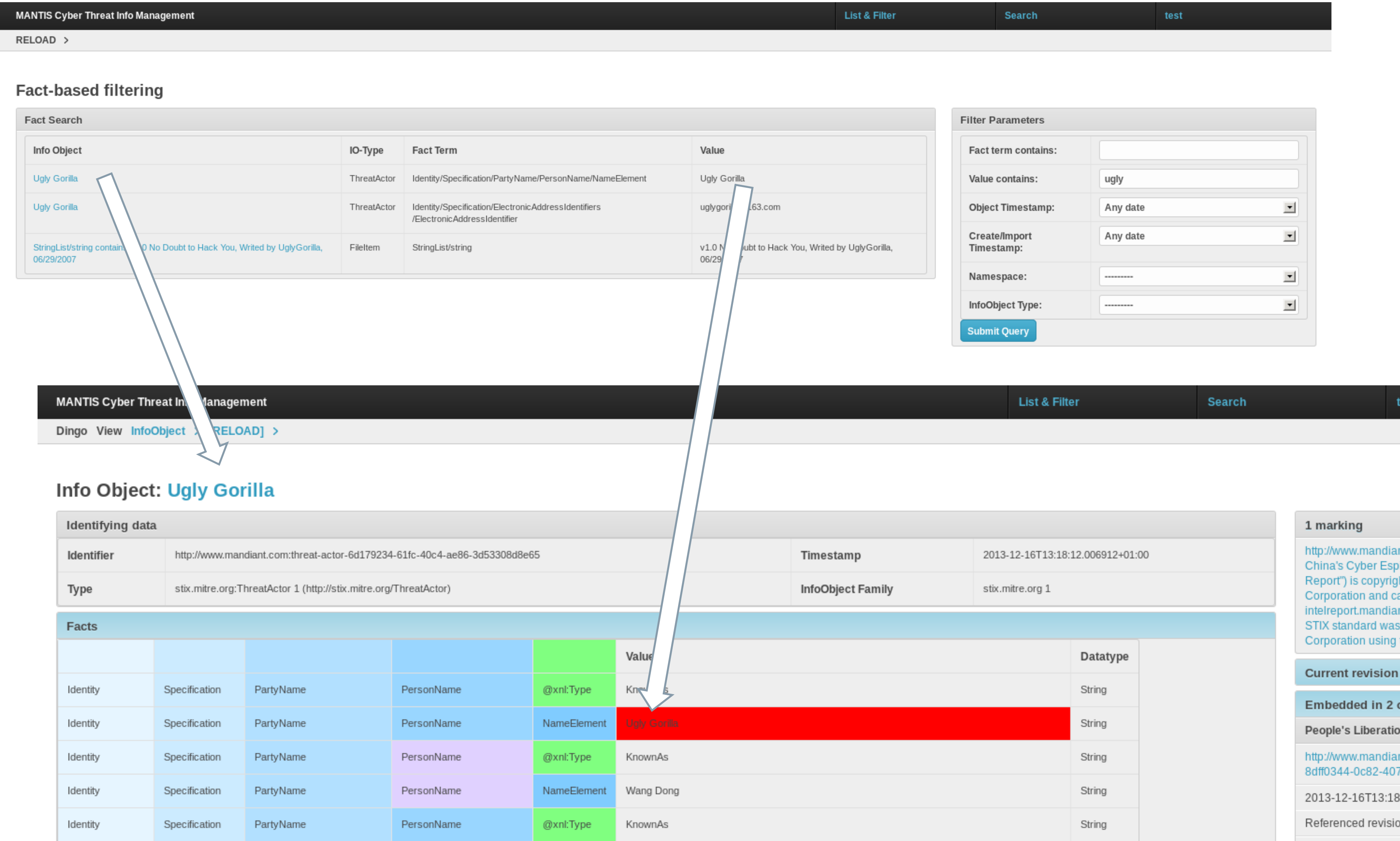
Referenced revision: Latest revision

as Related_TTPs/Related_TTP/TTP

APT1: Exposing One of China's Cyber Espionage Units

http://www.mandiant.com:package-e33ffe07-2f4c-

Searching



MANTIS Cyber Threat Info Management | List & Filter | Search | test

RELOAD >

Fact-based filtering

Fact Search

Info Object	IO-Type	Fact Term	Value
Ugly Gorilla	ThreatActor	Identity/Specification/PartyName/PersonName/NameElement	Ugly Gorilla
Ugly Gorilla	ThreatActor	Identity/Specification/ElectronicAddressIdentifiers /ElectronicAddressIdentifier	uglygori 163.com
StringList/string contain 0 No Doubt to Hack You, Writed by UglyGorilla, 06/29/2007	FileItem	StringList/string	v1.0 N ubt to Hack You, Writed by UglyGorilla, 06/29 7

Filter Parameters

Fact term contains:	
Value contains:	ugly
Object Timestamp:	Any date
Create/Import Timestamp:	Any date
Namespace:	---------
InfoObject Type:	---------

Submit Query

MANTIS Cyber Threat In Management | List & Filter | Search | t

Dingo View InfoObject > RELOAD] >

Info Object: Ugly Gorilla

Identifying data

Identifier	http://www.mandiant.com:threat-actor-6d179234-61fc-40c4-ae86-3d53308d8e65	Timestamp	2013-12-16T13:18:12.006912+01:00
Type	stix.mitre.org:ThreatActor 1 (http://stix.mitre.org/ThreatActor)	InfoObject Family	stix.mitre.org 1

Facts

					Value	Datatype
Identity	Specification	PartyName	PersonName	@xnl:Type	Kn s	String
Identity	Specification	PartyName	PersonName	NameElement	Ugly Gorilla	String
Identity	Specification	PartyName	PersonName	@xnl:Type	KnownAs	String
Identity	Specification	PartyName	PersonName	NameElement	Wang Dong	String
Identity	Specification	PartyName	PersonName	@xnl:Type	KnownAs	String

1 marking

http://www.mandiar
China's Cyber Esp
Report") is copyrig
Corporation and ca
intelreport.mandiar
STIX standard was
Corporation using

Current revision

Embedded in 2 c

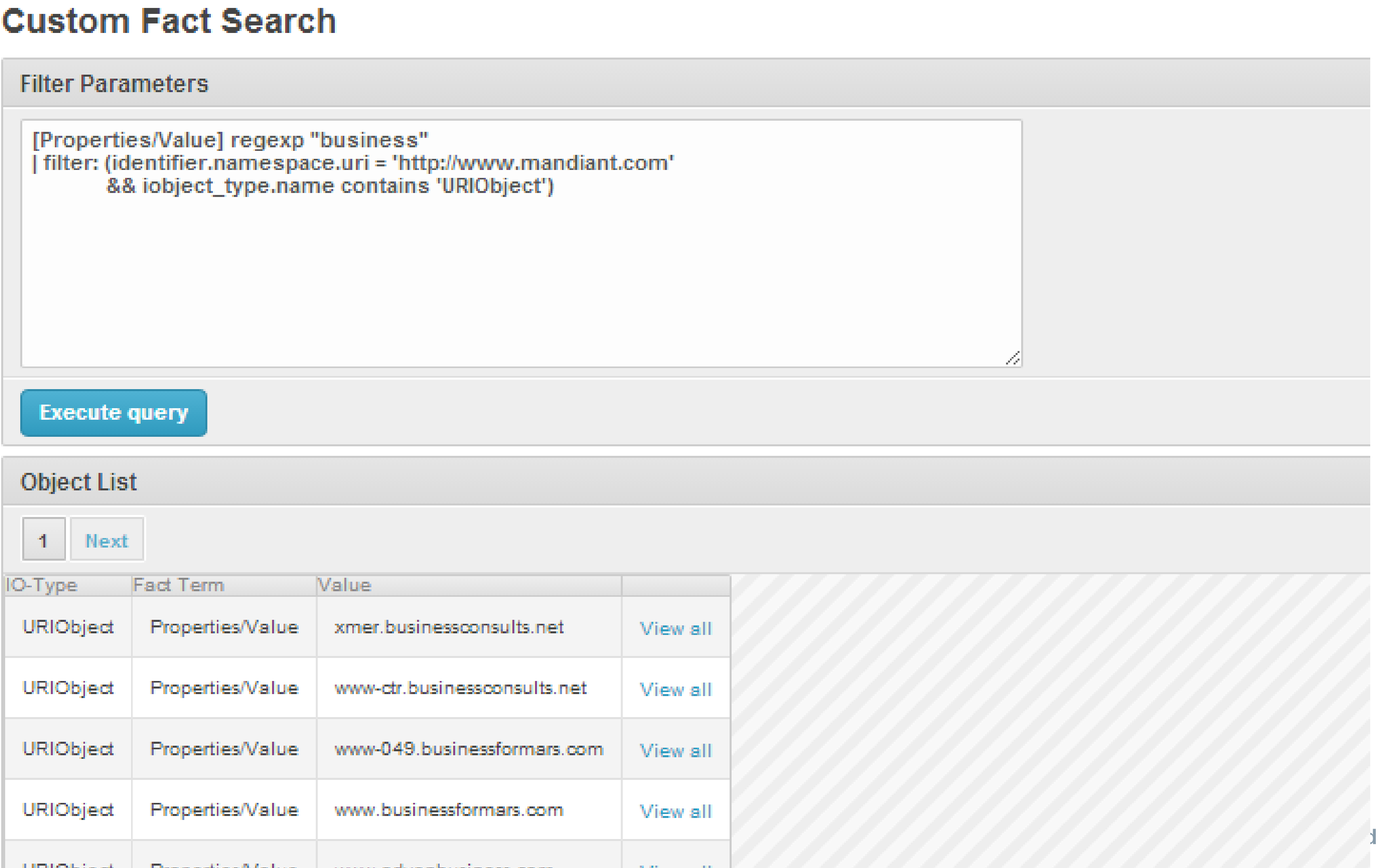
People's Liberatio

http://www.mandiar
8dff0344-0c82-407

2013-12-16T13:18

Referenced revisio

Searching with custom search (upcoming feature)



Custom Fact Search

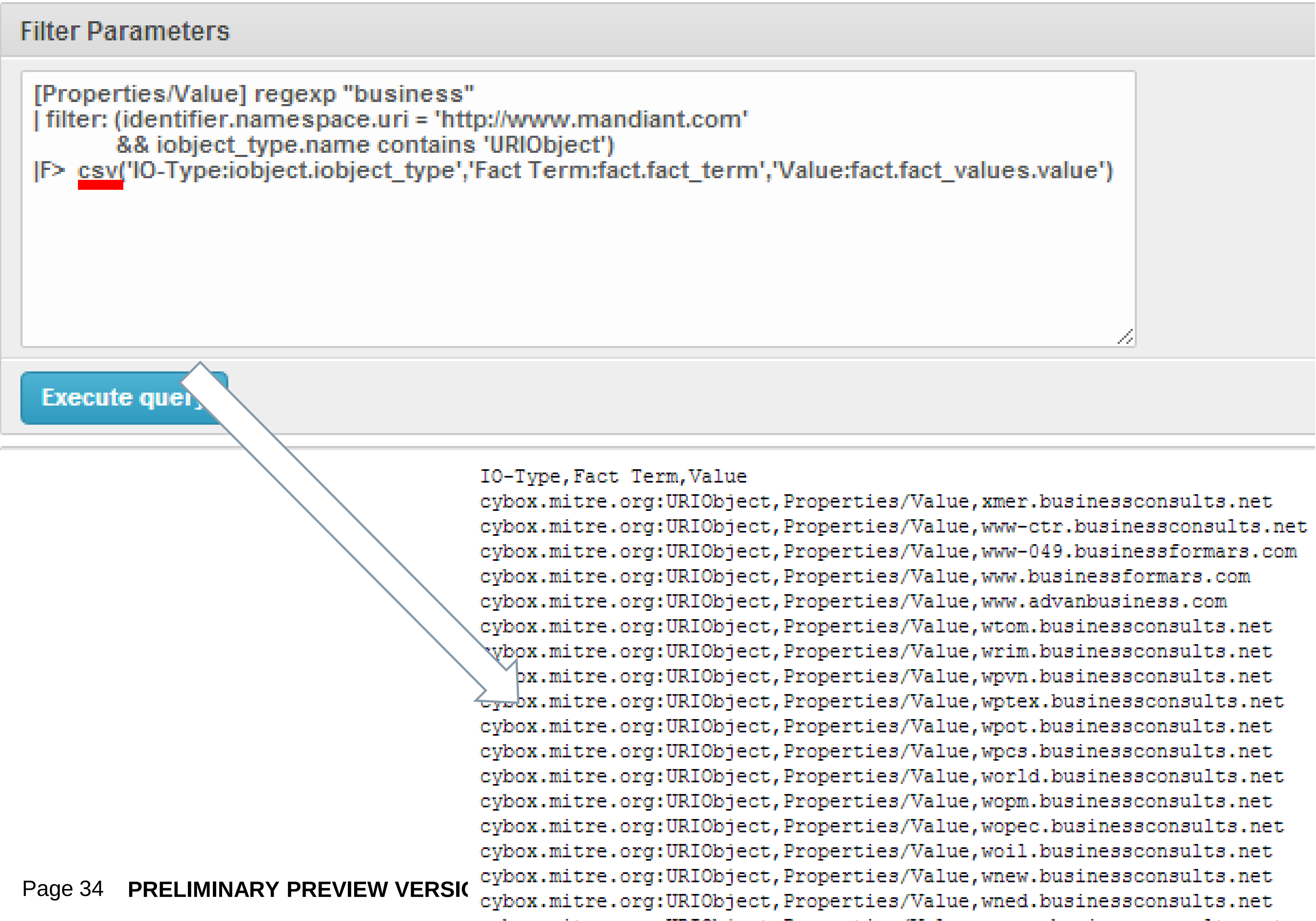
Filter Parameters

```
[Properties/Value] regexp "business"
| filter: (identifier.namespace.uri = 'http://www.mandiant.com'
          && iobject_type.name contains 'URIObject')
```

Object List

IO-Type	Fact Term	Value	
URIObject	Properties/Value	xmer.businessconsults.net	View all
URIObject	Properties/Value	www-ctr.businessconsults.net	View all
URIObject	Properties/Value	www-049.businessformars.com	View all
URIObject	Properties/Value	www.businessformars.com	View all
URIObject	Properties/Value	www.advanbusiness.com	View all

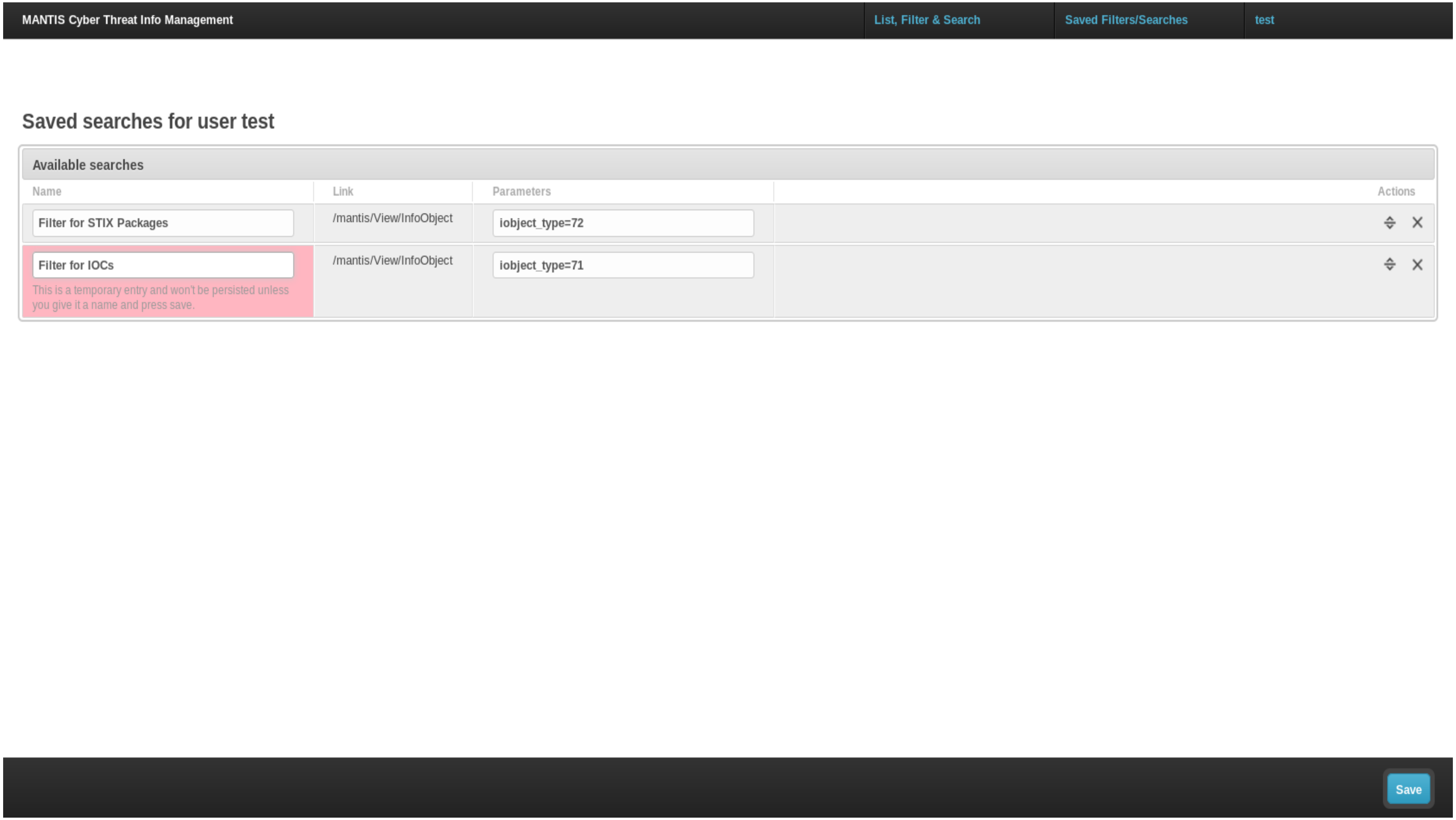
Searching with custom search (upcoming feature)



```
[Properties/Value] regexp "business"
| filter: (identifier.namespace.uri = 'http://www.mandiant.com'
          && iobject_type.name contains 'URIObject')
|F> csv('IO-Type:iobject.iobject_type','Fact Term:fact.fact_term','Value:fact.fact_values.value')
```

```
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,wpvn.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
```

Editing Custom Searches

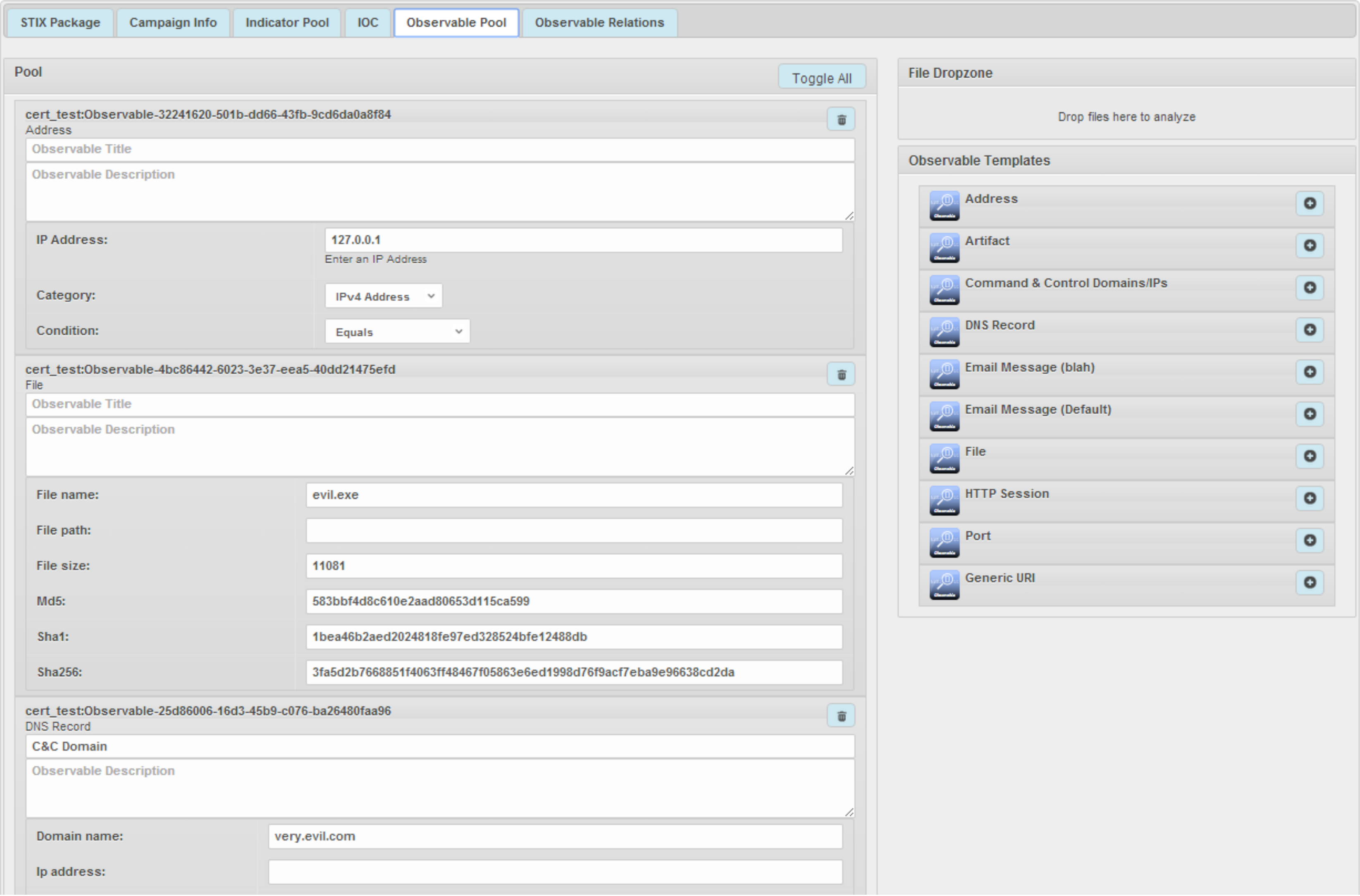


Saved searches for user test

Available searches

Name	Link	Parameters	Actions
Filter for STIX Packages	/mantis/View/InfoObject	iobject_type=72	⇕ ✕
Filter for IOCs This is a temporary entry and won't be persisted unless you give it a name and press save.	/mantis/View/InfoObject	iobject_type=71	⇕ ✕

Authoring: Entering Observables



Pool

cert_test:Observable-32241620-501b-dd66-43fb-9cd6da0a8f84
Address

Observable Title

Observable Description

IP Address:	127.0.0.1 Enter an IP Address
Category:	IPv4 Address
Condition:	Equals

cert_test:Observable-4bc86442-6023-3e37-eea5-40dd21475efd
File

Observable Title

Observable Description

File name:	evil.exe
File path:	
File size:	11081
Md5:	583bbf4d8c610e2aad80653d115ca599
Sha1:	1bea46b2aed2024818fe97ed328524bfe12488db
Sha256:	3fa5d2b7668851f4063ff48467f05863e6ed1998d76f9acf7eba9e96638cd2da

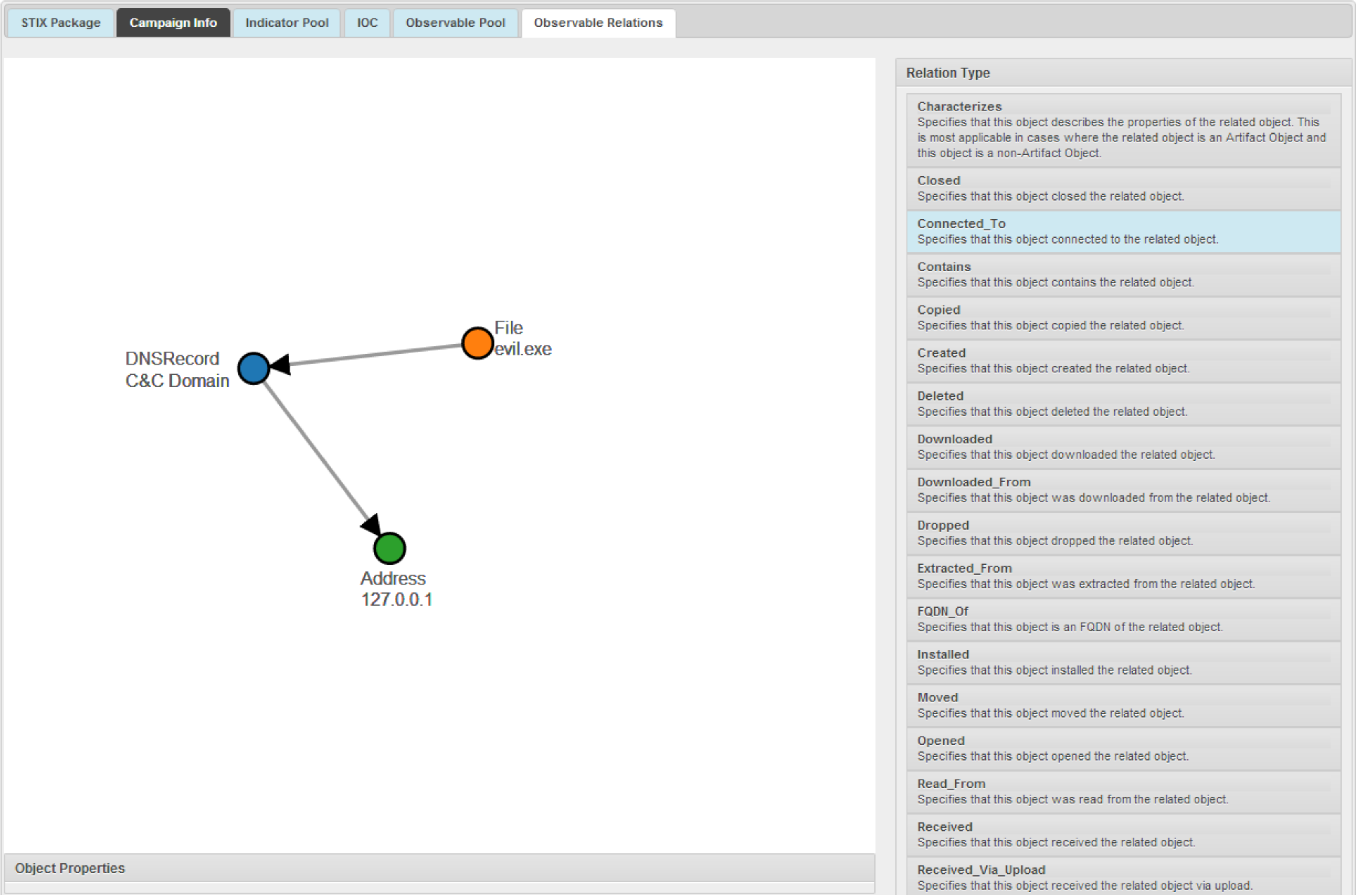
cert_test:Observable-25d86006-16d3-45b9-c076-ba26480faa96
DNS Record

C&C Domain

Observable Description

Domain name:	very.evil.com
Ip address:	

Authoring: Defining Relations between Objects



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.

Moved
Specifies that this object moved the related object.

Opened
Specifies that this object opened the related object.

Read_From
Specifies that this object was read from the related object.

Received
Specifies that this object received the related object.

Received_Via_Upload
Specifies that this object received the related object via upload.

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.