SIEMENS

Bernd Grobauer| Siemens CERT

Theory and Practice of Cyber Threat-Intelligence Management Using STIX and CybOX

Siemens Core Topics

The Future of Energy

It is becoming increasingly important to handle energy responsibly as prices increase, the threat of climate change continues, and resources dwindle worldwide. ↗

IT and Software

Whether it's optimizing manufacturing processes, managing traffic, or analyzing patient data in hospitals – IT solutions are essential in every industry today. ↗

The Future of Manufacturing

With technological innovations Siemens supports industrial enterprises to become more productive, efficient and flexible. ↗

Healthcare

The basic objective of good healthcare is not just to save people's lives but to improve their quality of life and their overall happiness. ↗

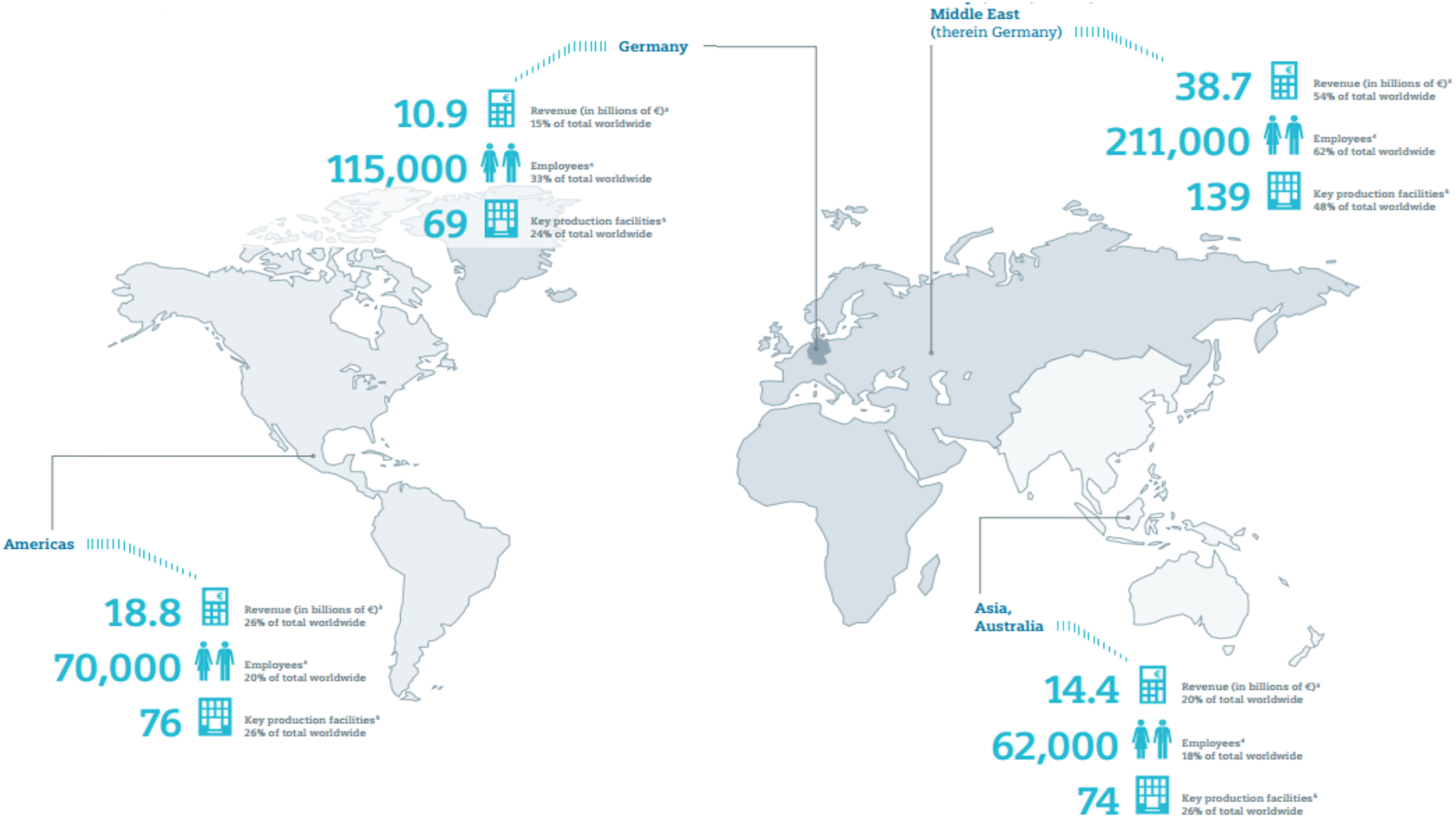
Sustainable Cities

With the right technology, cities and metropolitan areas can become more environmentally-friendly. ↗

Financial Services

Financial Services is an international provider of financing solutions. Our financial and industry know-how creates customer value and enhances customer competitiveness. ↗

Siemens is a global company



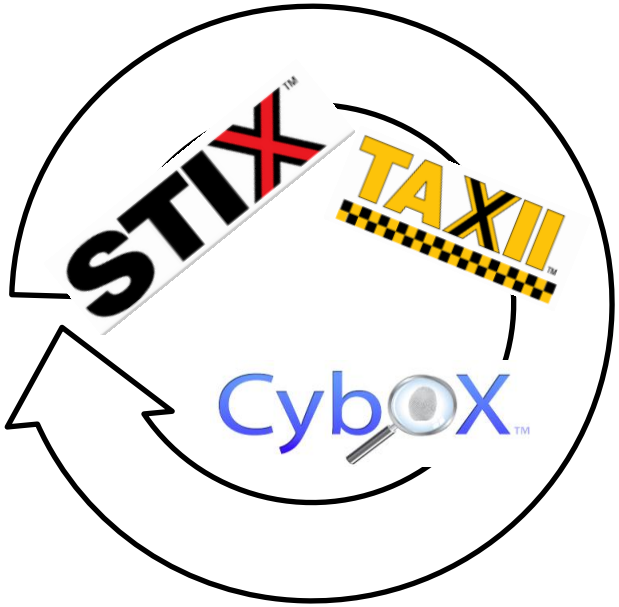
Corporate Technology – the center of Siemens research: 1,600 scientists, 4,400 software developers, and about 420 Intellectual Property experts

SIEMENS

Global organization of CT (major locations)

What we have been working towards for the past few years

SIEMENS

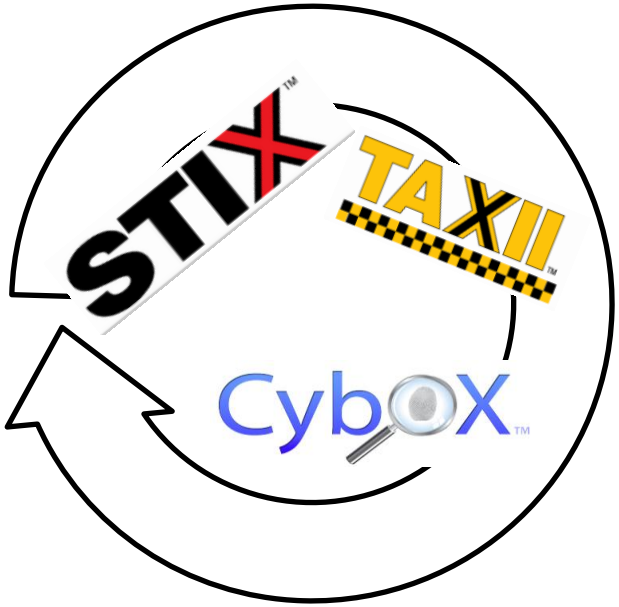


GOAL:
We receive lot‘s and lot‘s of cyber threat intelligence based on STIX & CybOX

Exchange has taken off
Now what?

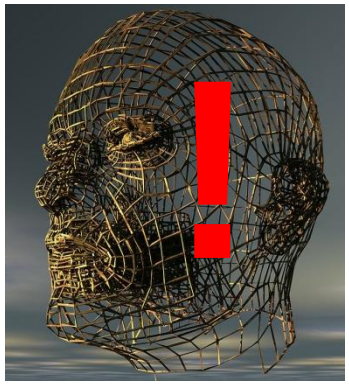
SIEMENS

Let‘s see



We receive lot‘s and lot‘s of cyber threat intelligence based on STIX & CybOX

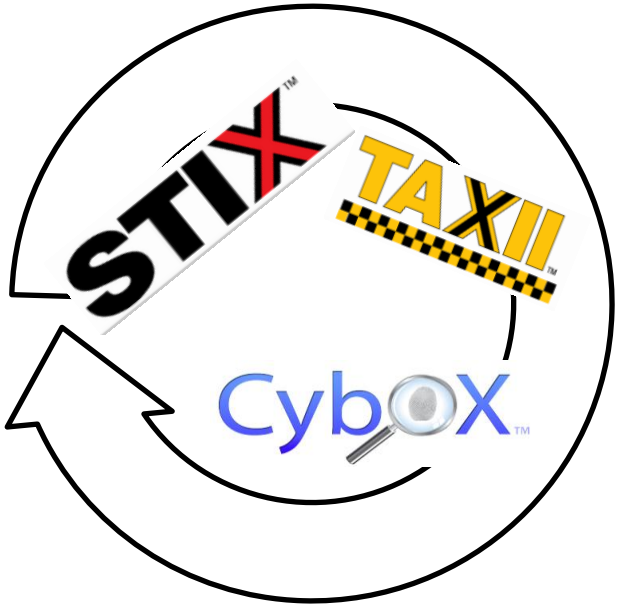
Then a Miracle Occurs



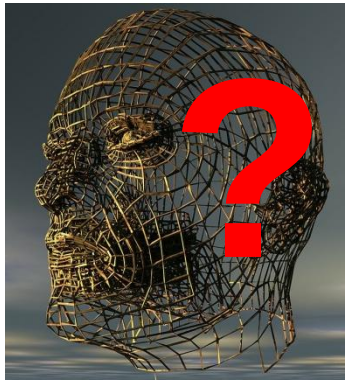
Analysts know what‘s important

Detection tools know what to look for

Reality



We receive lot‘s and lot‘s of cyber threat intelligence based on STIX & CybOX



Analysts don‘t know what‘s important

Detection tools don‘t really know what to look for

What is the heart of the problem?

SIEMENS

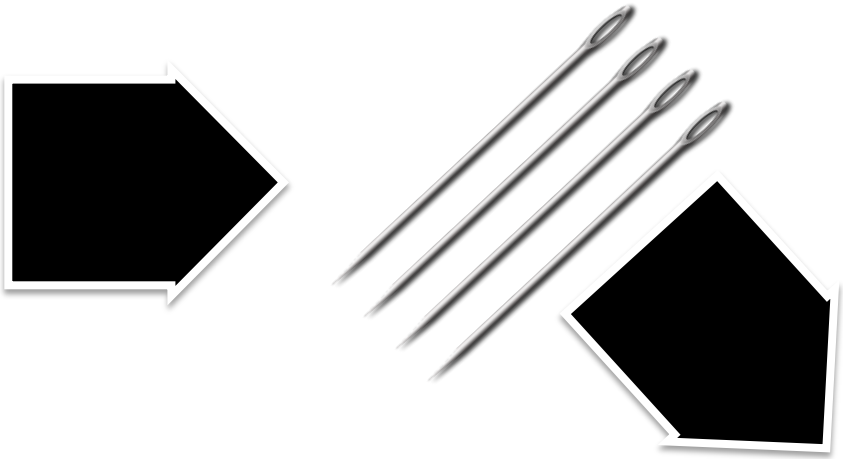
Drinking from a fire hose

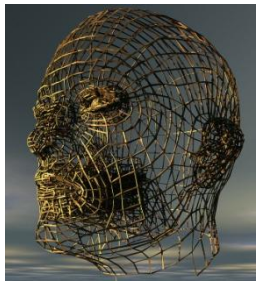
Detection:
Finding the needle in the haystack

SIEMENS

Detection with Cyber-Threat-Intelligence Sharing: The second-order haystack problem

SIEMENS

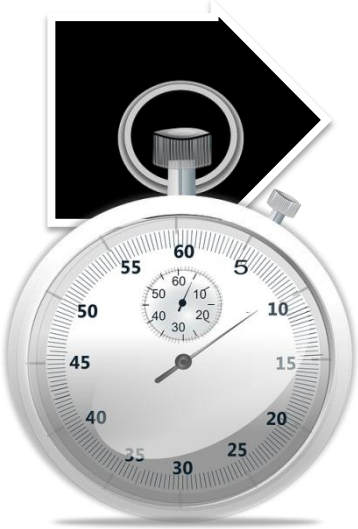


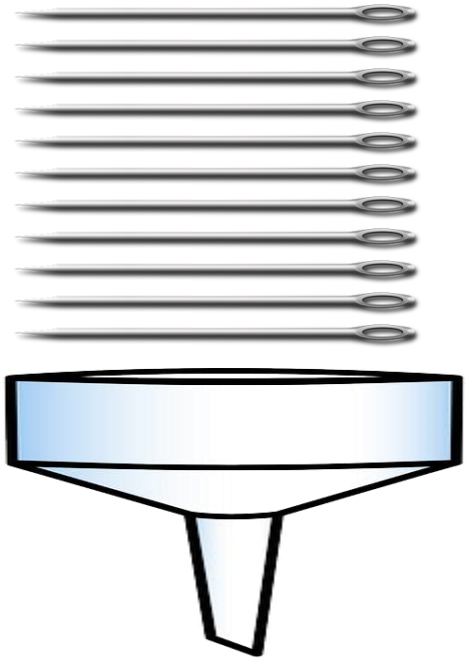


You need to find the needles that you need to find in your haystack

Detection with Cyber-Threat-Intelligence Sharing: The second-order haystack problem

SIEMENS

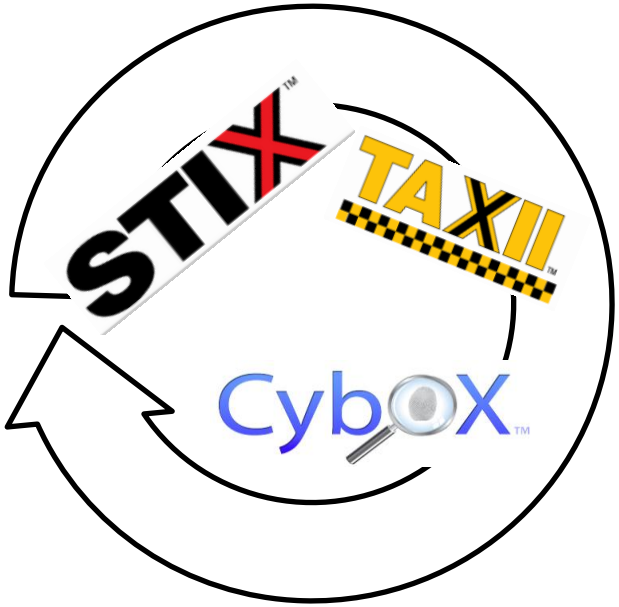




You need to be able to access all relevant needles almost instantly

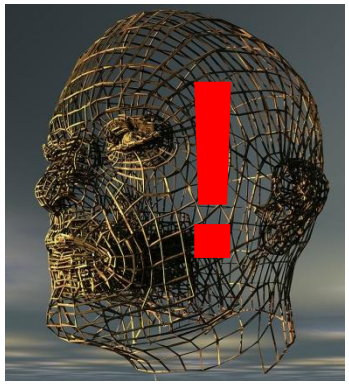
What are essential ingredients of the miracle we are trying to work?

SIEMENS



We receive lot‘s and lot‘s of cyber threat intelligence based on STIX & CybOX

Then a Miracle Occurs



Analysts know what‘s important

Detection tools know what to look for

Two essential components for working the Cyber Threat Intelligence Miracle based on STIX/CybOX

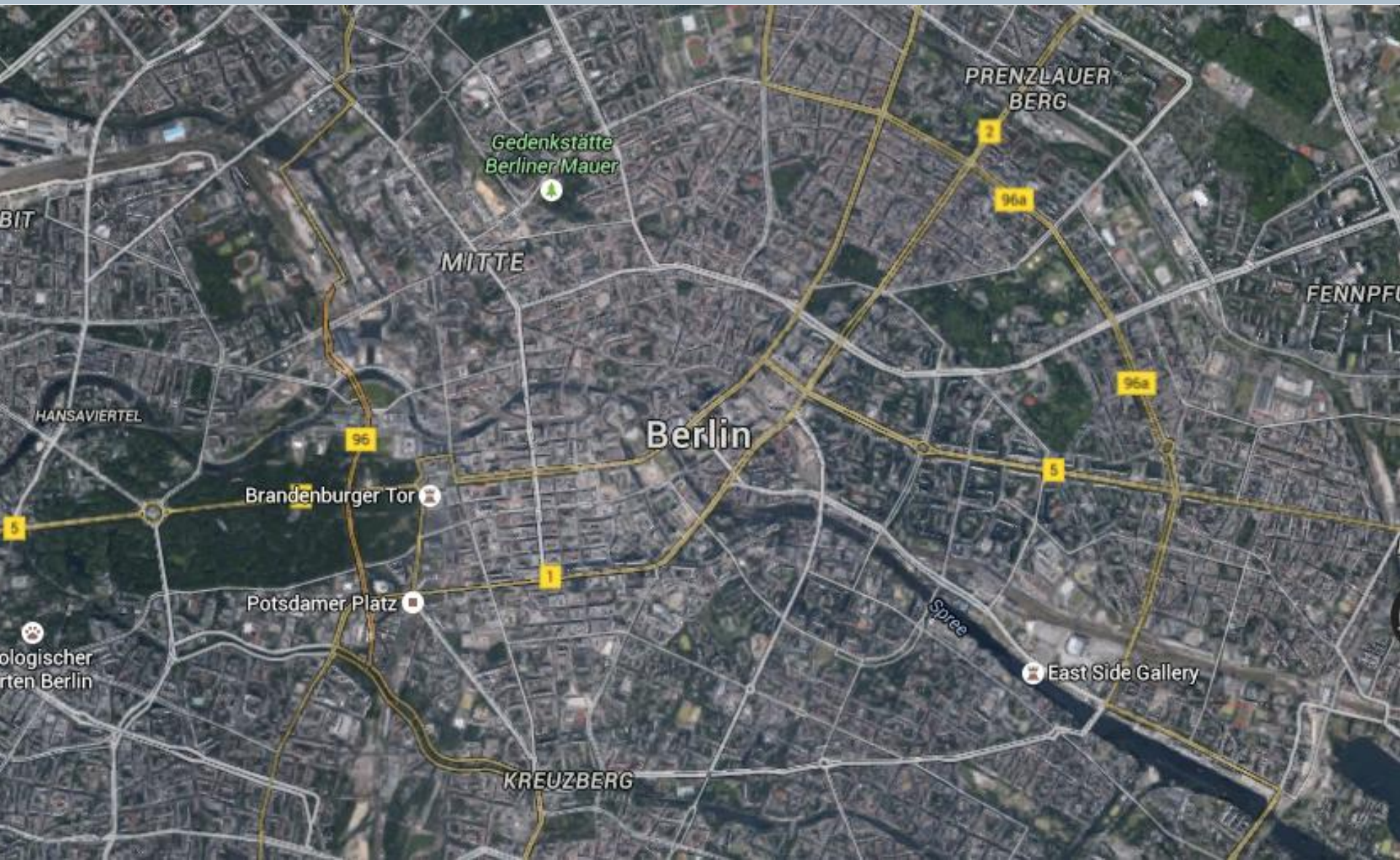
SIEMENS

CORRELATION

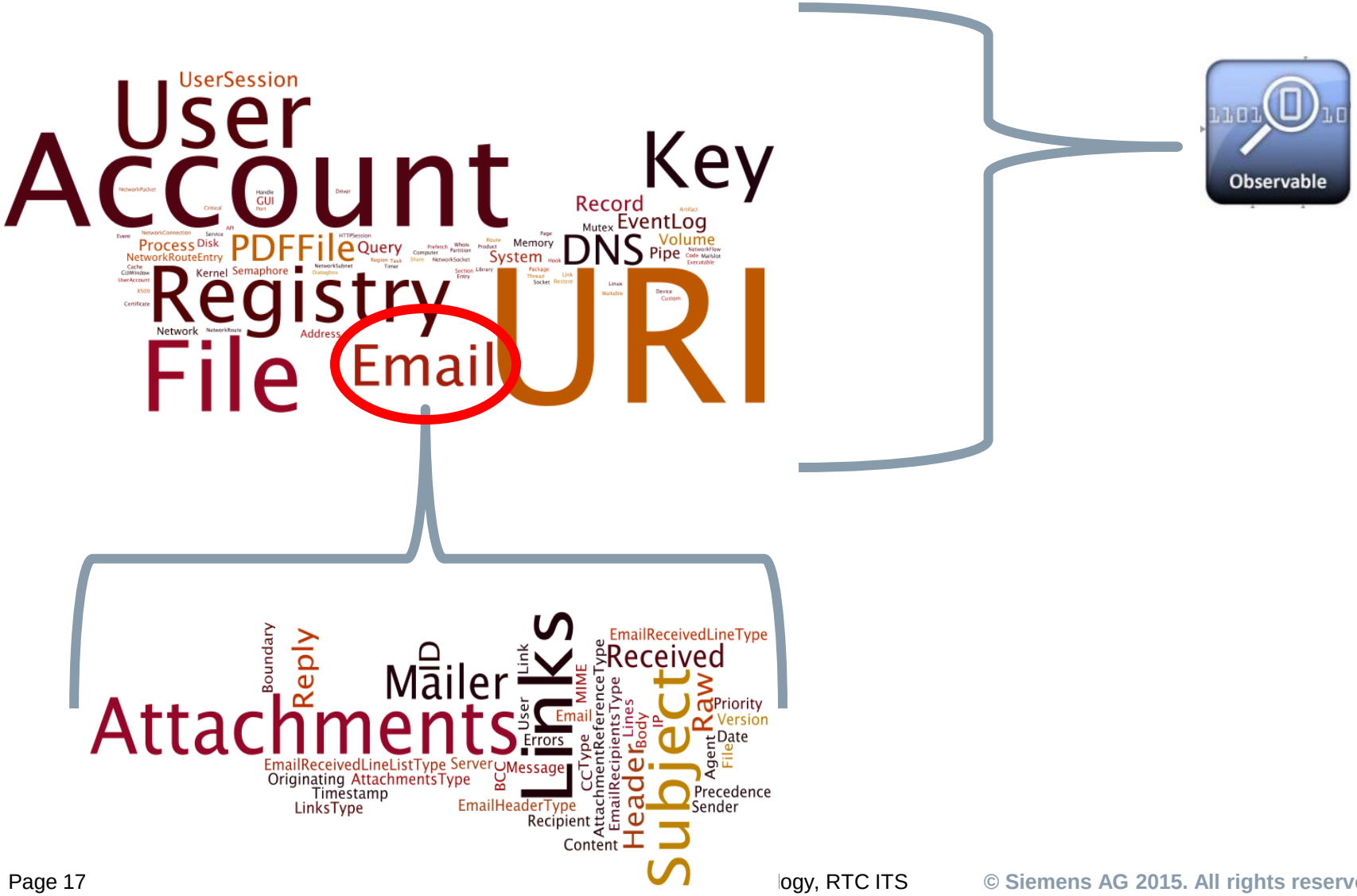
DERIVATION & RATING OF „BASIC“ INDICATORS

SIEMENS

STIX and CybOX from 10,000 feet



Cyber Observables



(Threat) Information

Where we come from:

In shared data, contextual information that supports a precise analysis of what is happening / has happened often was

- missing completely
- or provided
  - rudimentary
  - within a document that is only fit for human consumption (e.g., PDF report)

Threat Intelligence

How confident am I, what stage of the kill-chain are we talking about, …

What kind of activity does this belong to?

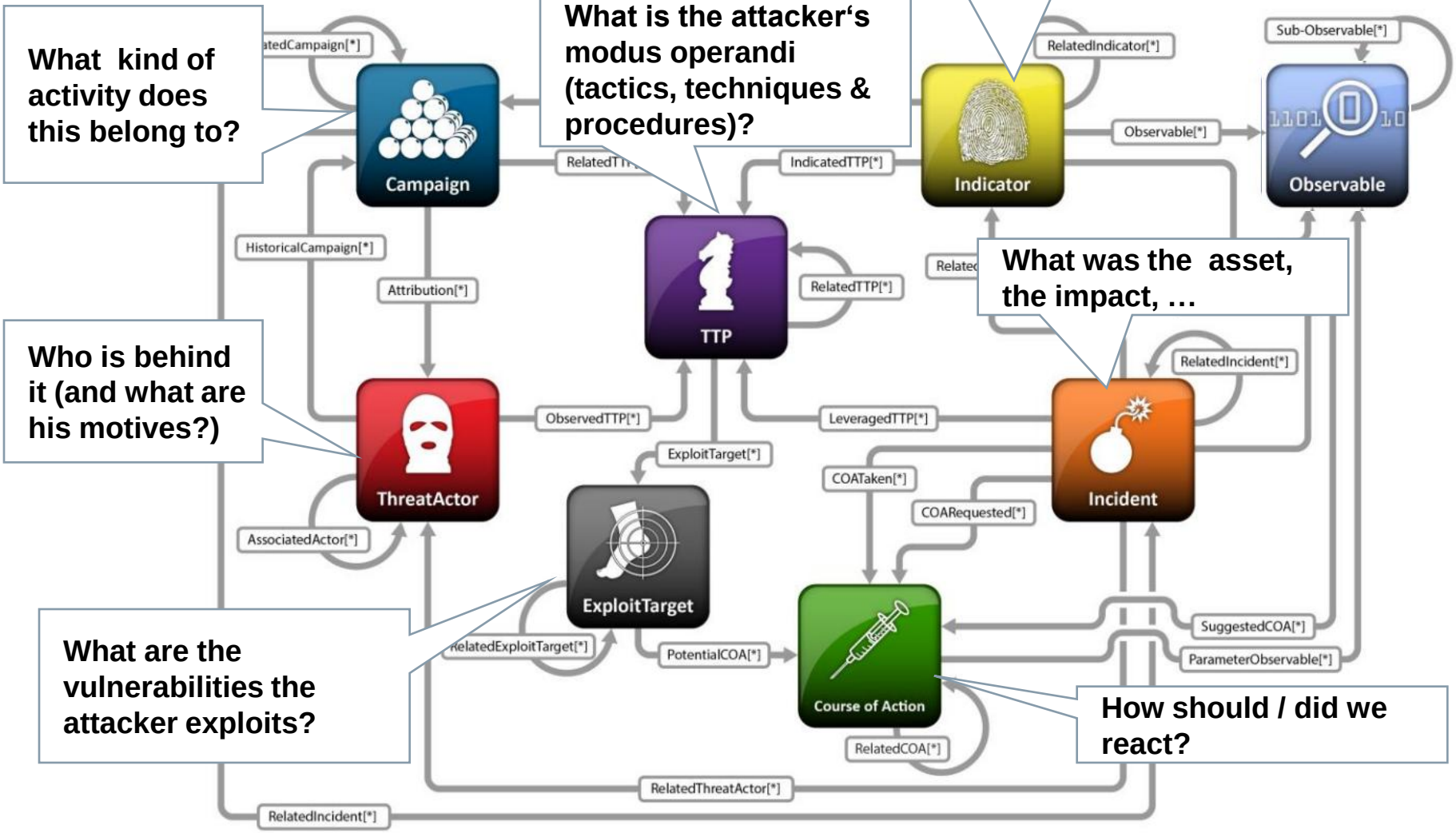
What is the attacker's modus operandi (tactics, techniques & procedures)?

What was the asset, the impact, …

Who is behind it (and what are his motives?)

What are the vulnerabilities the attacker exploits?

How should / did we react?



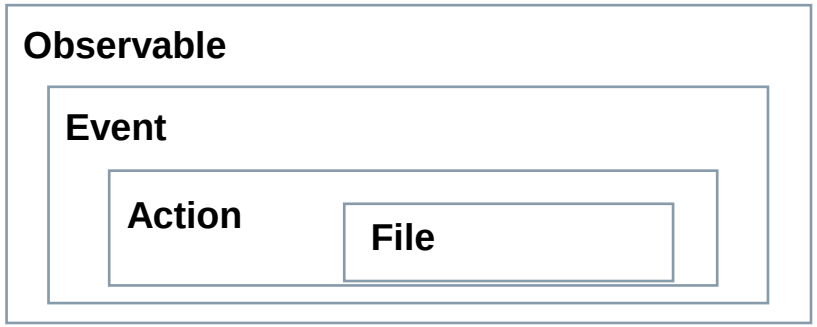
Source: http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf

SIEMENS

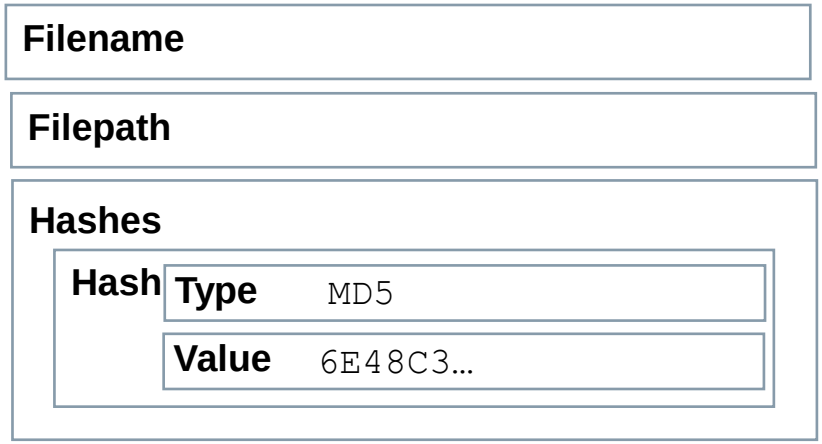
STIX and CybOX seen from 1 inch

Relationships and Facts in STIX/CybOX

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



  - structuring of facts



Example: A CybOX Observable XML Source

SIEMENS


```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
                        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

SIEMENS


```
<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>
```


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

SIEMENS

```
<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>
```

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

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

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

SIEMENS

```
<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
```

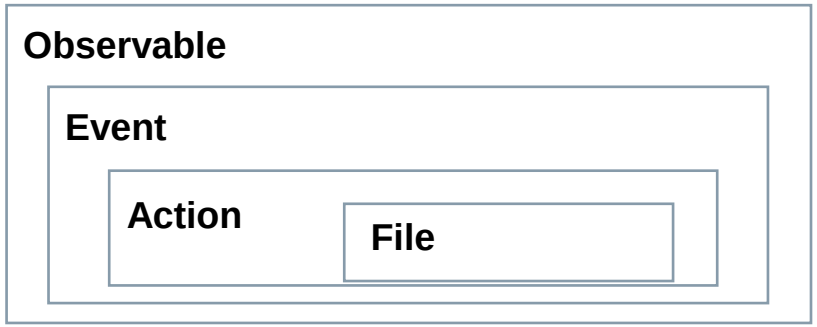
The facts we are really interested into about the observed file are:

- Properties/File_Name = foobar.dll
- Properties/File_Path = C:\Windows\system32
- *Properties/Hashes/Hash/Type = MD5*
- *Properties/Hashes/Hash/Simple_Hash_Value = 6E48C34D74A931EC2CE90ABD7DAC6A*

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

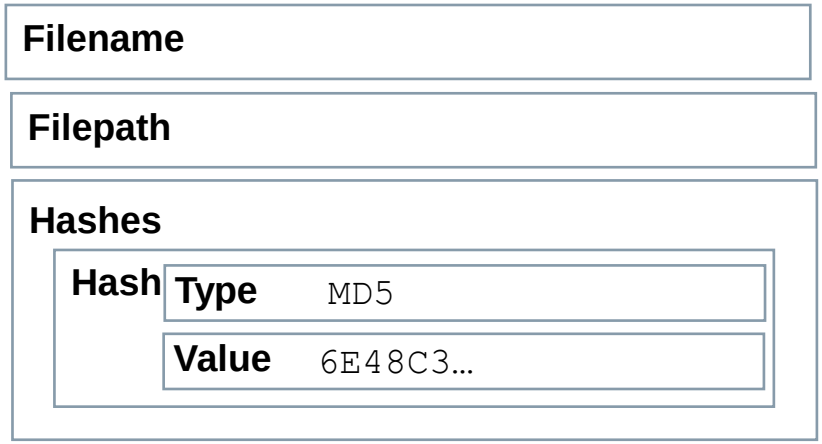
Relationships and Facts in STIX/CybOX

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



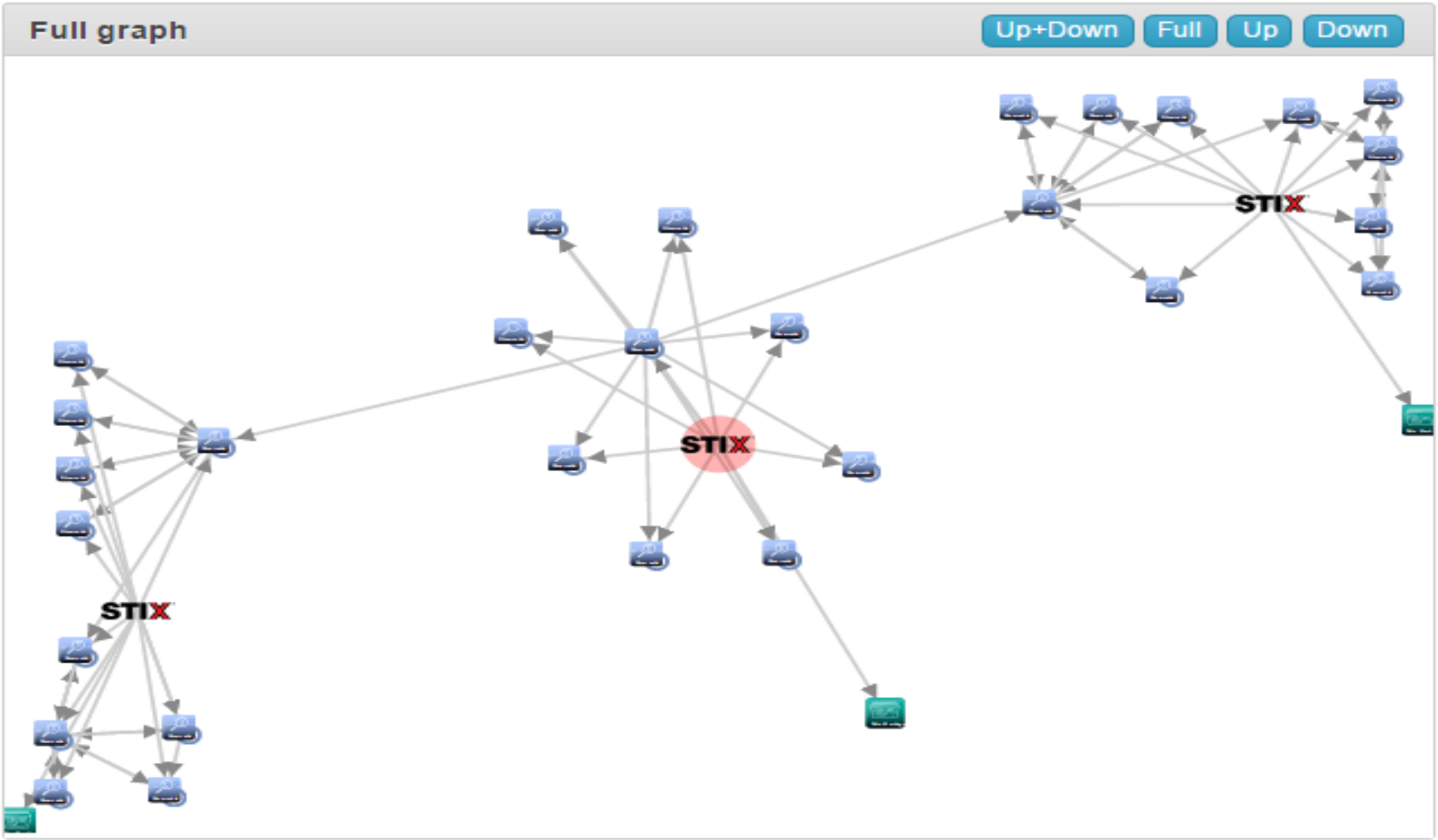
This leads to nodes and edges

  - structuring of facts

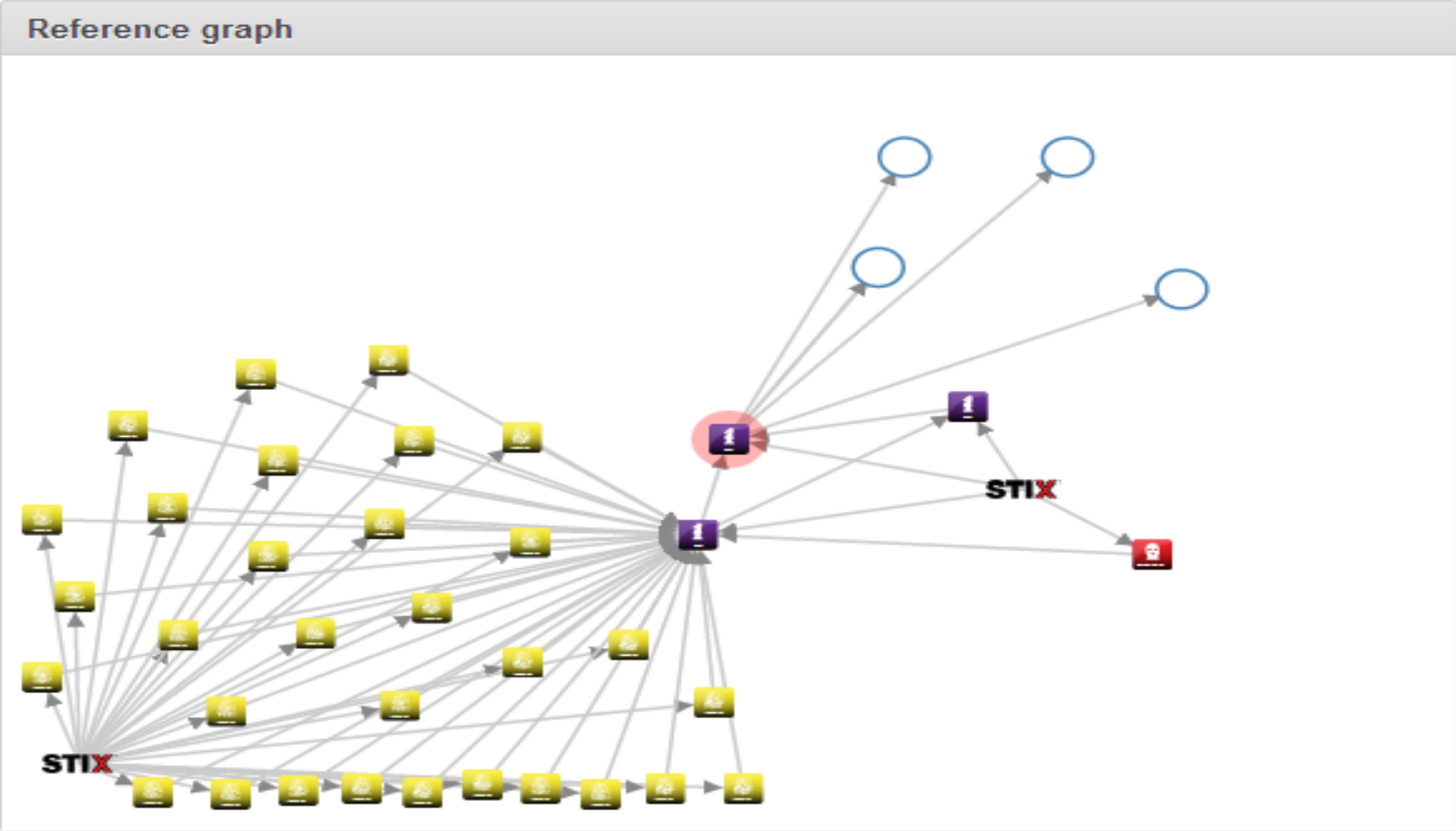


This leads to facts about a node

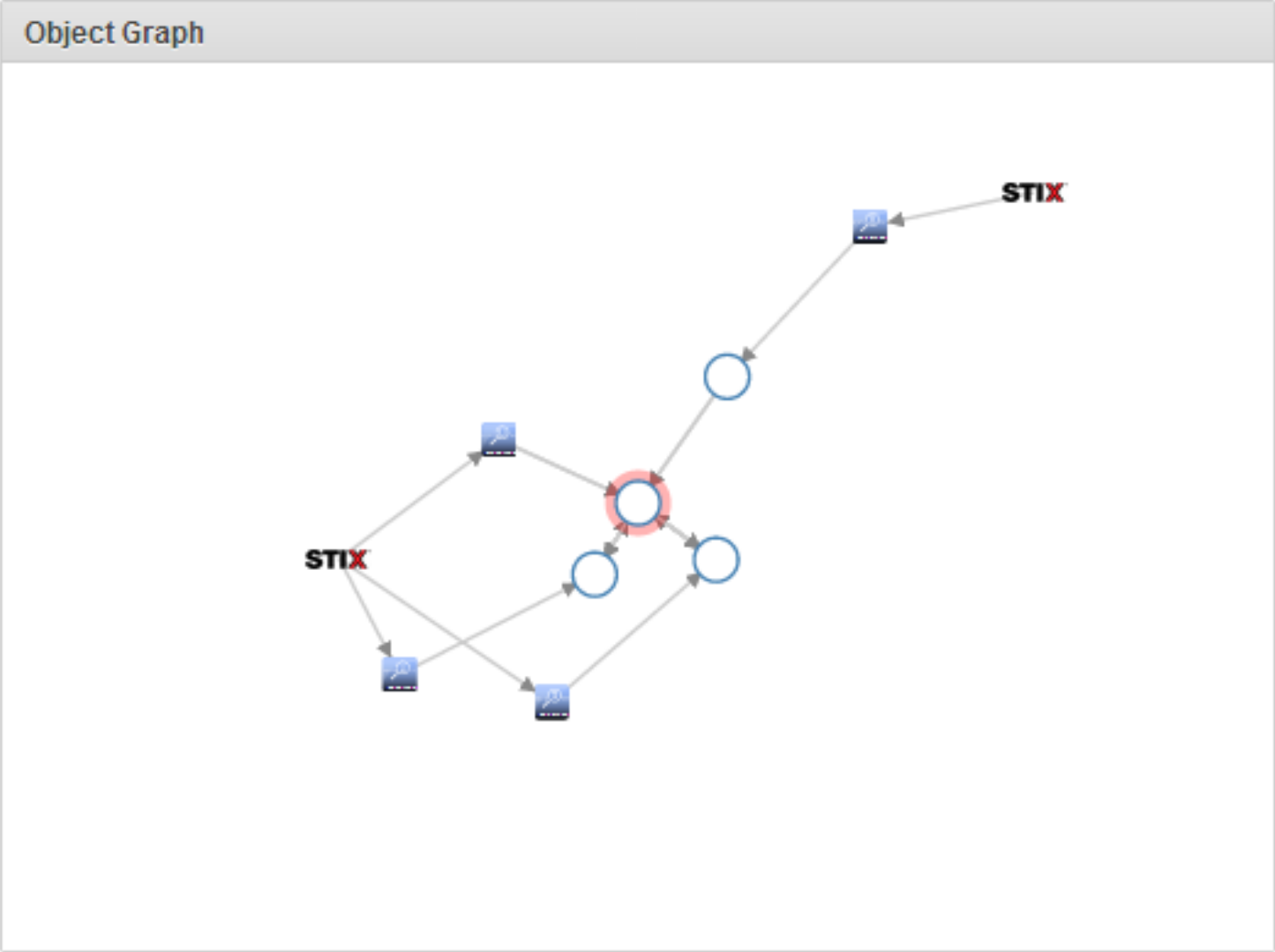
STIX/Cybox Graph: Example



STIX/Cybox Graph: Example



STIX/Cybox Graph: Example



SIEMENS

STIX/CybOX node: example facts

Properties	File_ Name	foobar.dll		
	File_ Path	C:\Windows\system32		
	Hashes	Hash	Type	MD5
			Simple_ Hash_ Value	6E48C348D

Two essential components for working the Cyber Threat Intelligence Miracle based on STIX/CybOX

SIEMENS

CORRELATION

DERIVATION & RATING OF „BASIC“ INDICATORS

Two essential components for working the Cyber Threat Intelligence Miracle

SIEMENS

CORRELATION

SIEMENS

So, how to solve the following?

Subject: [VISP] New documents posted to the VISP portal

The following new reports have been added to our knowledge base:

TLP:AMBER - CSI-4711 Phishing attacks targeting Oil & Gas sector

TLP:AMBER - CSI-0815 Glulx Malware Variant communicating using specific HTTPS POST

We are interested in any additional information that your organization may be able to share regarding this or similar activity. For any questions or feedback related to this report, please contact us at:
1-874-555-0199
VISP@QUOXI.COM

How do we find out whether these two reports have anything in common with our other 18628 reports???

SIEMENS

Object List

18628 results | 1 | 2 | ... | 466

Identifier	Object Timestamp	Import Timestamp	Name
SIEMENS CERT :guid-c295357a-9221-11e3-b24e-005056971bba	2014-02-10 08:00:26 +0100	2014-02-13 15:43:12 +0100	Analysis report: Profoma_Invoice.exe
SIEMENS CERT :guid-c3574502-9221-11e3-a9ba-005056971bba	2014-02-10 08:00:27 +0100	2014-02-13 15:43:37 +0100	Analysis report: Profoma_Invoice.exe
SIEMENS	2014-02-10	2014-02-13	Analysis report: DF8_fdp.exe

So, how to solve the following?

Subject: [VISP] New documents posted to the VISP portal

The following new reports have been added to our knowledge base:

TLP:AMBER - CSI-4711 Phishing attacks targeting Oil & Gas sector

TLP:AMBER - CSI-0815 Glulx Malware Variant communicating using specific HTTPS POST

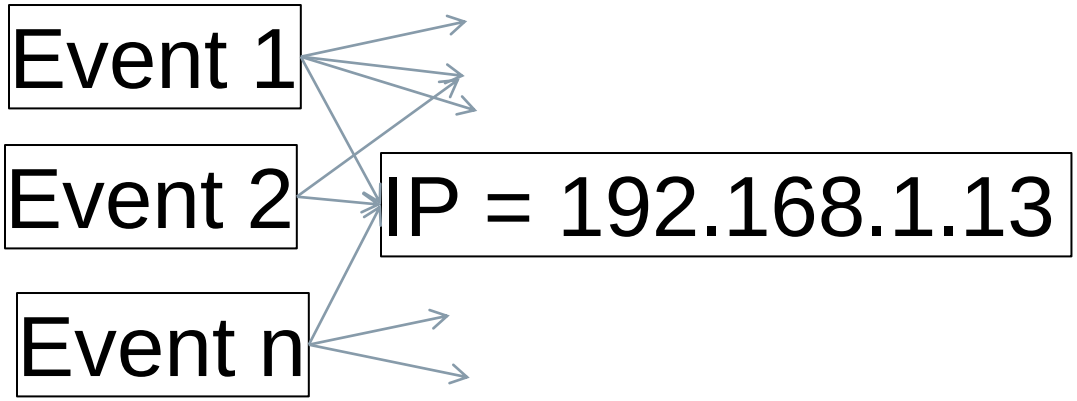
We are interested in any additional information that your organization may be able to share regarding this or similar activity. For any questions or feedback related to this report, please contact us at:
1-874-555-0199
VISP@QUOXI.COM

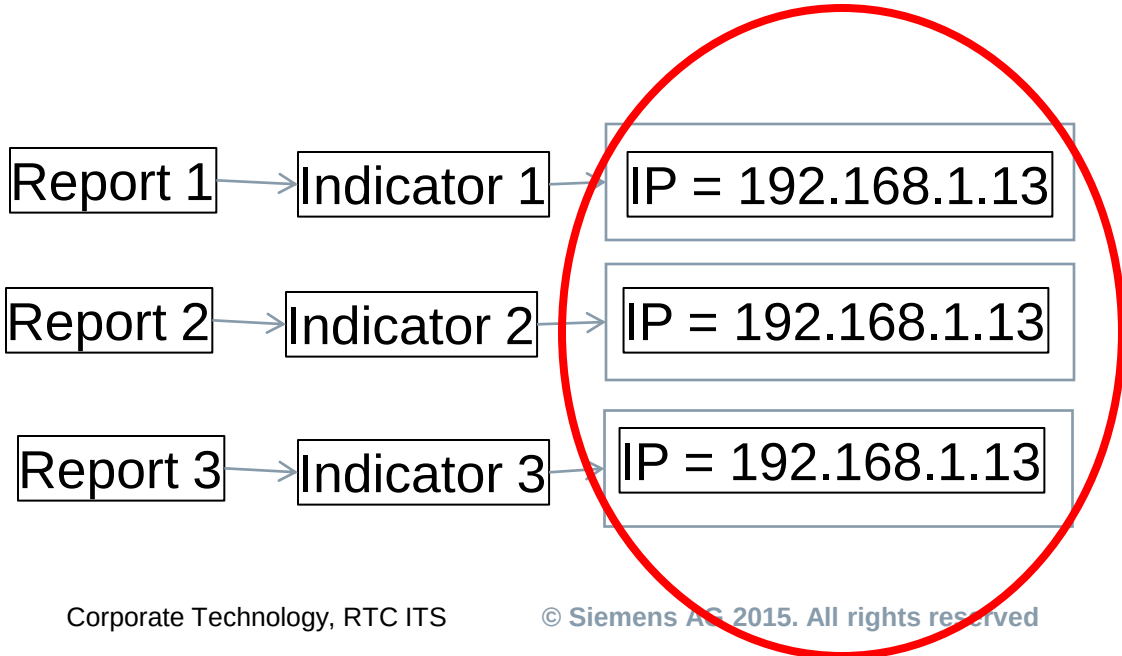
192.168.1.13

STIX/CybOX add a layer of complexity regarding correlation

SIEMENS

E.g.,





A STIX/CybOX-specific motivation for correlation: Same observable information occurs in many different observables

SIEMENS

192.168.1.13

```
<stix:STIX_Package
    xmlns:dingos_author="cert.siemens.com"

<cybox:Observable id="dingos_author:Observable-efa62066-709a-f46c-9e31-a59e30823246">
    <cybox:Object id="dingos_author:Address-efa62066-709a-f46c-9e31-a59e30823246">
        <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr"
            <AddressObj:Address_Value condition="Equals">192.168.1.13</AddressObj:Addr
        </cybox:Properties>
    </cybox:Object>
</cybox:Observable>
```

Munich CERT has observed 192.168.1.13

192.168.1.13

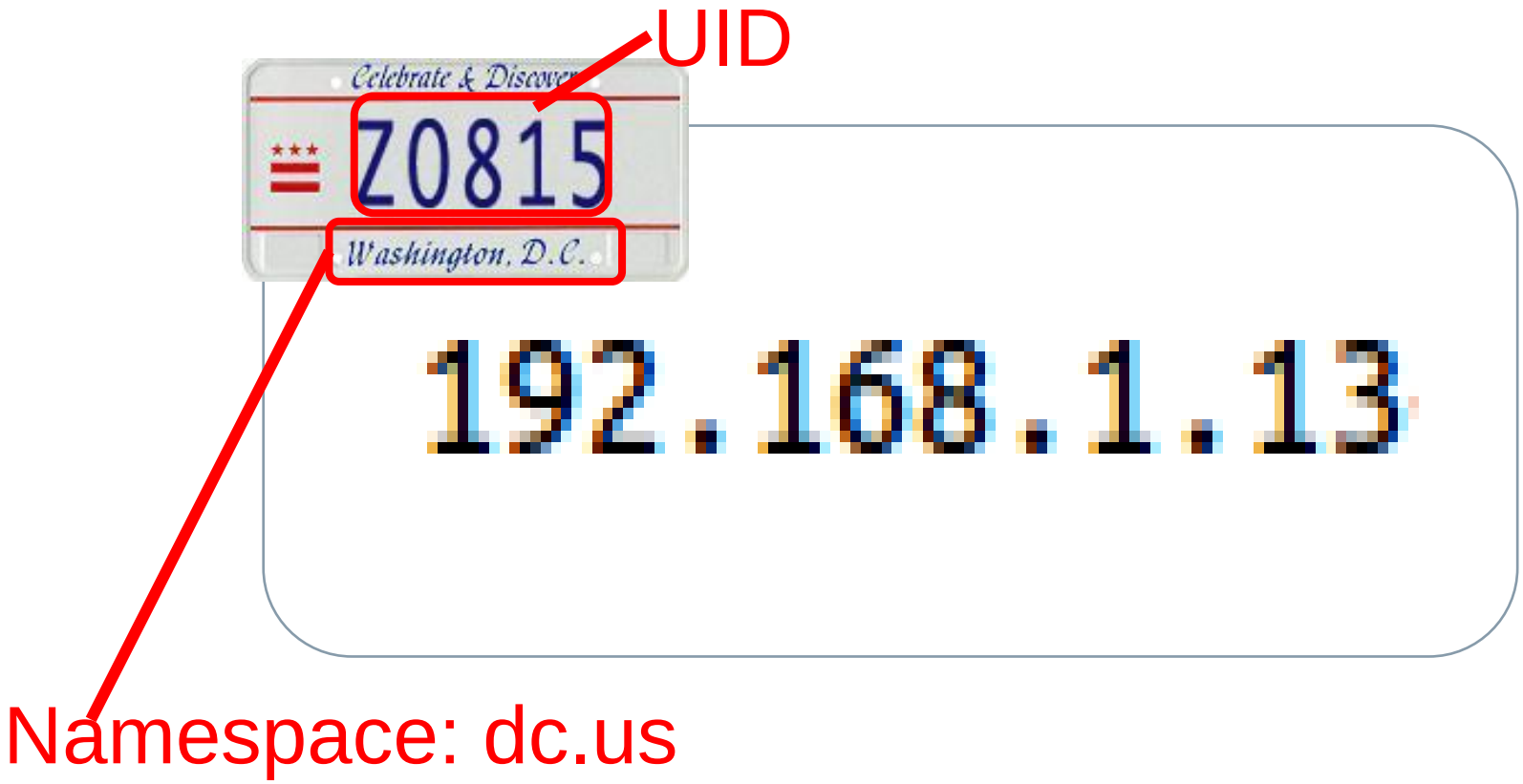
Munich CERT has observed 192.168.1.13

UID

192.168.1.13

Namespace: munich.de

Washington D.C. CERT has observed 192.168.1.13, as well



Hamburg CERT has also observed 192.168.1.13

UID

192.168.1.13

Namespace: hamburg.de

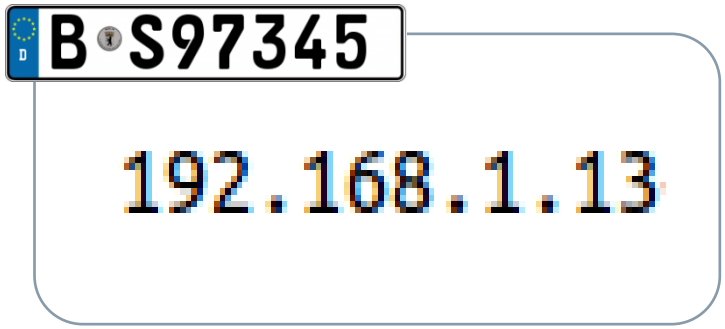
Further, Berlin CERT has observed 192.168.1.13

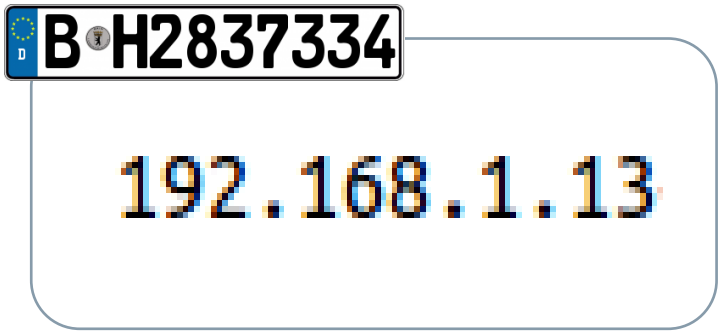
UID

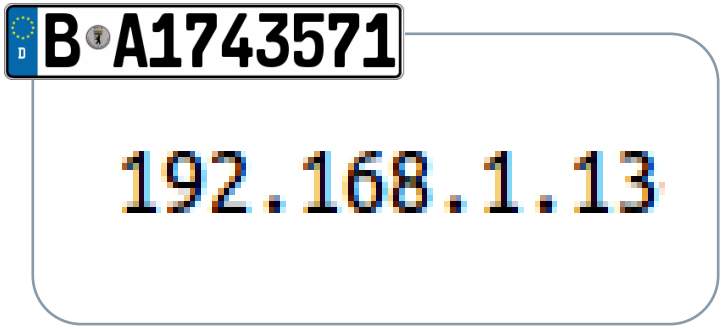
192.168.1.13

Namespace: berlin.de

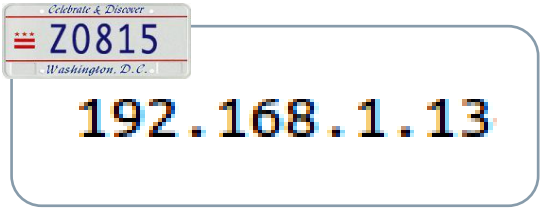
Further, Berlin CERT has a Sandbox that saw 192.168.1.13 in five malware samplesB

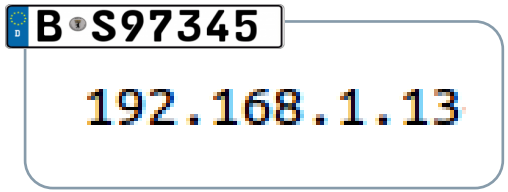


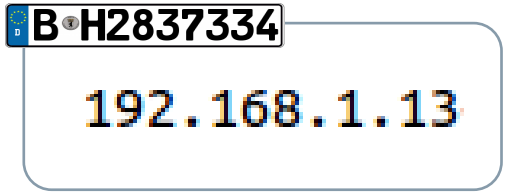


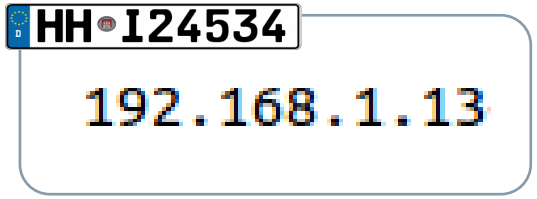


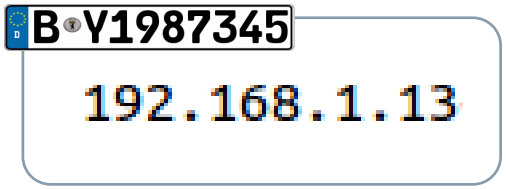
So now we have seven observables that describe 192.168.1.13 …

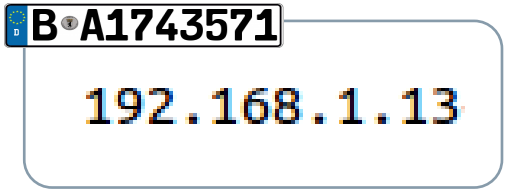


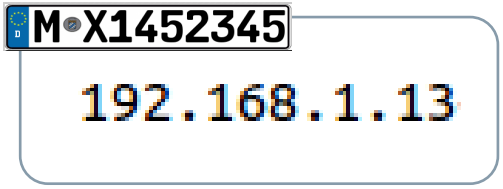






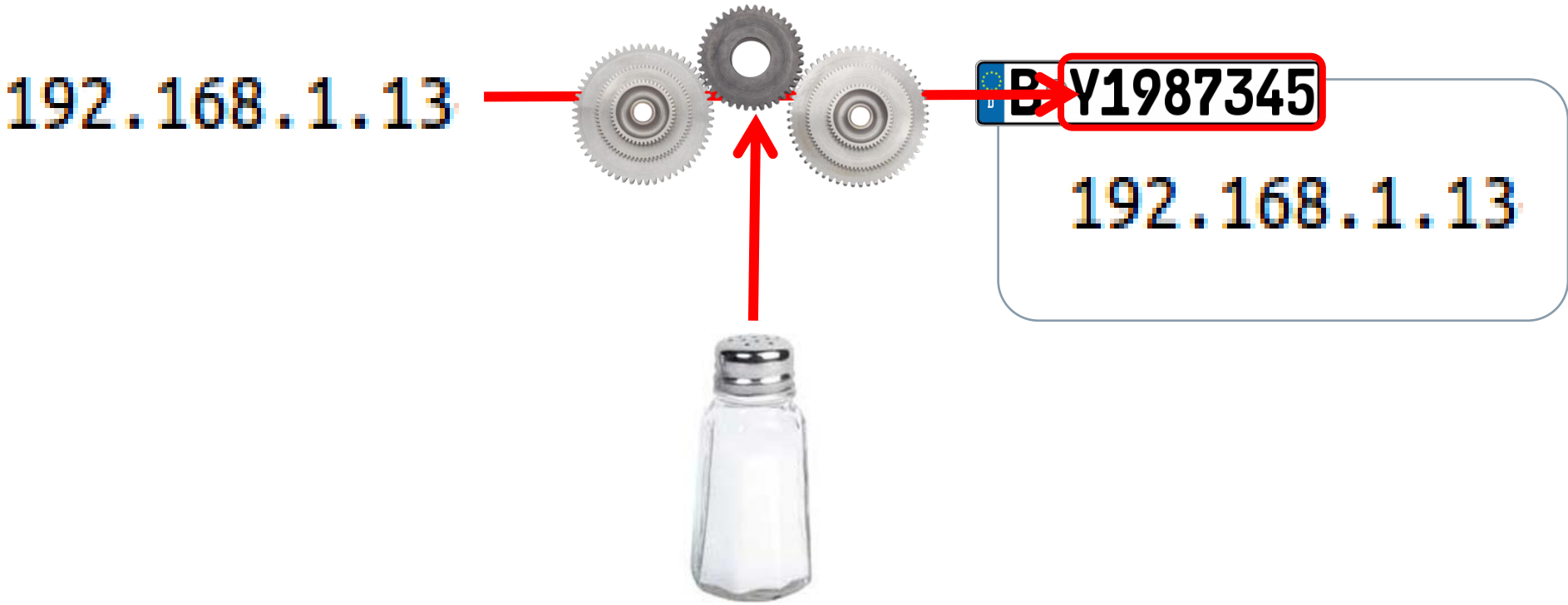




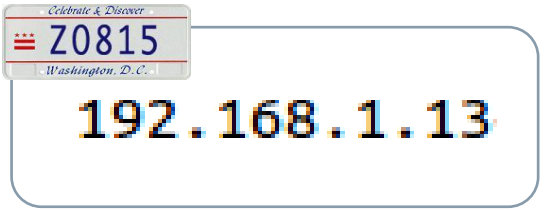


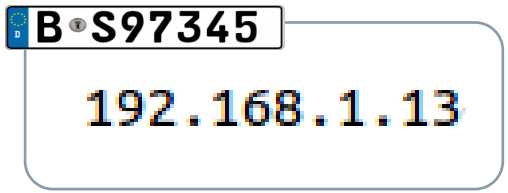
For simple cases, you could avoid using several UIDs via a naming scheme that derives the UID from the primitive observable

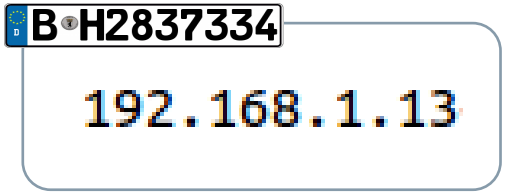
SIEMENS

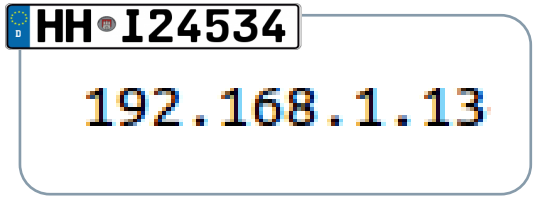


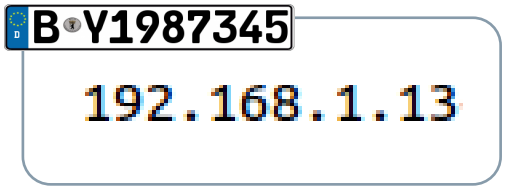
So you can get rid of some observables …

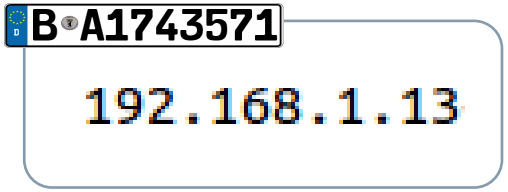


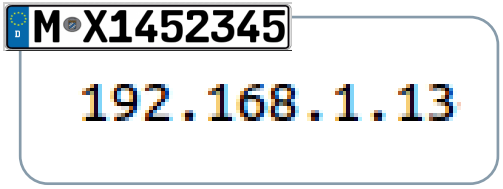








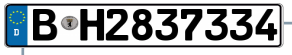




So we might as well forget about deterministic naming schemes…

192.168.1.13

192.168.1.13



192.168.1.13

192.168.1.13

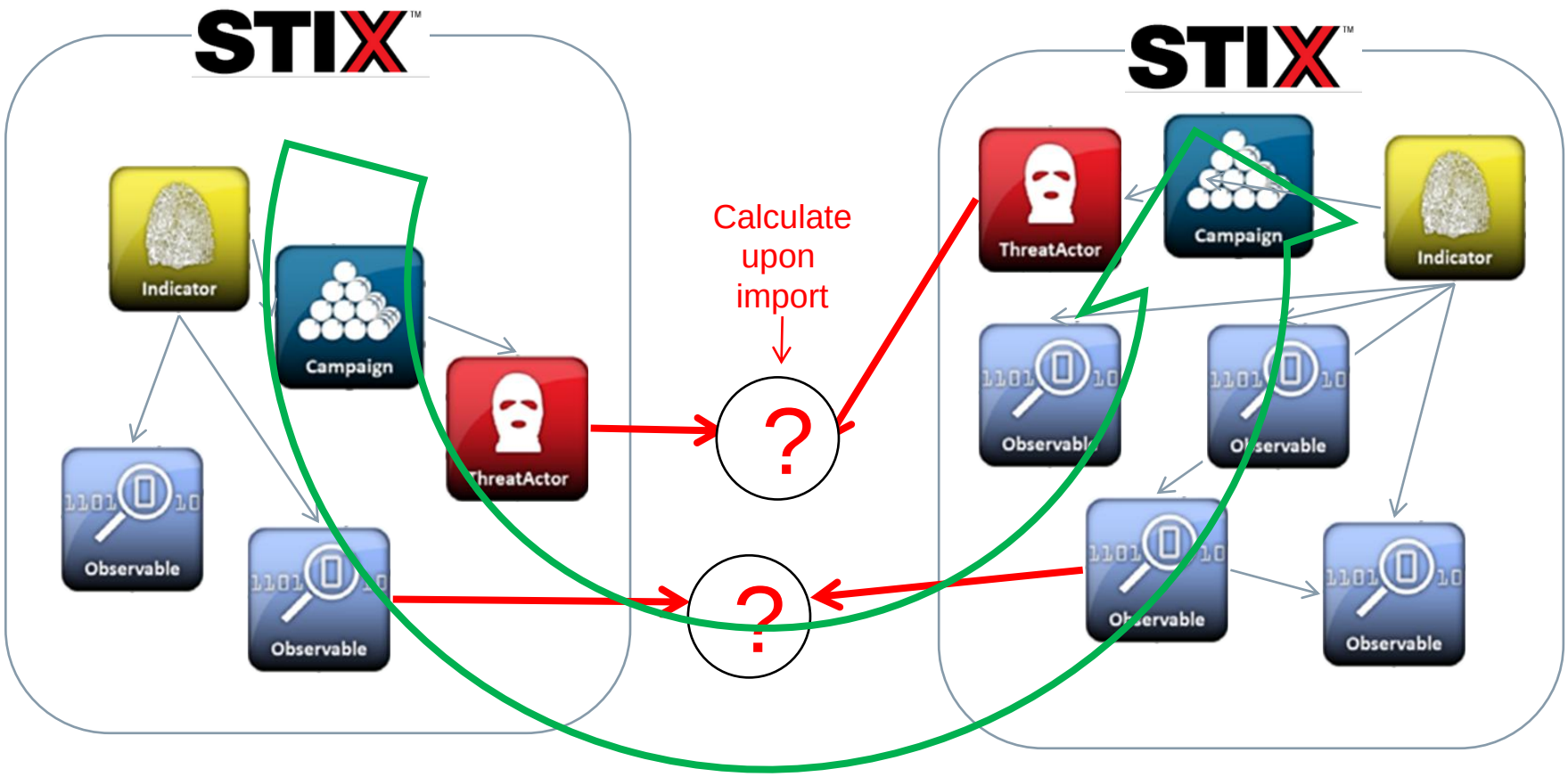
192.168.1.13

192.168.1.13

192.168.1.13

Most promissing approach for correlating reports: find correlations on STIX/CybOX entities and „walk the graph“

SIEMENS



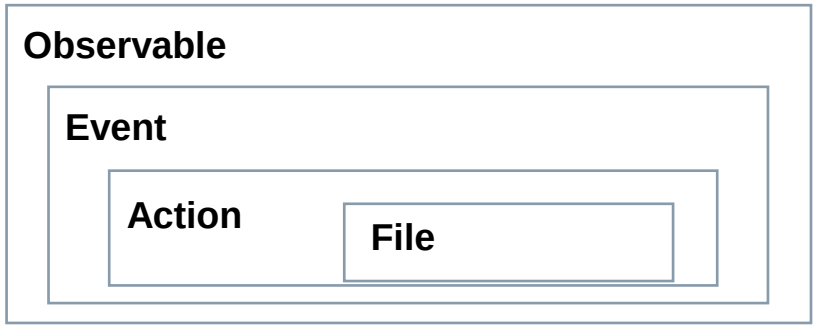
SIEMENS

Some examples of calculating the ?

- **Design of data model**
  - In Mantis, we exploit a feature of the mantis data model for carrying out correlation on “fact level”
- **Use “normalized basic indicators”**
  - see second part of talk
- **Machine learning approaches**
  - Basic idea: calculate “similarity” on STIX/CybOX entities
  - Ongoing research with University of Göttingen
  - Stay tuned

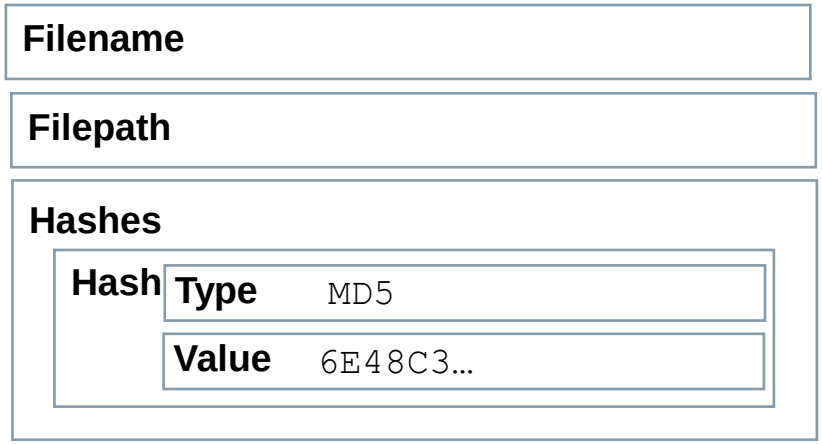
Facts as correlation basis

- 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
Extracting „flat“ facts from hierarchical XML

SIEMENS

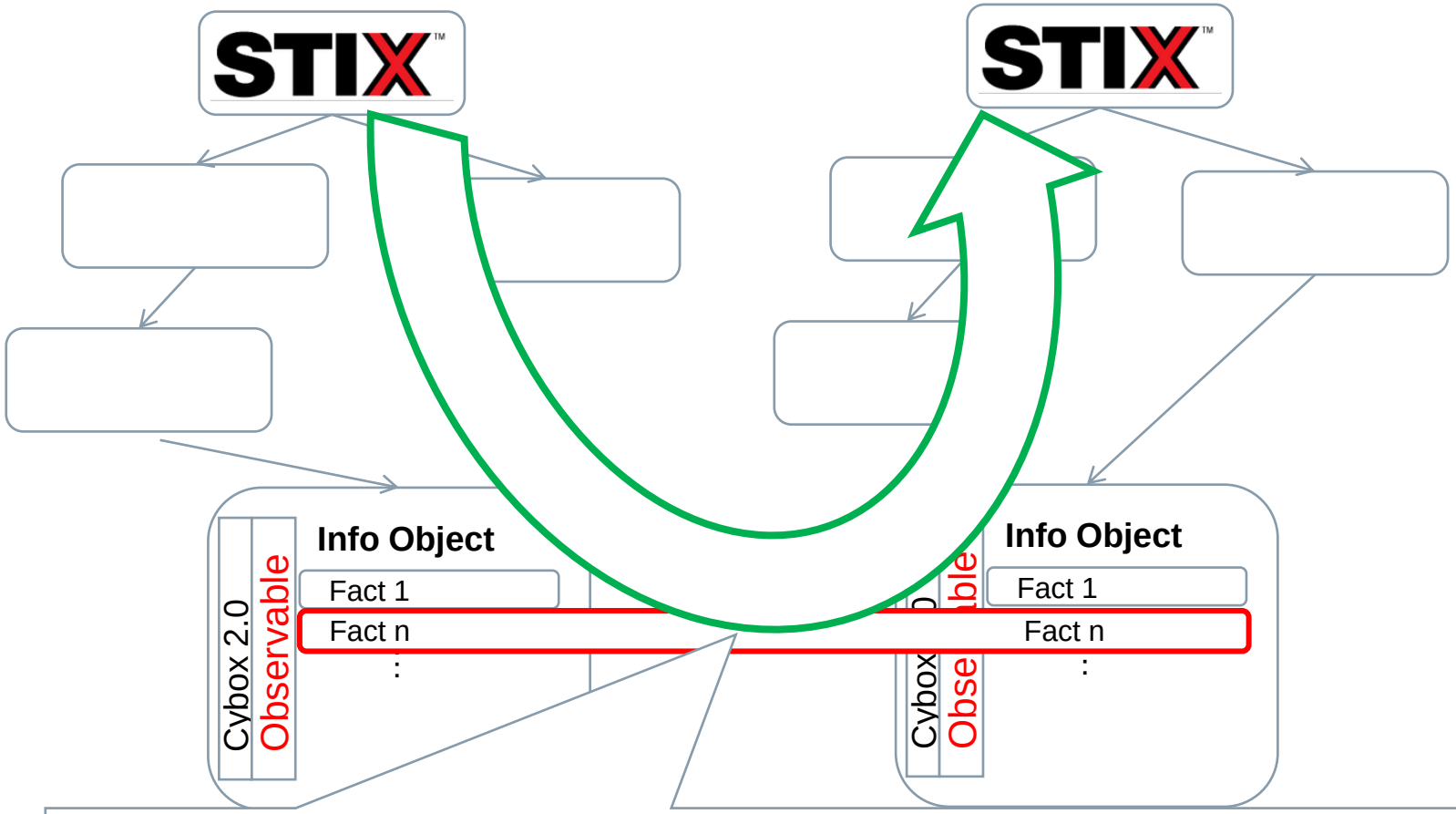
```
<cybox:Observable id="example:Observable-a727a717-1852-4c79-9a16-2f3a8b4632c2">
    <cybox:Event id="example:Event-44578866-b0c5-4551-84dd-0f1f02f8210f">
        <cybox:Actions>
            <cybox:Action id="example:Action-a18a058c-effa-4060-b8be-25e1b1ade75f" action_status="Success"
                          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 = 6E48C34D74A931EC2CE90ABD7DAC6A*

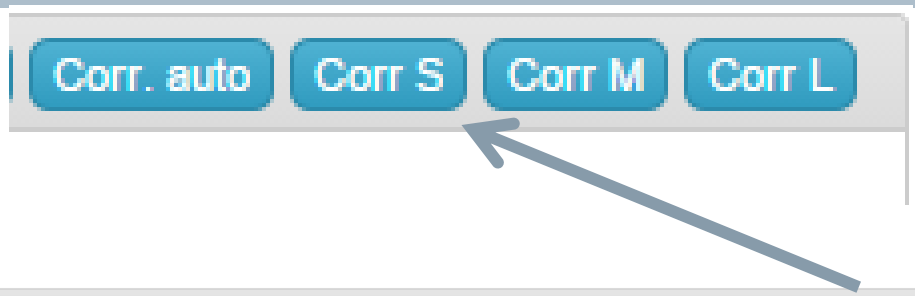
```
</cybox:Observable>
```

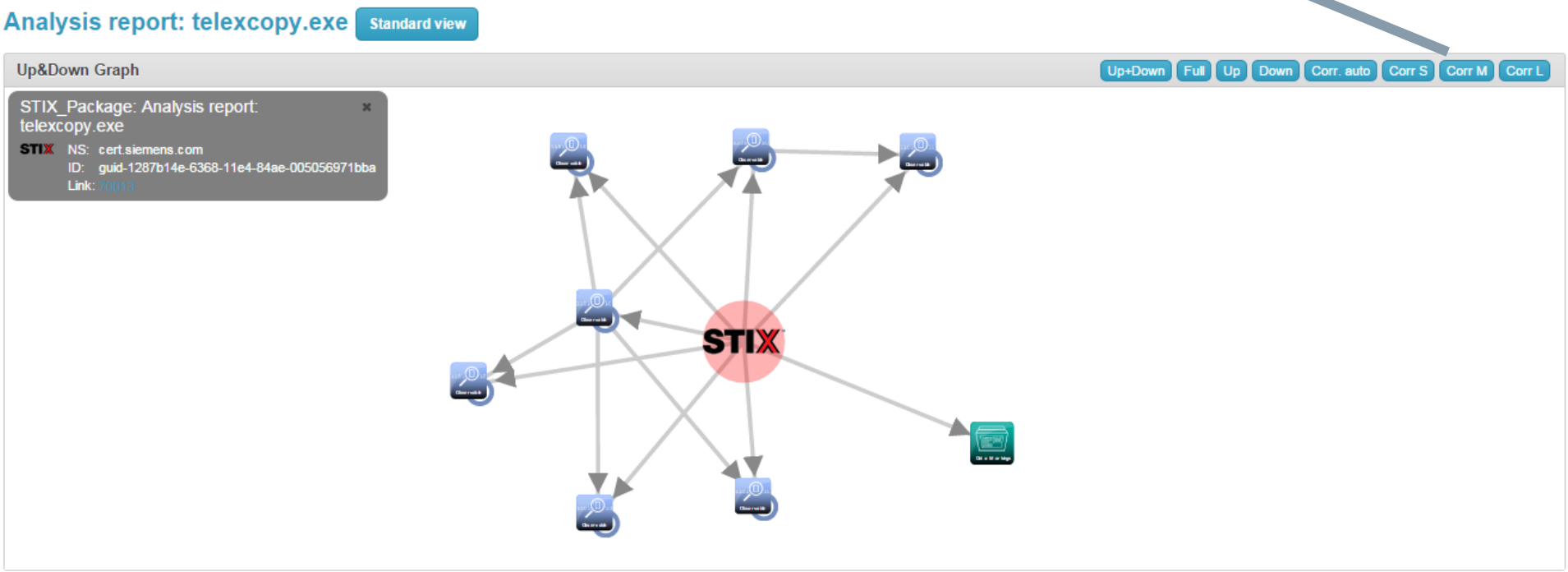
Correlation by Facts using the MANTIS data model



Properties/Hashes/Hash/SimpleHashValue=6E48C3… is shared between two different InfoObjects

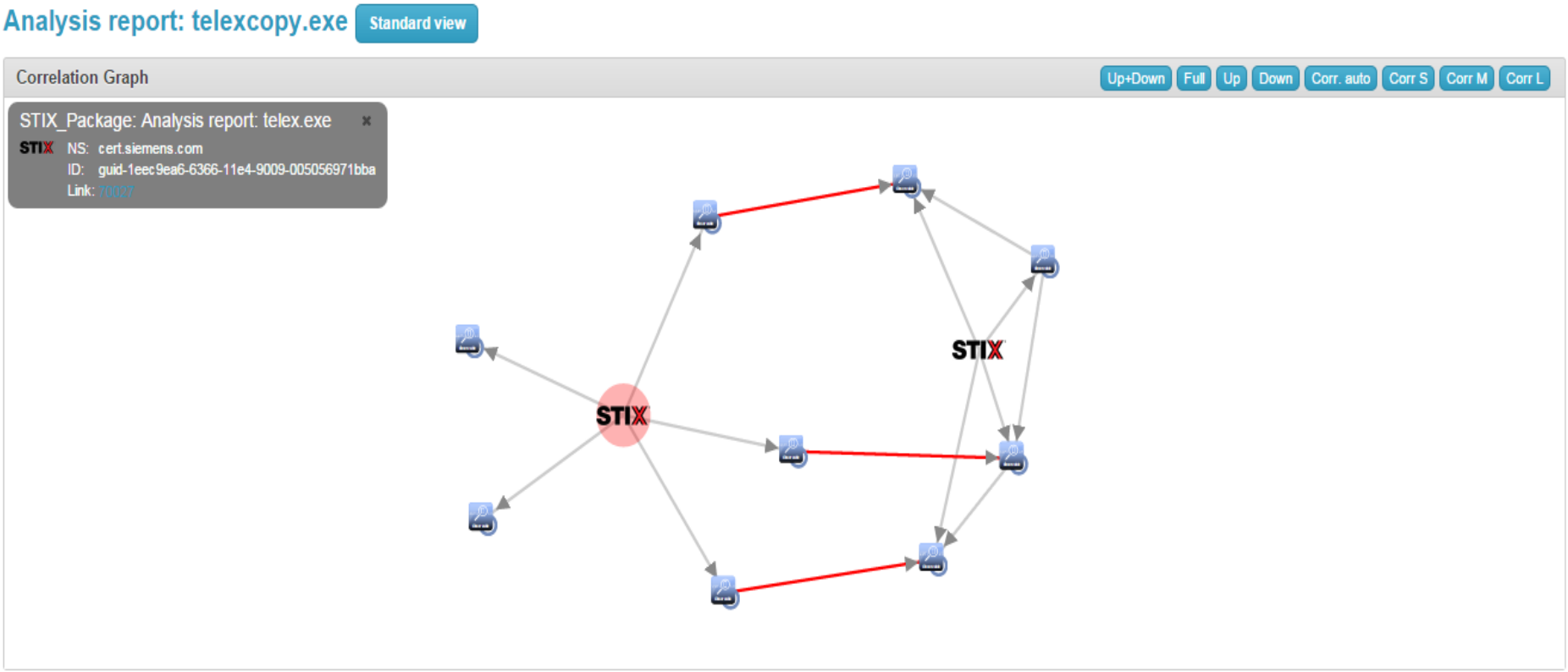
A correlation graph view





Here, the algorithm found correlations between the report in question and another malware report

SIEMENS



Detailed information is provided about what the relationship entails (which common facts were found in which sub objects of the related reports)

SIEMENS

Analysis report: telexcopy.exe

Identifying data			
Identifier	SIEMENS CERT:guid-1287b14e-6368-11e4-84ae-005056971bba	Timestamp	2014-11-03T15:16:28+01:00
Type	stix.mitre.org:STIX_Package 1 (http://stix.mitre.org/stix)	Import Timestamp	2014-12-08T14:15:21.867249+01:00

Correlations (Grouped by correlated fact)			
Properties/File_Name = run.dat	SIEMENS CERT:File-a591c5ca-e406-4941-ac41-6be222c97fe9 run.dat (8 Bytes)	SIEMENS CERT:File-c1b7fab2-c7b1-40b4-8fcc-fb1cc2440451 run.dat (8 Bytes)	SIEMENS CERT:guid-1eec9ea6-6366-11e4-9009-005056971bba Analysis report: telex.exe
Properties/Address_Value = 107.6.122.202	SIEMENS CERT:Address-943d4986-bc0e-486f-aa22-fe64fca60ff5 107.6.122.202 (2 facts)	SIEMENS CERT:Address-bcfbfa88-d552-4414-b1eb-6c6f65586c42 107.6.122.202 (2 facts)	SIEMENS CERT:guid-1eec9ea6-6366-11e4-9009-005056971bba Analysis report: telex.exe
Properties/Value = blisterednano.zapto.org	SIEMENS CERT:URI-343e630b-c053-4718-84a4-3176e08f6882 blisterednano.zapto.org (3 facts)	SIEMENS CERT:URI-35dfce86-af6b-4918-a5c2-18609b42de3b blisterednano.zapto.org (3 facts)	SIEMENS CERT:guid-1eec9ea6-6366-11e4-9009-005056971bba Analysis report: telex.exe

Detailed information is provided about what the relationship entails (which common facts were found in which sub objects of the related reports)

SIEMENS

Analysis report: telexcopy.exe

Identifying data

Identifier	SIEMENS CERT .guid-1287b14e-6368-11e4-84ae-005056971bba	Timestamp	2014-11-03T15:16:28+01:00
Type	stix.mitre.org:STIX_Package 1 (http://stix.mitre.org/stix)	Import Timestamp	2014-12-08T14:15:21.867249+01:00

Correlations (Grouped by correlated fact)

Properties/File_Name = run.dat	SIEMENS CERT :File-a591c5ca-e406-4941-ac41-6be222c97fe9 run.dat (8 Bytes)	SIEMENS CERT :File-c1b7fab2-c7b1-40b4-8fcc-fb1cc2440451 run.dat (8 Bytes)	SIEMENS CERT :guid-1eec9ea6-6366-11e4-9009-005056971bba Analysis report: telex.exe
Properties/Address_Va	SIEMENS CERT :Address-	SIEMENS CERT :Address-	SIEMENS CERT :guid-1eec9ea6-6366-11e4-
Properties			

The fact „**`Properties/File_Name = run.dat`**“ was found in descendant object „*such and such*“ of STIX Package „*Analysis report. Telexcopy.exe”* – the same fact is present in object „*so and so*“, which is a descendant of STIX Package „*Analysis report : telex.exe*“

In this case, the name of the malware binary already hinted at a possible relation, but for the really interesting cases, this is not the case

SIEMENS

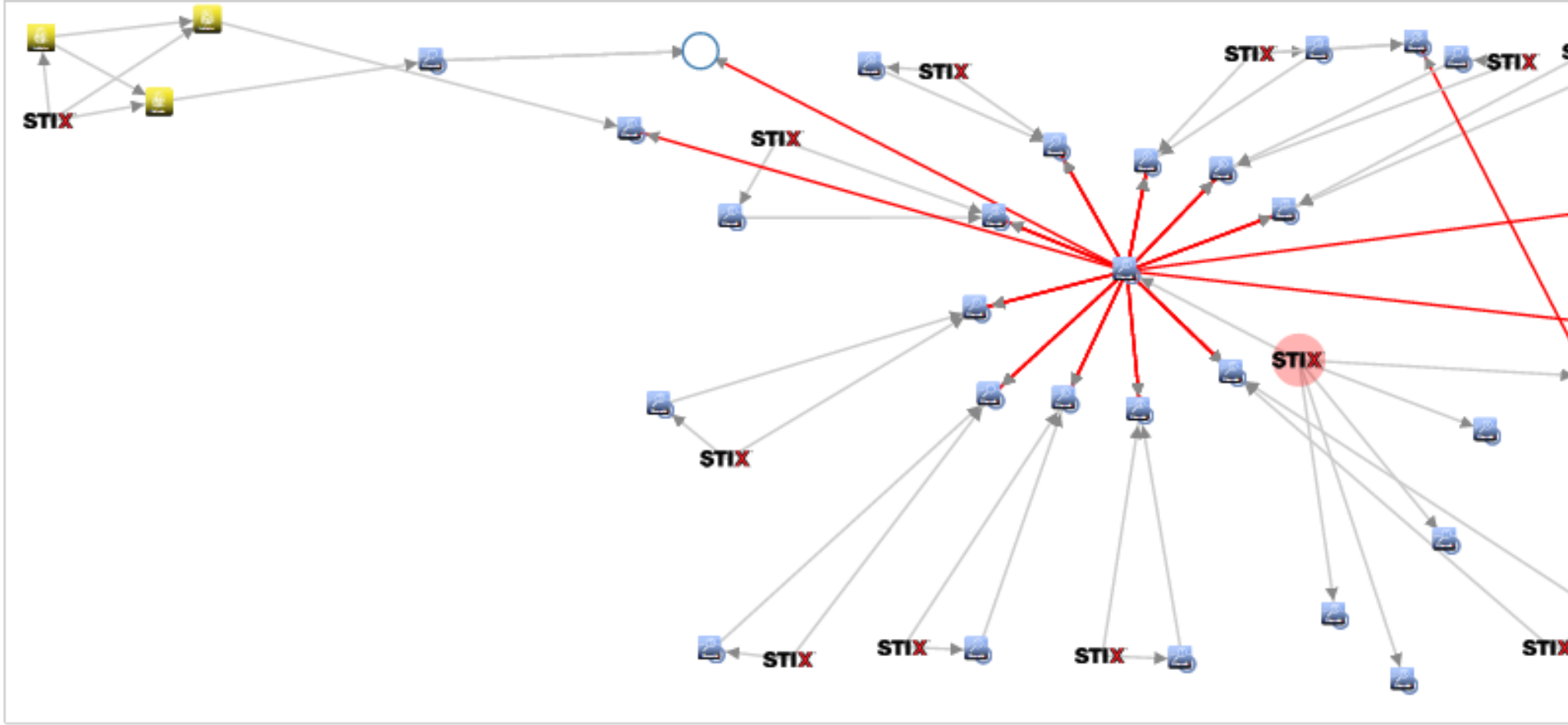
Name	Object Type
Analysis report: Order_Demands.exe	STIX_Package
Analysis report: telexcopy.exe	STIX_Package
Analysis report: dogovor_po_zakazu_76888677.scr	STIX_Package
Analysis report: telex.exe	STIX_Package
Analysis report: Ihre___Rechnung___04.11.2014___PDF.exe	STIX_Package
Analysis report: Visualizar-boleto-fatura-atrasada-10-2014-104921305948000200047.cpl	STIX_Package
Analysis report: PI-64539ENDB.exe	STIX_Package
Analysis report: Remittance_copy.exe	STIX_Package

Possible pitfalls

Analysis report: Order_Demands.exe

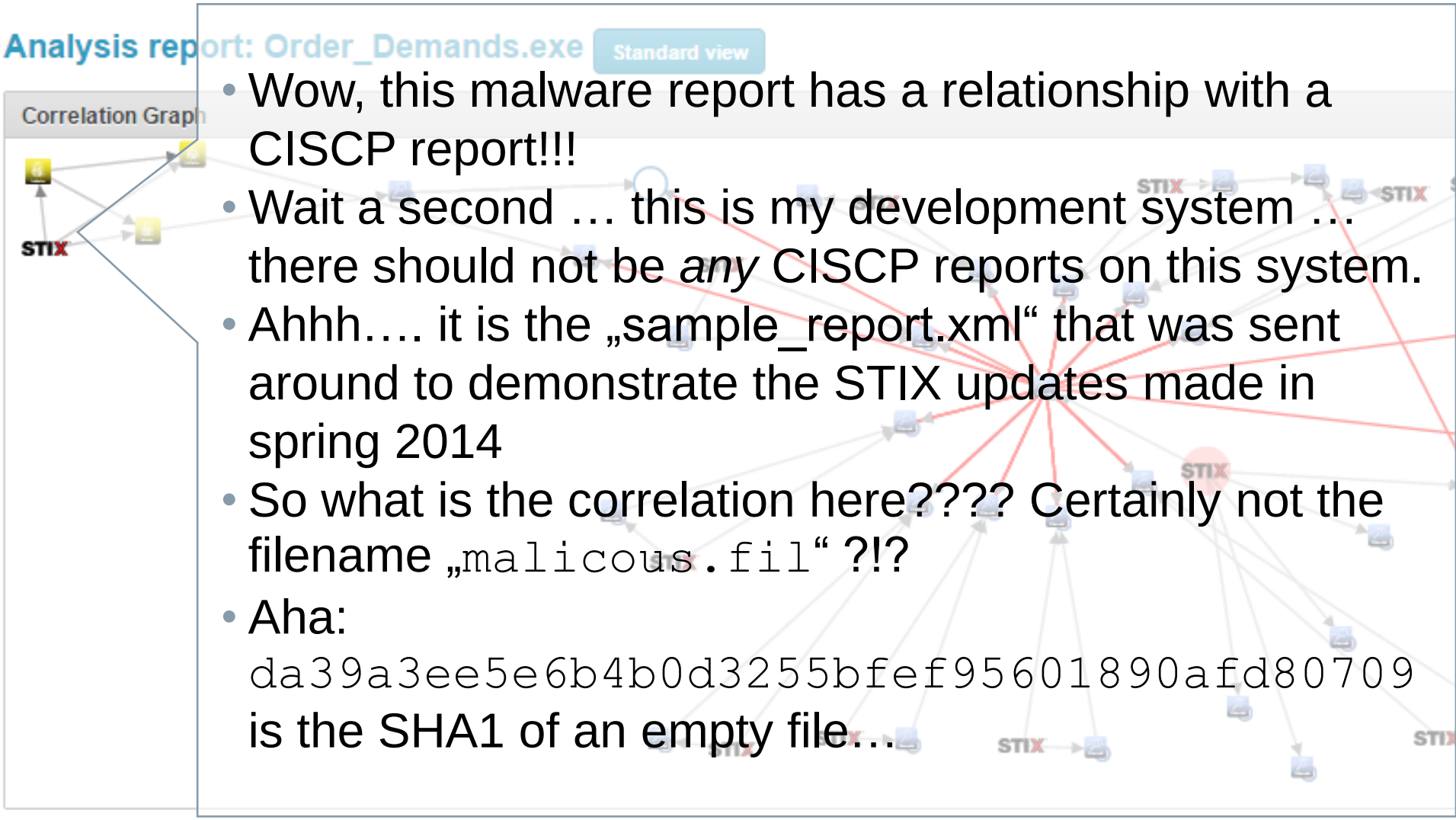
Standard view

Correlation Graph



SIEMENS

Possible pitfalls



- Wow, this malware report has a relationship with a CISCP report!!!
- Wait a second … this is my development system … there should not be *any* CISCP reports on this system.
- Ahhh…. it is the „sample_report.xml“ that was sent around to demonstrate the STIX updates made in spring 2014
- So what is the correlation here???? Certainly not the filename „`malicous.fil`“ ?!?
- Aha: `da39a3ee5e6b4b0d3255bfef95601890afd80709` is the SHA1 of an empty file…

SIEMENS

DERIVATION & RATING OF BASIC INDICATORS

SIEMENS

DERIVATION & RATING OF BASIC INDICATORS

SIEMENS

A rather easy, 1:1 mapping

```
<cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
    <AddressObj:Address_Value condition="Equals">192.168.1.13</AddressObj:Addres
</cybox:Properties>
```

```
AddressObj:AddressObjectType" category="ipv4-addr">
e condition="Equals">192.168.1.13</AddressObj:Address_
```

Type	Subtype	Value
IP	v4	192.168.1.13

SIEMENS

A file object may contain several basic indicators …

```
ox:Properties xsi:type="FileObj:FileObjectType">
<FileObj:File_Name>a cunning plan.exe</FileObj:File_Name>
<FileObj:File_Extension>exe</FileObj:File_Extension>
<FileObj:Size_In_Bytes>10562</FileObj:Size_In_Bytes>
<FileObj:Hashes>
    <cyboxCommon:Hash>
        <cyboxCommon:Type condition="Equals" xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5</cy
        <cyboxCommon:Simple_Hash_Value condition="Equals">cca0baf09c0e8e4d50075425606105ab</c
    </cyboxCommon:Hash>
    <cyboxCommon:Hash>
        <cyboxCommon:Type condition="Equals" xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA1</c
        <cyboxCommon:Simple_Hash_Value condition="Equals">9f5fc5eafc2e7679a15d4810dd4aa326994
    </cyboxCommon:Hash>
    <cyboxCommon:Hash>
        <cyboxCommon:Type condition="Equals" xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256<
        <cyboxCommon:Simple_Hash_Value condition="Equals">ff947cbc61cafea4499e146b14957684cb1
    </cyboxCommon:Hash>
</FileObj:Hashes>
box:Properties>
```

SIEMENS

A file object may contain several basic indicators …

Type	Subtype	Value
Hash	SHA256	ff947cbc61cafea4499e146b14
Hash	SHA1	9f5fc5eafc2e7679a15d4810dd
Hash	MD5	cca0baf09c0e8e4d500754256
Filename		a_cunning_plan.exe

SIEMENS

Another example: an observed email

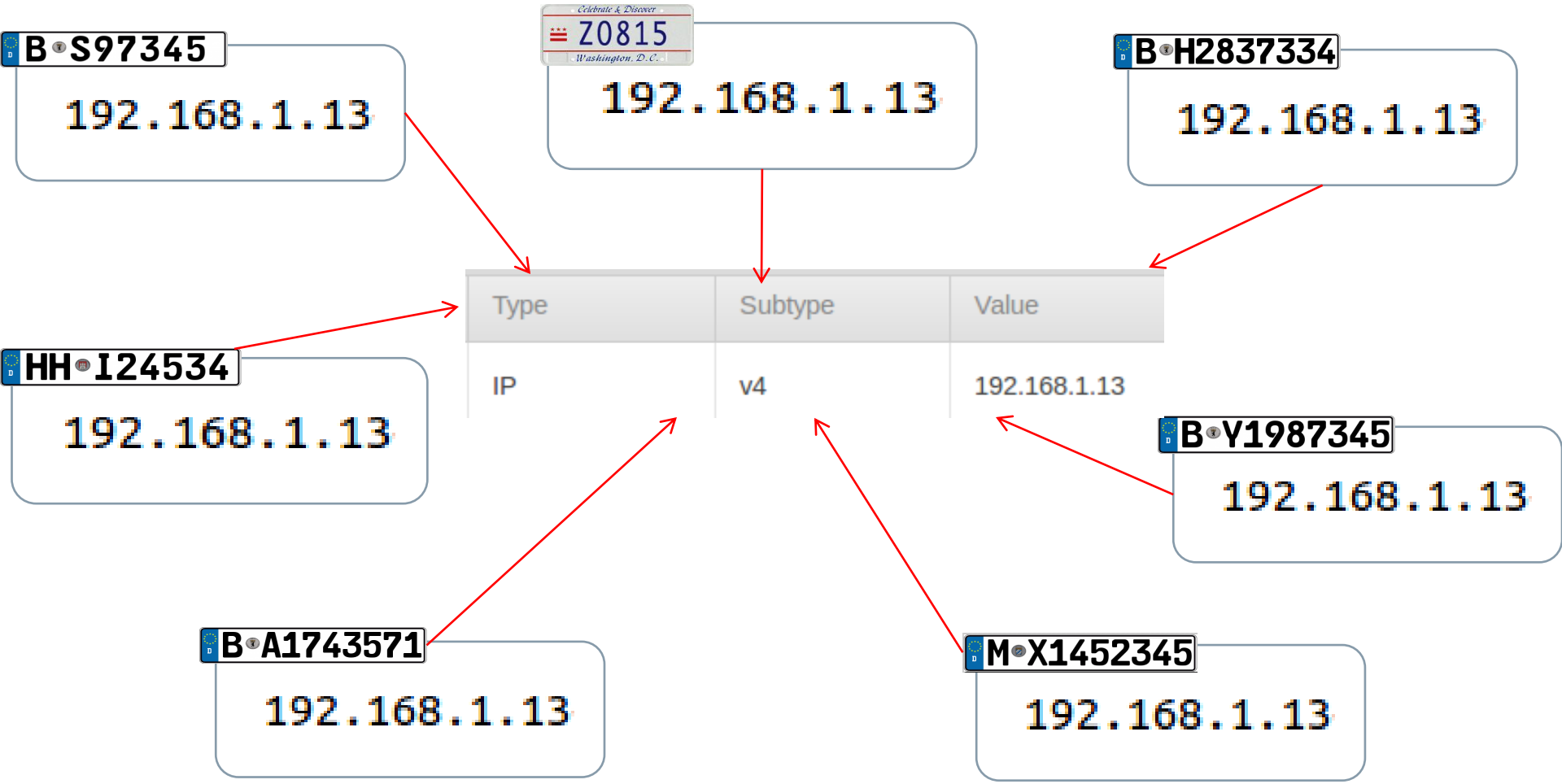
```
<cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
    <EmailMessageObj:Header>
        <EmailMessageObj:To>
            <EmailMessageObj:Recipient xsi:type="AddressObj:AddressObjectType" categ
                <AddressObj:Address_Value>an.innocent.victim@my-organization.com</Ad
            </EmailMessageObj:Recipient>
        </EmailMessageObj:To>
        <EmailMessageObj:From xsi:type="AddressObj:AddressObjectType" category="e-ma
            <AddressObj:Address_Value>professor.moriarty@criminal-mastermind.com</Ad
        </EmailMessageObj:From>
        <EmailMessageObj:Subject>An offer you really cannot refuse</EmailMessageObj:
        <EmailMessageObj:In_Reply_To>4711</EmailMessageObj:In_Reply_To>
        <EmailMessageObj:Date>2015-04-01T11:11:11</EmailMessageObj:Date>
    </EmailMessageObj:Header>
</cybox:Properties>
```

SIEMENS

Another example: an observed email

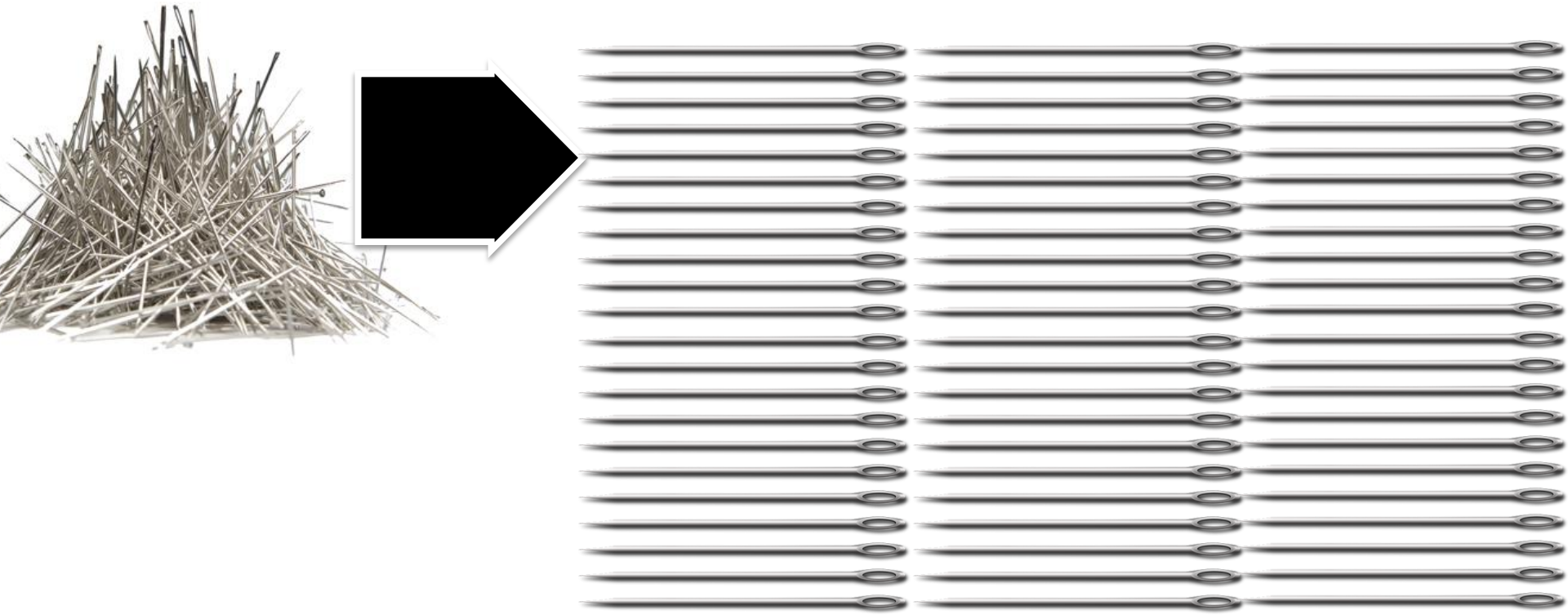
Type	Subtype	Value
Email_Address	sender	professor.moriarty@criminal-mastermind.com
Email_Address	recipient	an.innocent.victim@my-organization.com
Email_Subject		An offer you really cannot refuse

Note: For CybOX observables, you can use the derived basic indicator(s) for correlation!



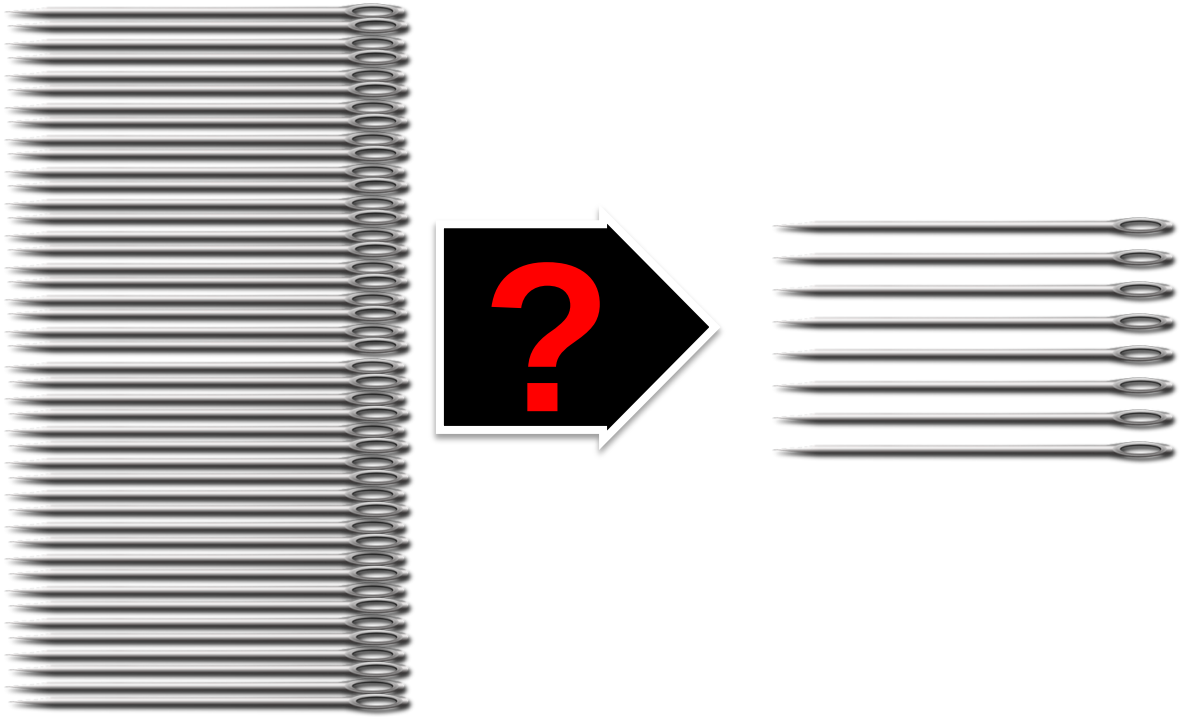
Type	Subtype	Value
IP	v4	192.168.1.13

Derivation of *possibly* actionable indicators



Processing each STIX/CybOX XML upon import yields a table of basic indicators that is fit for import into detection/prevention mechanisms.

How to get from *possibly* actionable indicators to indicators that make action worthwhile?



Processing each STIX/CybOX XML upon import yields a table of basic indicators that is fit for import into detection/prevention mechanisms.

SIEMENS

DERIVATION & RATING OF ACTIONABLE INDICATORS

For rating a possible indicator, we need context

Dictionary

context

SAVE POPULARITY

noun | con·text | \'kän-ˌtekst\

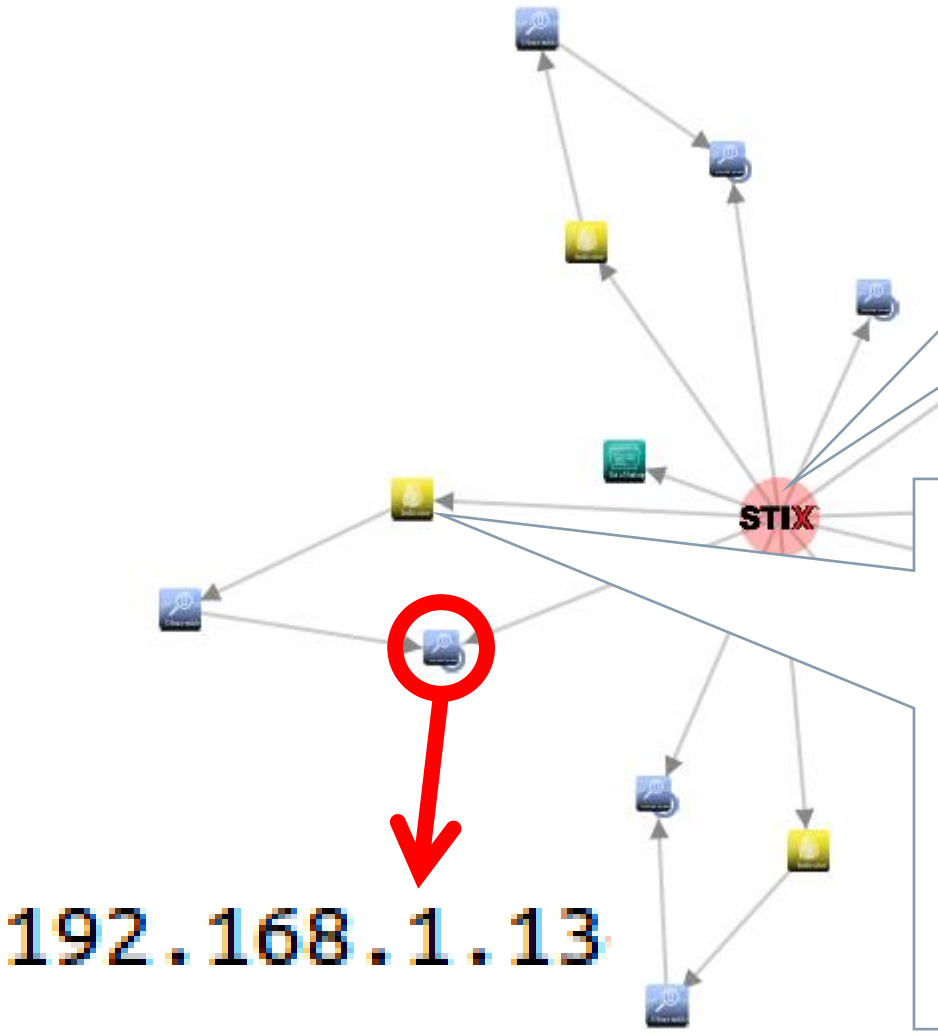
Cite! Share g+1 Tweet

1 : the parts of a discourse that surround a word or passage and can throw light on its meaning

2 : the interrelated conditions in which something exists or occurs : ENVIRONMENT, SETTING <the historical *context* of the war>

Possible sources of context: Within a report

SIEMENS



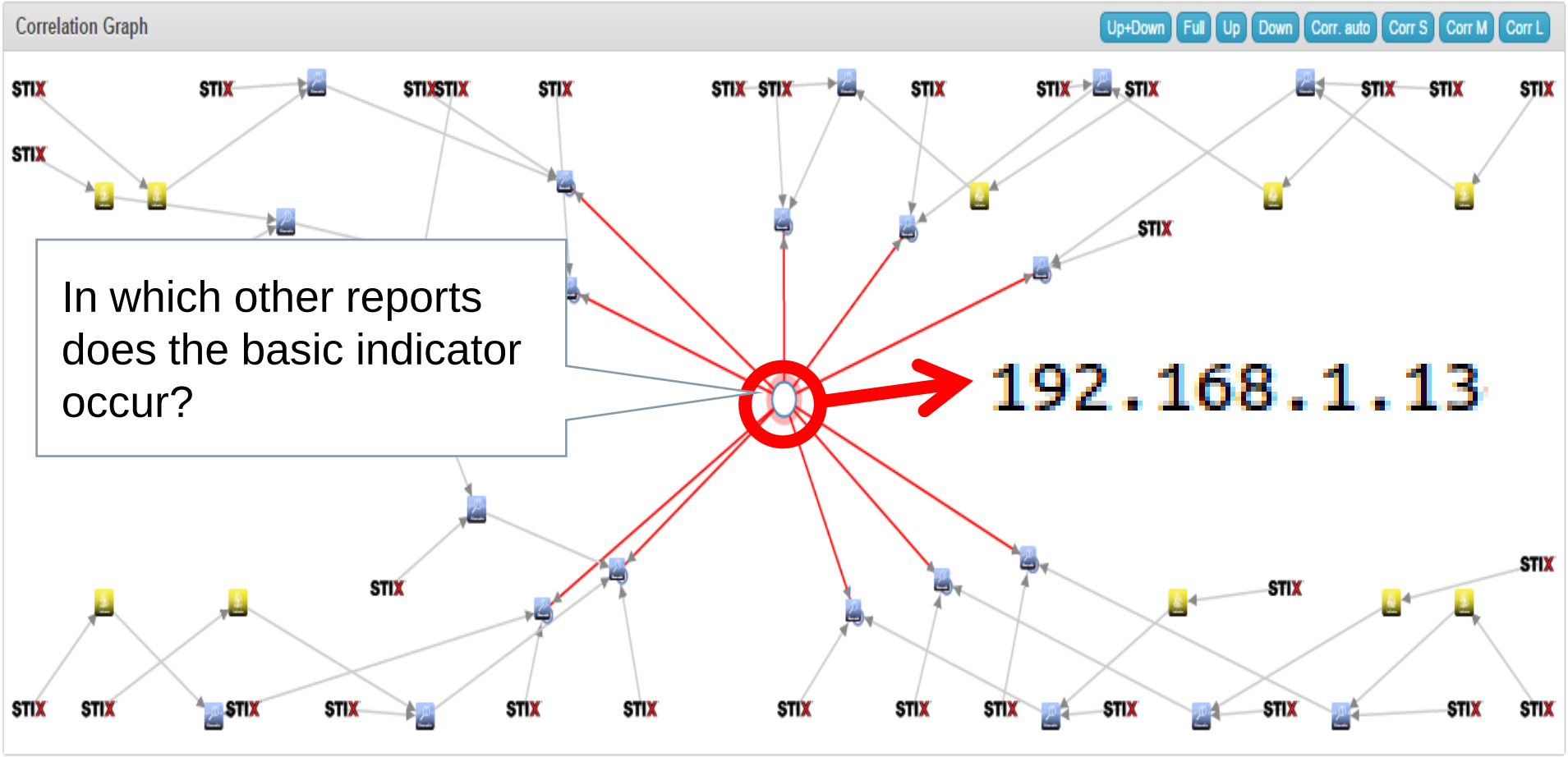
Who is the sender of the report?

What contextual information does the STIX indicator yield?

- Kill chain
- Confidence
- Associated Campaign & Threat Actor
- …

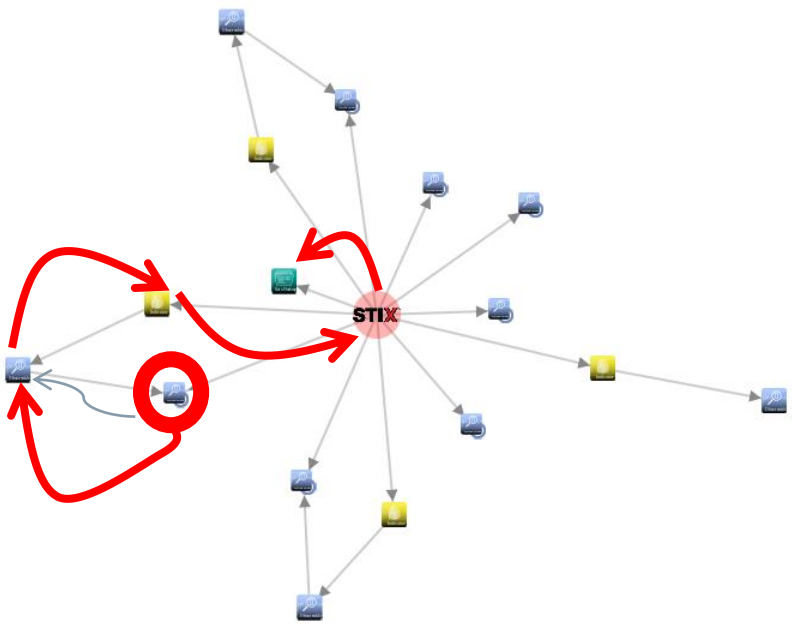
Possible sources of context: Between reports

SIEMENS



In which other reports does the basic indicator occur?

Rating basic indicators
First component: Walk the graph



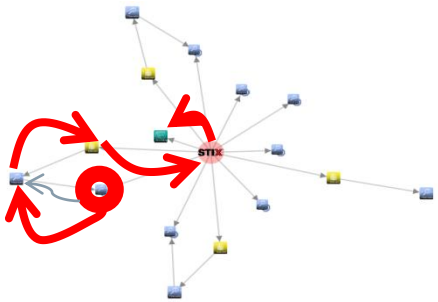
192.168.1.13

TLP	Amber
Confidence	High
Kill Chain	C&C
Campaign	World Domination
Threat Actor	Cunning Cricket
…	

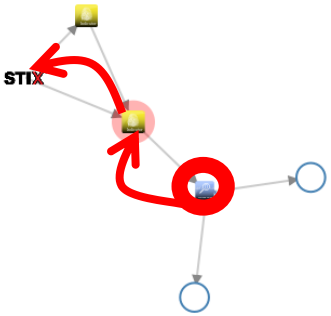
- Extract context information from STIX/CybOX content upon arrival of an import
- This requires walking the graph that is formed by the STIX report
- Codify context in a status information

Rating basic indicators
Second component:
Cumulative status & Status update upon new reports

SIEMENS



TLP	Amber
Confidence	High
Kill Chain	C&C
Campaign	World Domination
Threat Actor	Cunning Cricket
…	



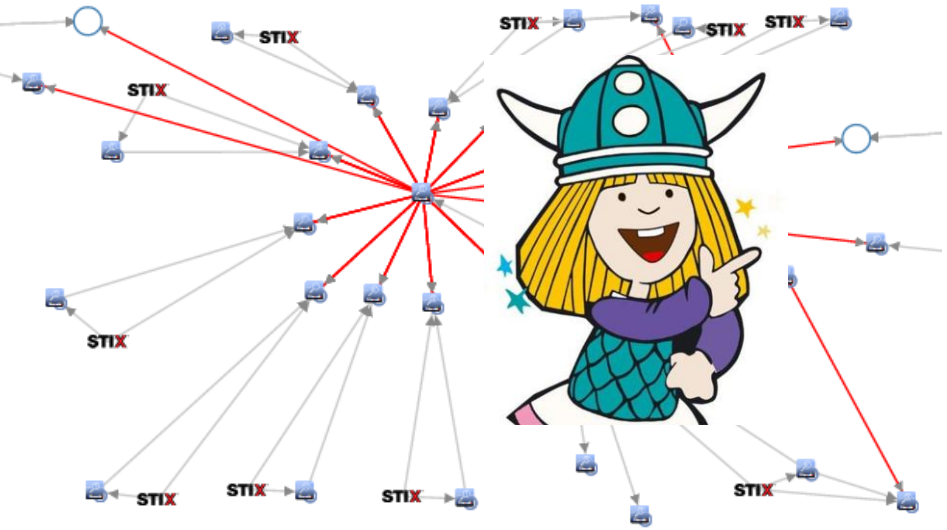
TLP	Amber
Confidence	High
Kill Chain	C&C
Campaign	World Domination
Threat Actor	Cunning Cricket
…	

192.168.1.13

Min. TLP	Green
Max. TLP	Amber
Min. Confidence	Low
Max. Confidence	High
Kill Chain	C&C; Delivery
Campaigns	World Domination, Gru‘s Plot
Threat Actors	Cunning Cricket, …

Rating basic indicators
Third component:
Analysts‘ input

SIEMENS



192.168.1.13

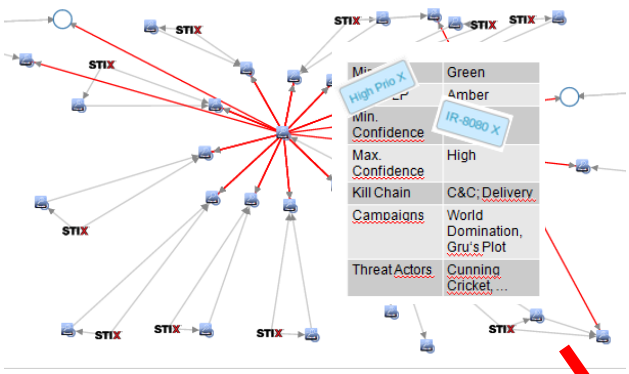
High Prio X

IR-8080 X

Mi…	Green
…P	Amber
Min. Confidence	
Max. Confidence	High
Kill Chain	C&C; Delivery
Campaigns	World Domination, Gru‘s Plot
Threat Actors	Cunning Cricket, …

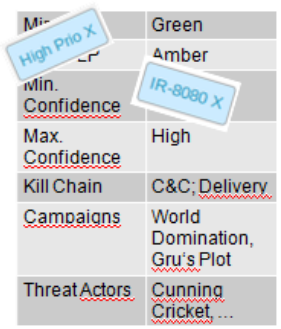
Independent from CybOX/STIX: use additional data sources (OSINT, …) to support indicator rating

SIEMENS

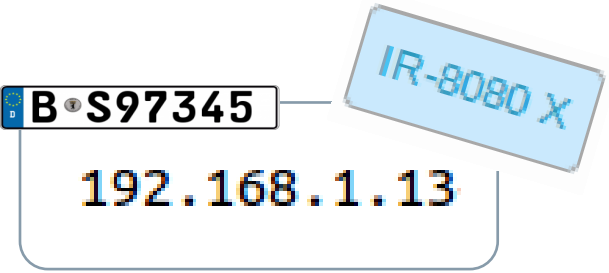


OSINT, …

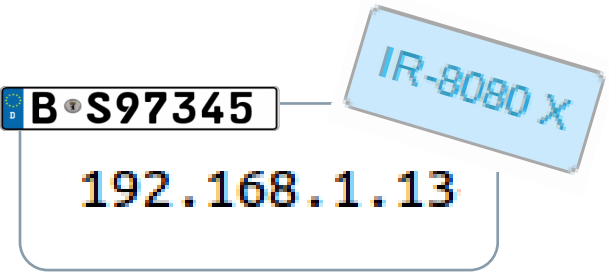
192.168.1.13

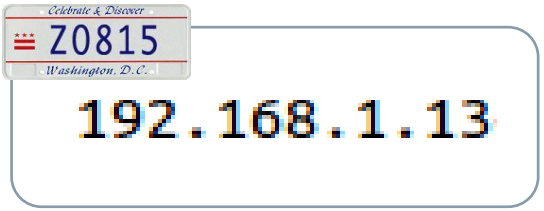


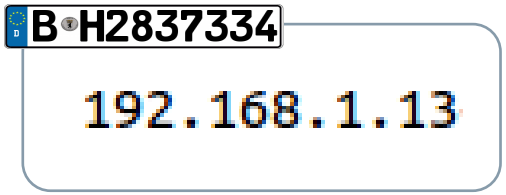
Note: For CybOX observables, you can use the derived basic indicator(s) for correlation!

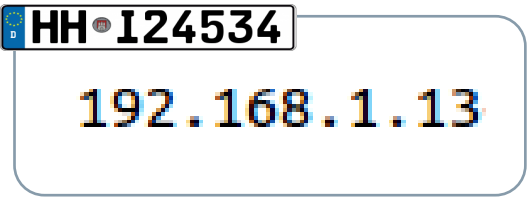


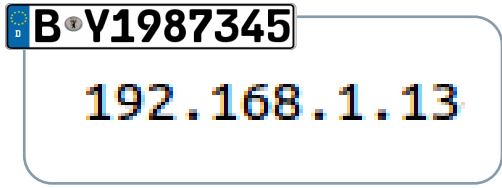
Note: For CybOX observables, you can use the derived basic indicator(s) for correlation!

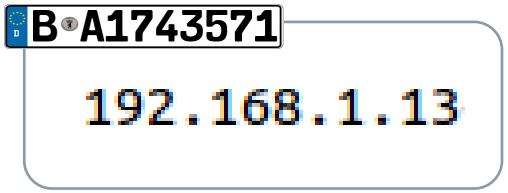


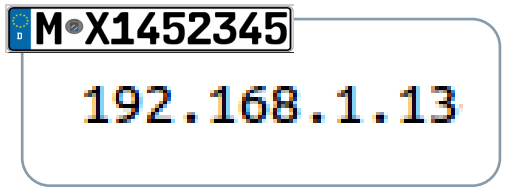




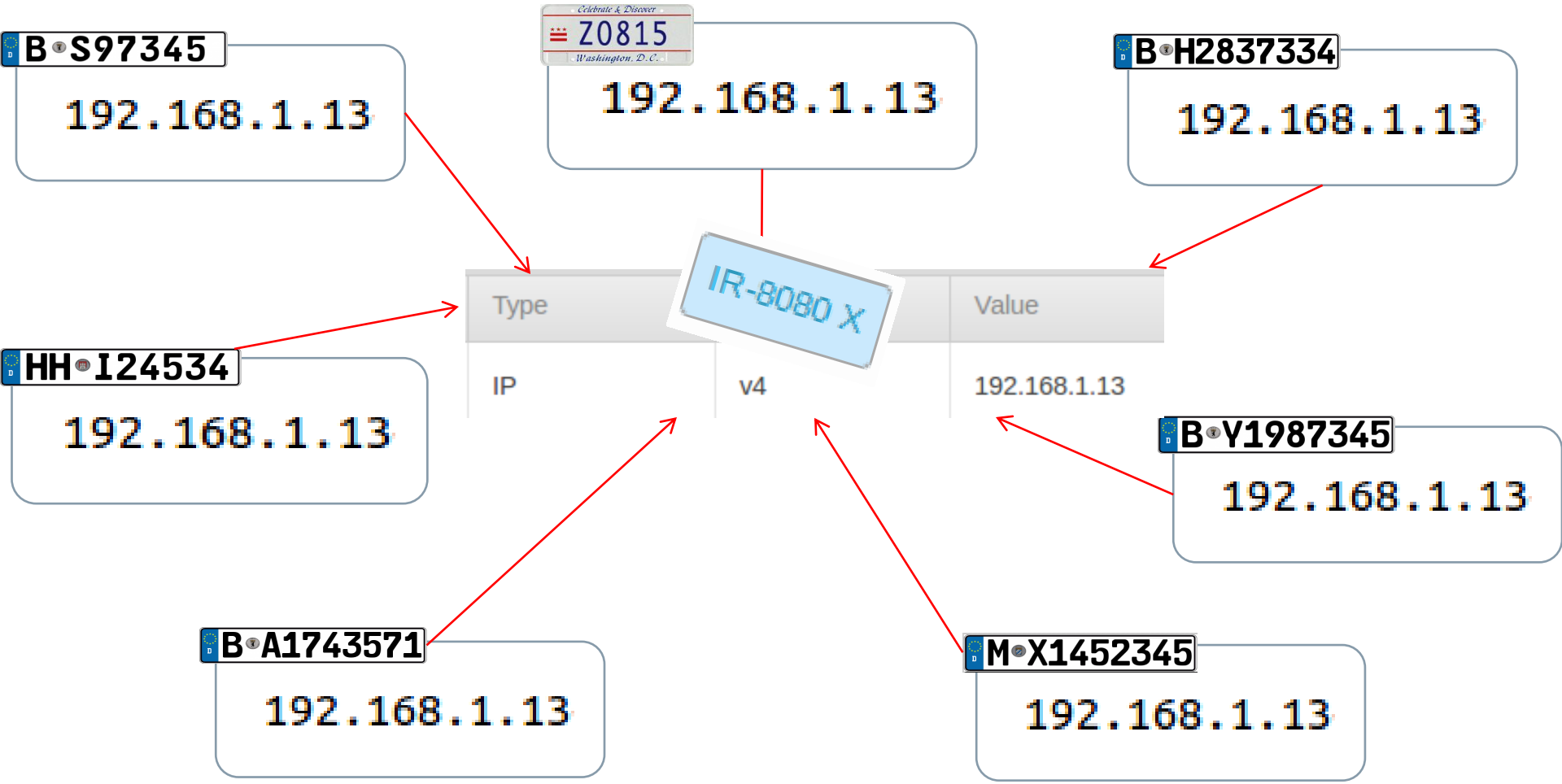




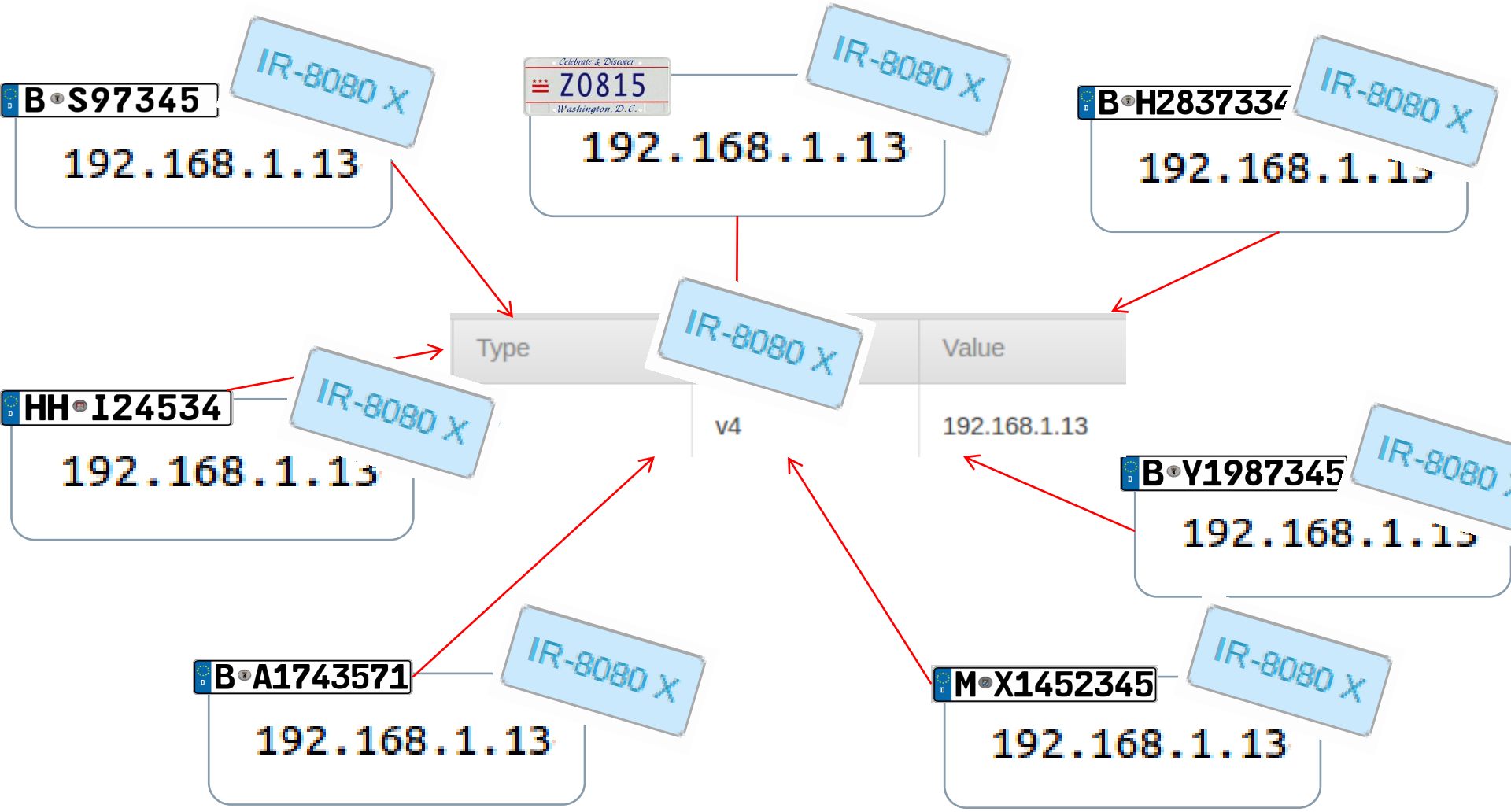




Note: For CybOX observables, you can use the derived basic indicator(s) for correlation!



Note: For CybOX observables, you can use the derived basic indicator(s) for correlation!



By the way ..

You can take a closer look into our cauldron:

Central arts of Siemens' threat-intelligence management framework MANTIS are available from

https://github.com/siemens/django-mantis

- **Please make sure to use the development branch!!! Follow the instructions at**
  http://django-mantis.readthedocs.org/en/development/installation.html
- **Note: this is not a finished product (see next slide)**

Caveat:
What MANTIS is and isn‘t

SIEMENS

- 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.

- 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.

SIEMENS

Summing up

- **Threat-Intel exchange using STIX/CybOX has taken off**
- **Now we need to learn to “drink from the fire hose”**
- **Nature of STIX/CybOX adds requirements for**
  - correlation of reports
  - extraction of basic indicators
  - rating of indicators (partly) based on contextual information contained in STIX-portion of reports
- **This talk has shown possible approaches**
- **Most likely, there are different approaches**
- **whatever tooling you use for dealing with STIX/CybOX: you cannot do without capabilities for correlation and indicator management**