Security in knowledge

THE SECRET TO EFFECTIVE CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

STIX™

Structured Threat Information eXpression

Sponsored by the
US Department of Homeland Security

Sean Barnum

MITRE

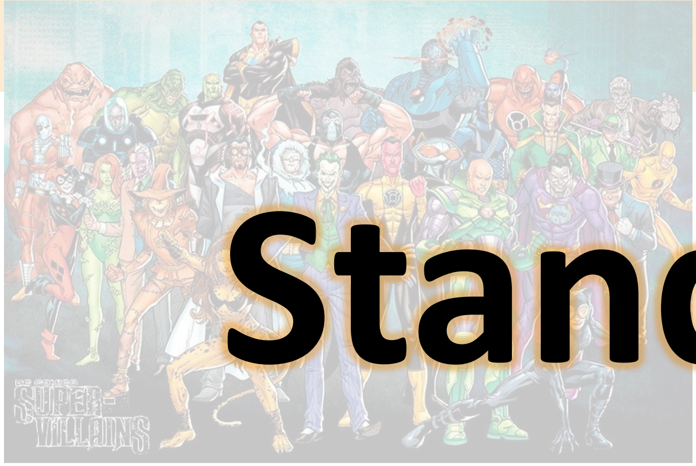
RSA®CONFERENCE2013

Session ID: DSP-R31

Session Classification: Intermediate

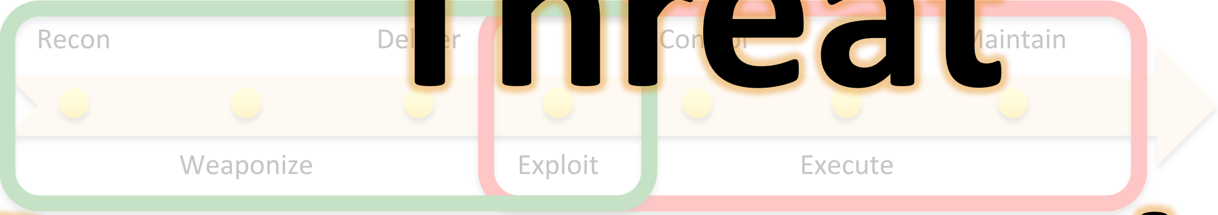
Standardized Threat Representation

Diverse and evolving threats



Balance inward & outward focus

Proactive & reactive actions



Information sharing

Need for holistic threat intelligence

Information Sharing

Cyber threat information (particularly indicators) sharing is not new

Typically very atomic and very limited in sophistication

IP lists, File hashes, URLs, email addresses, etc.

Most sharing is unstructured & human-to-human

Recent trends of machine-to-machine transfer of simple/atomic indicators

STIX aims to enable sharing of more expressive indicators as well as other full-spectrum cyber threat information.

What is STIX?

Language

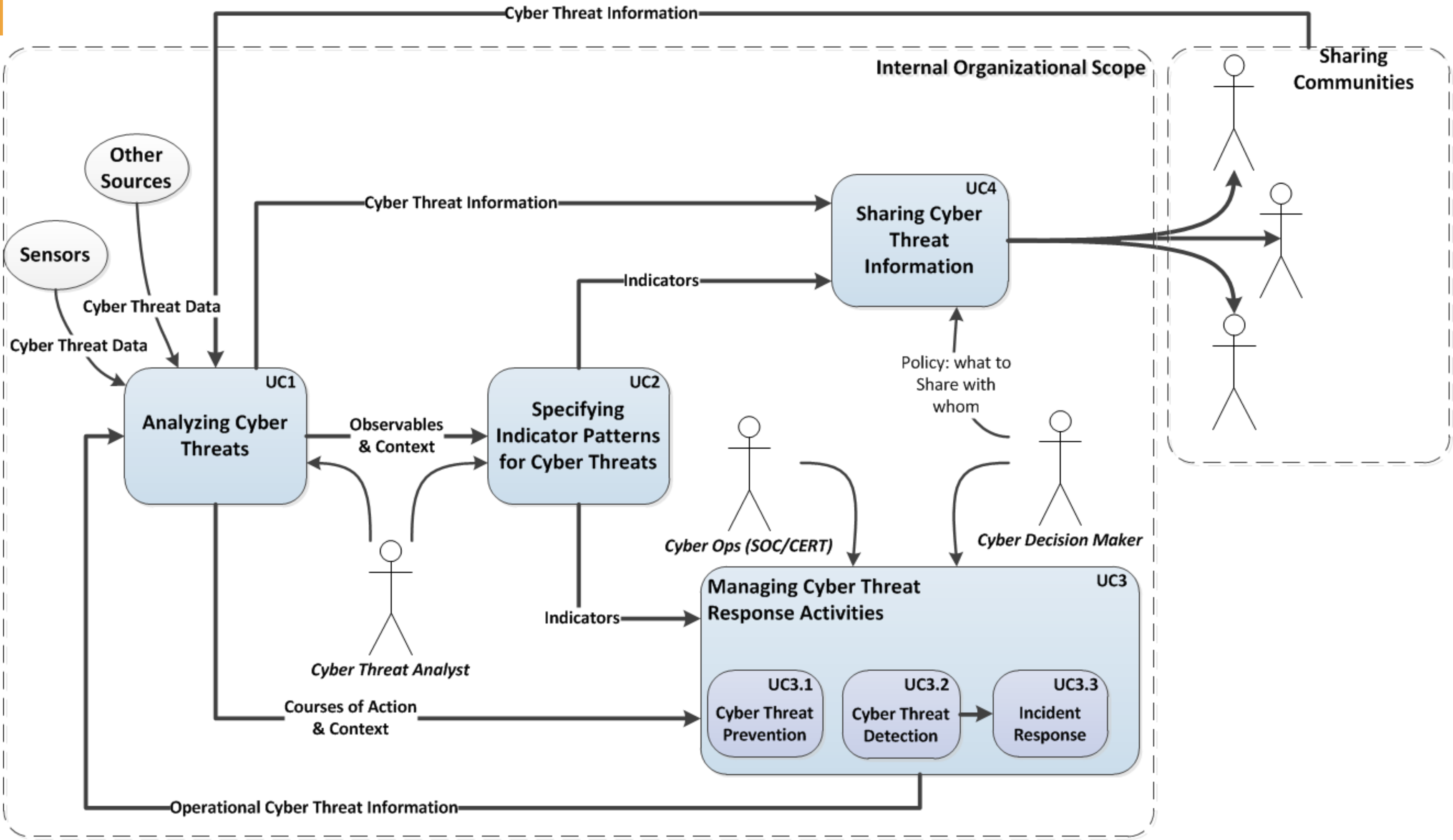
Specify **Capture** **Characterize** **Communicate**

Cyber Threat Information

Community-driven

Consistency **Clarity** **Support automation**

STIX Use Cases

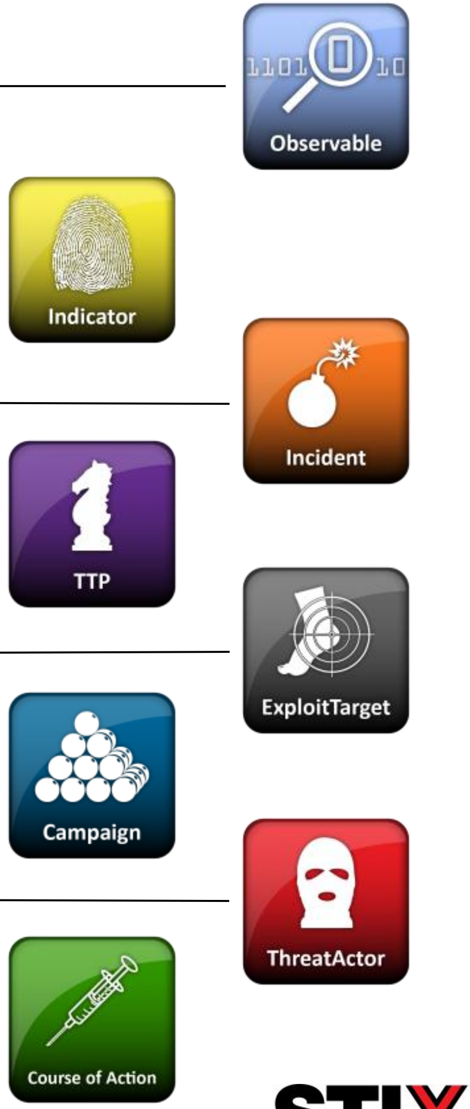


STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.

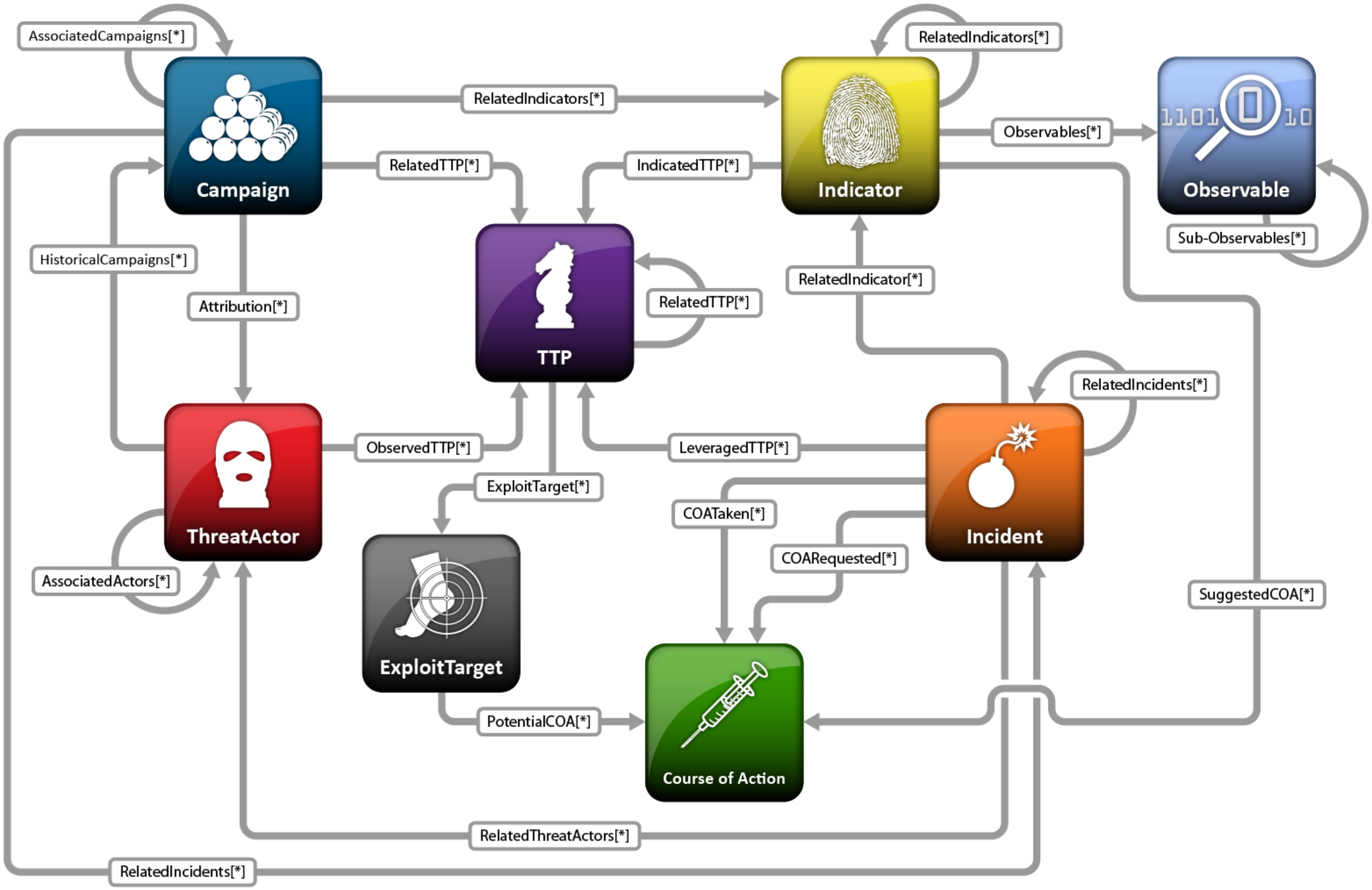
What is “Cyber Threat Intelligence”?

Consider these questions:

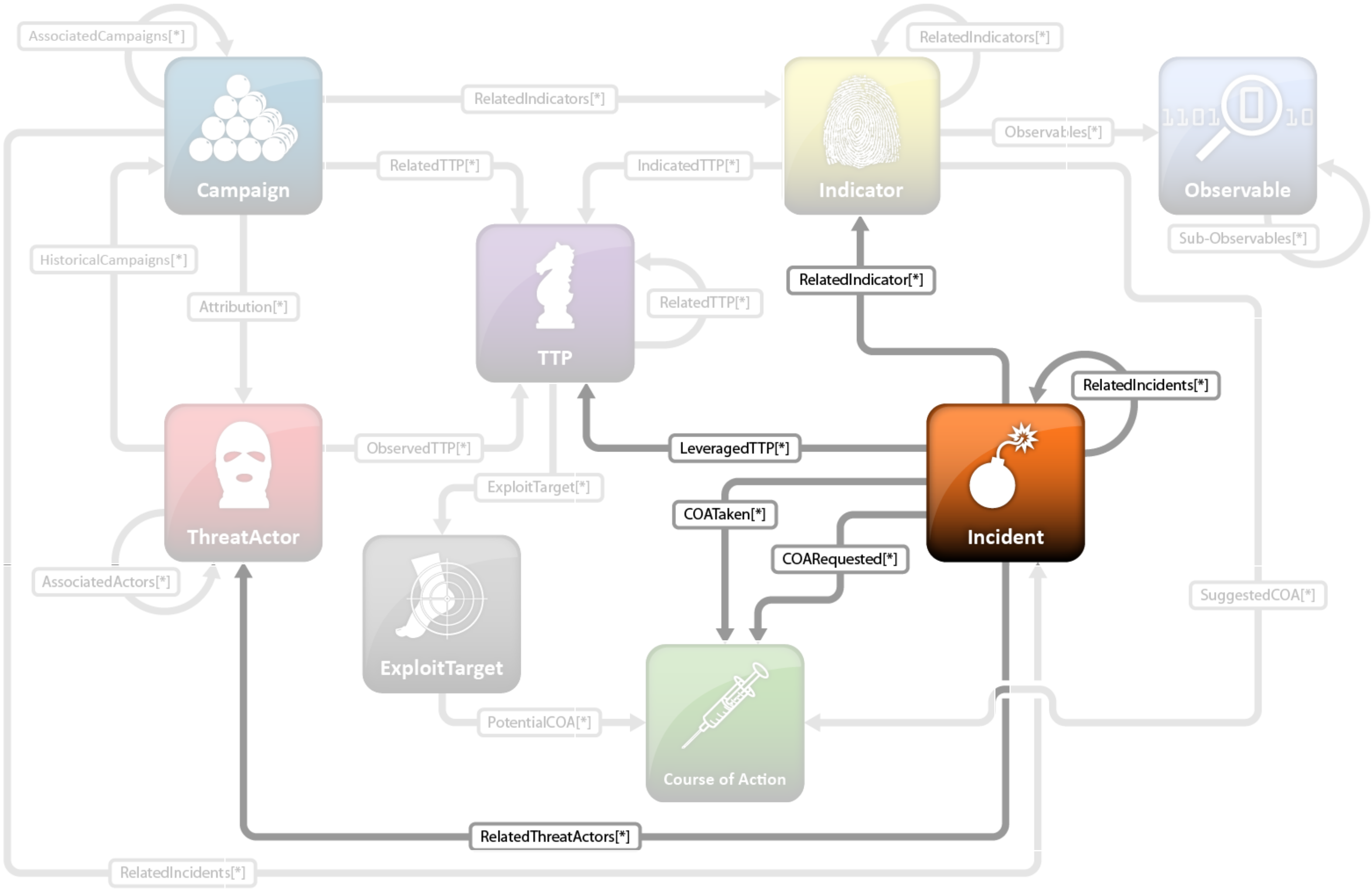
- What activity are we seeing?
- What threats should I look for on my networks and systems and why?
- Where has this threat been seen?
- What does it do?
- What weaknesses does this threat exploit?
- Why does it do this?
- Who is responsible for this threat?
- What can I do about it?



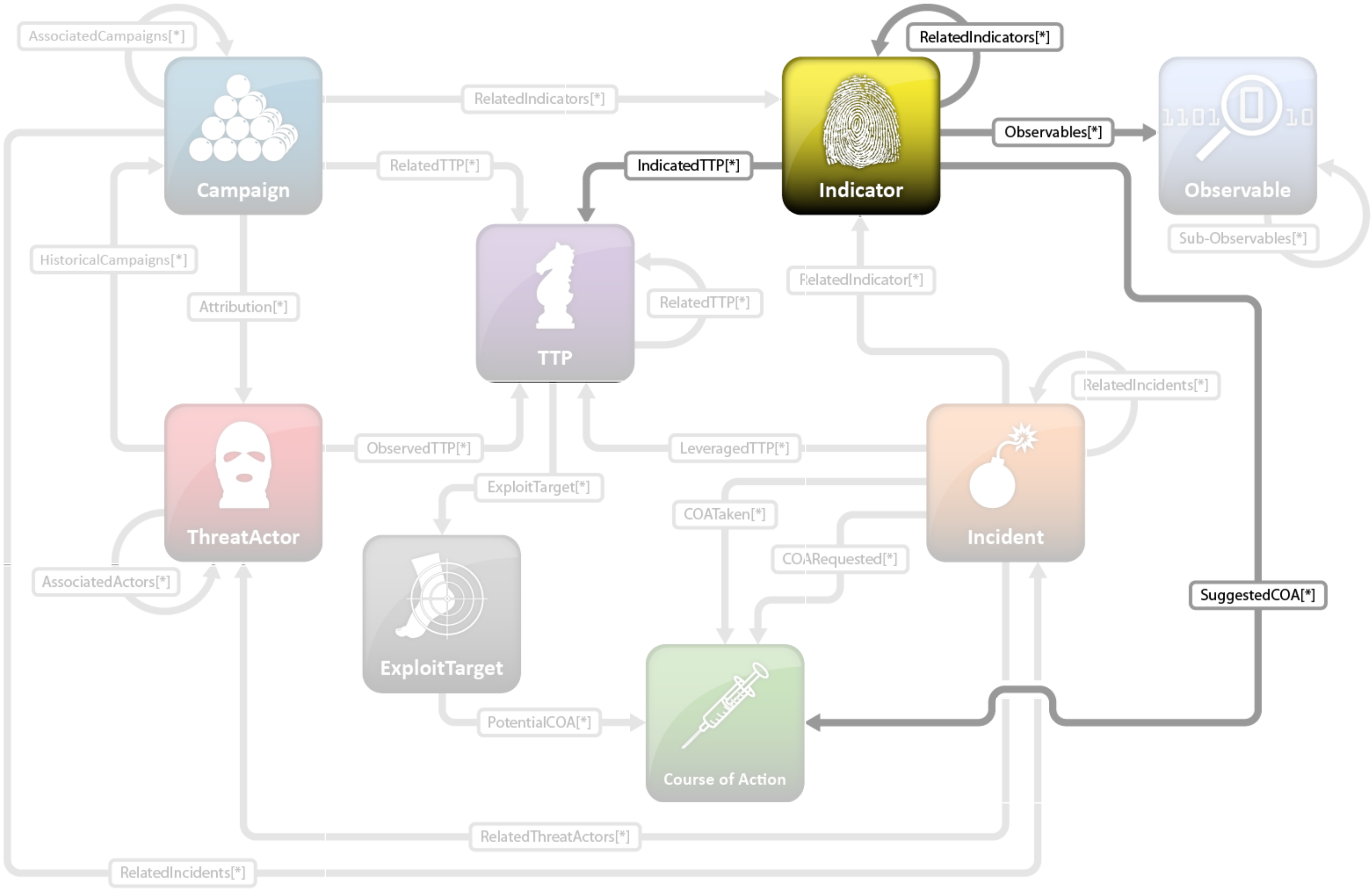
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



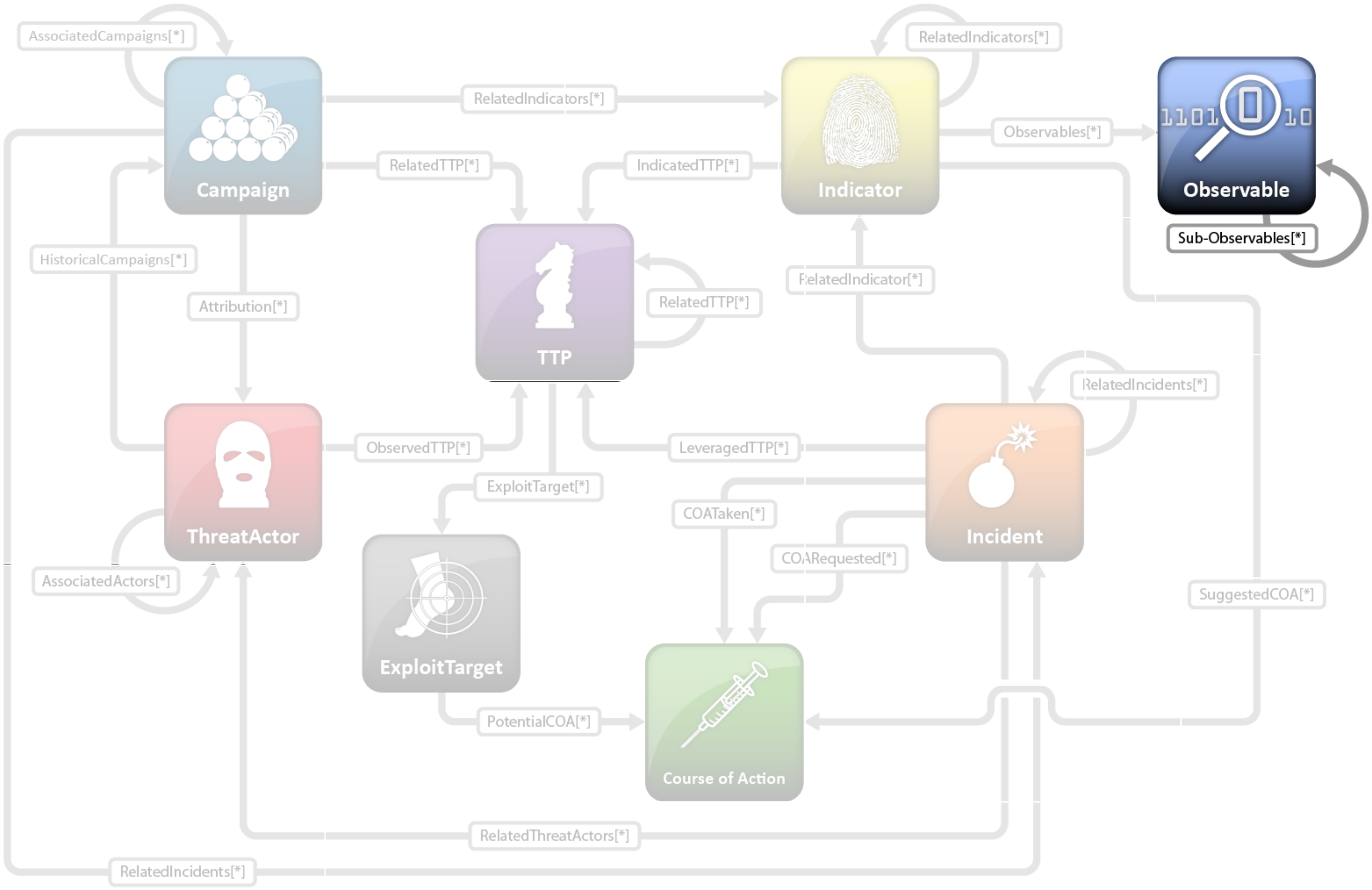
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



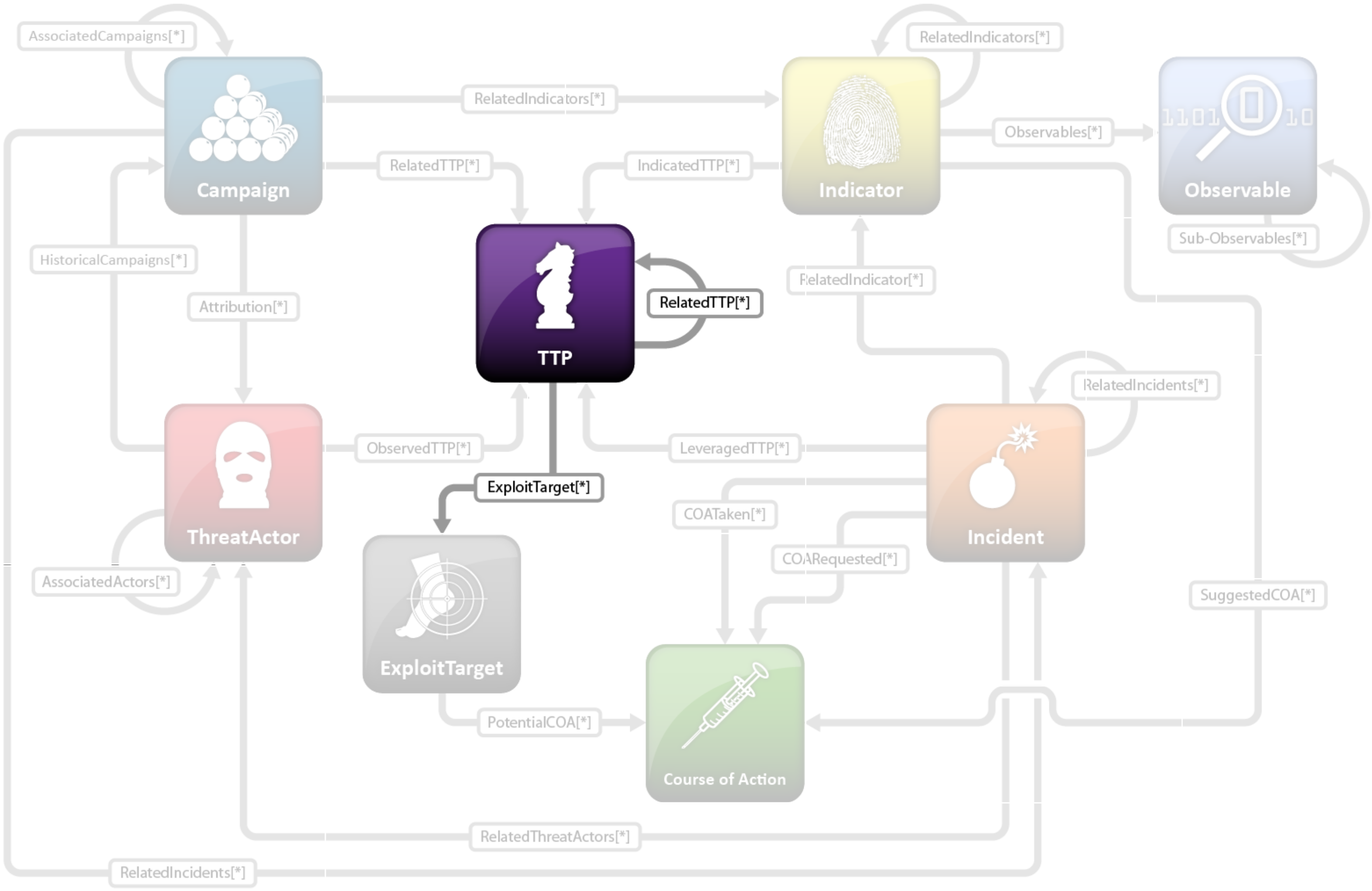
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



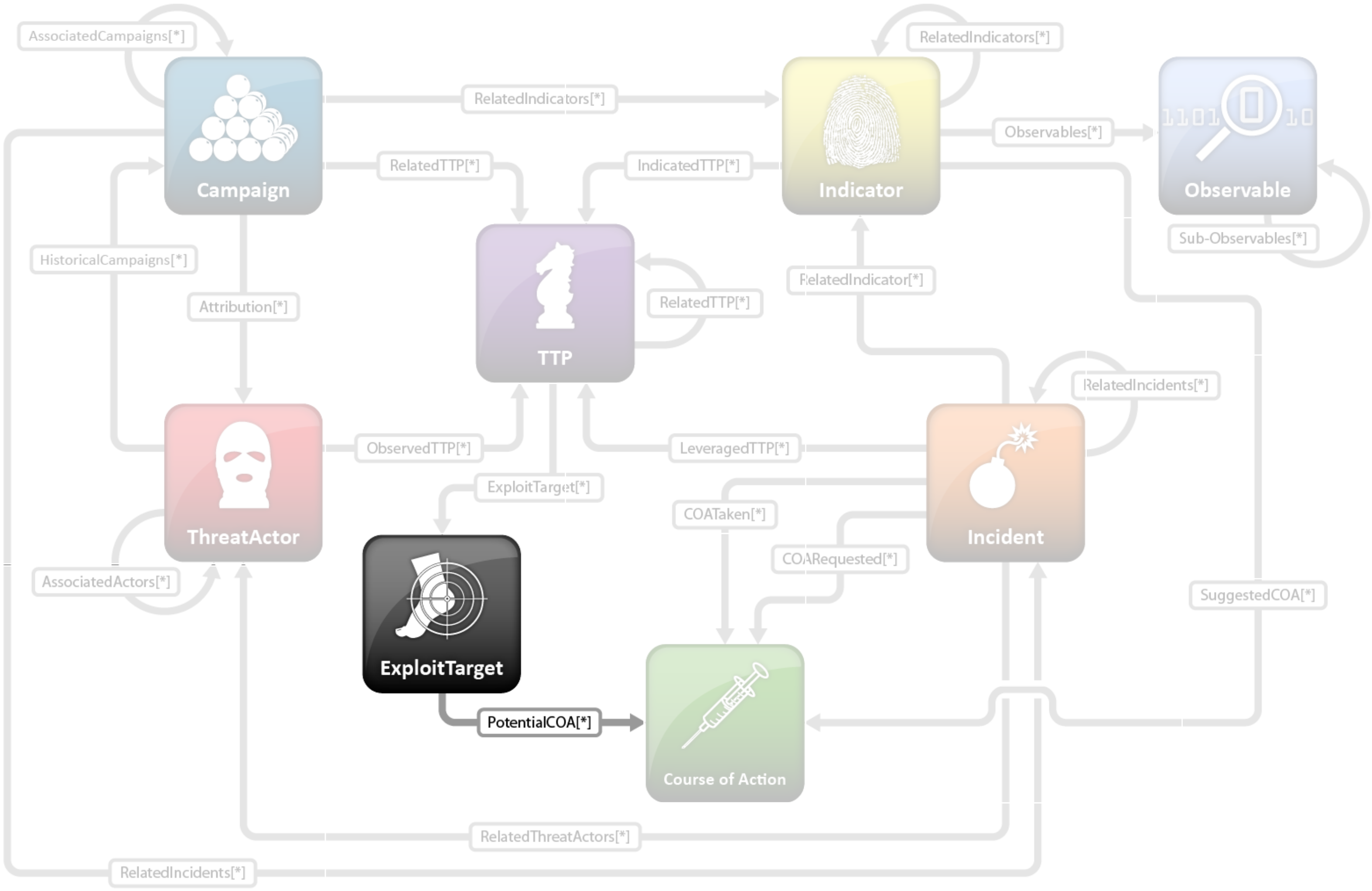
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



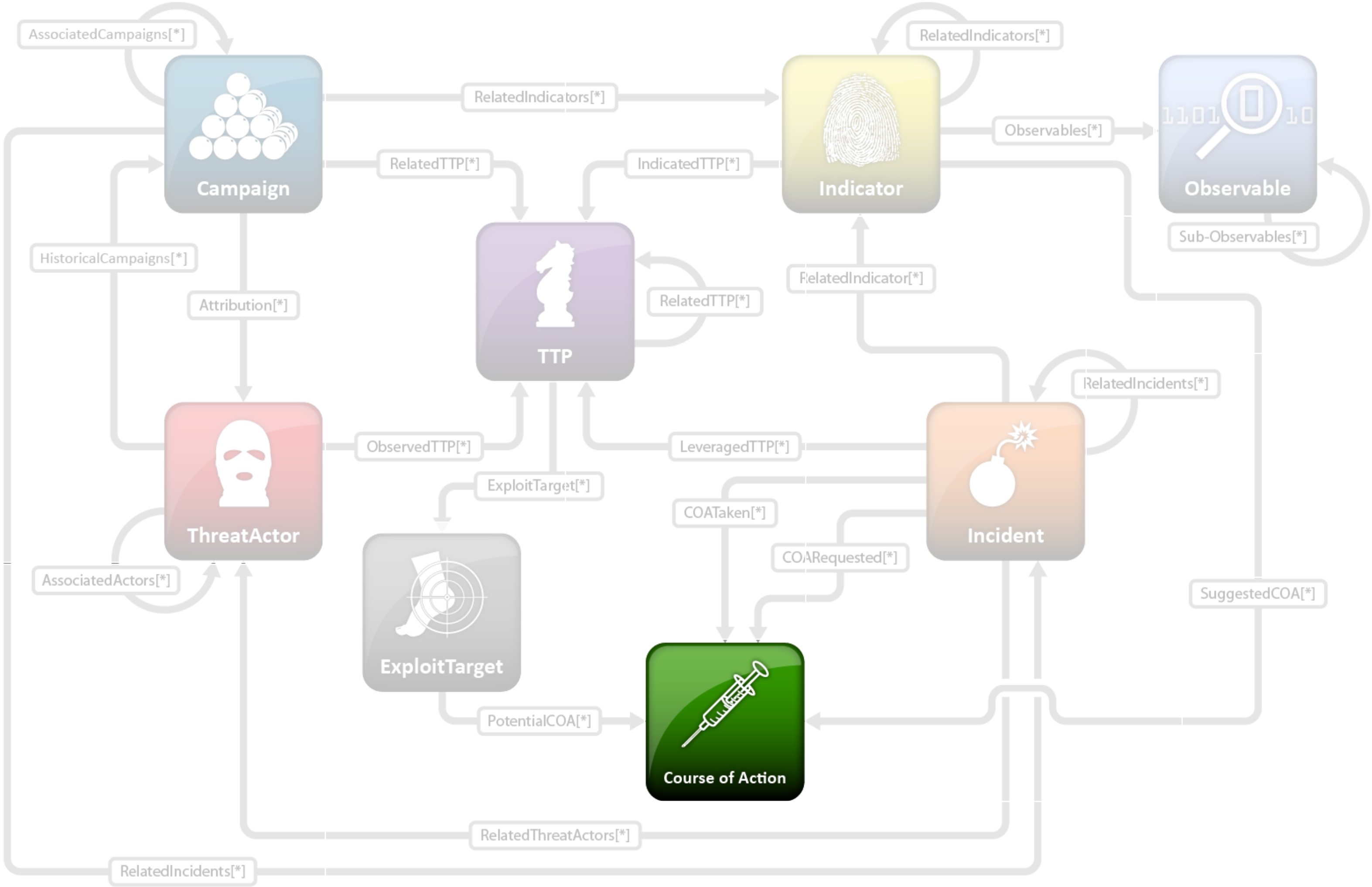
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



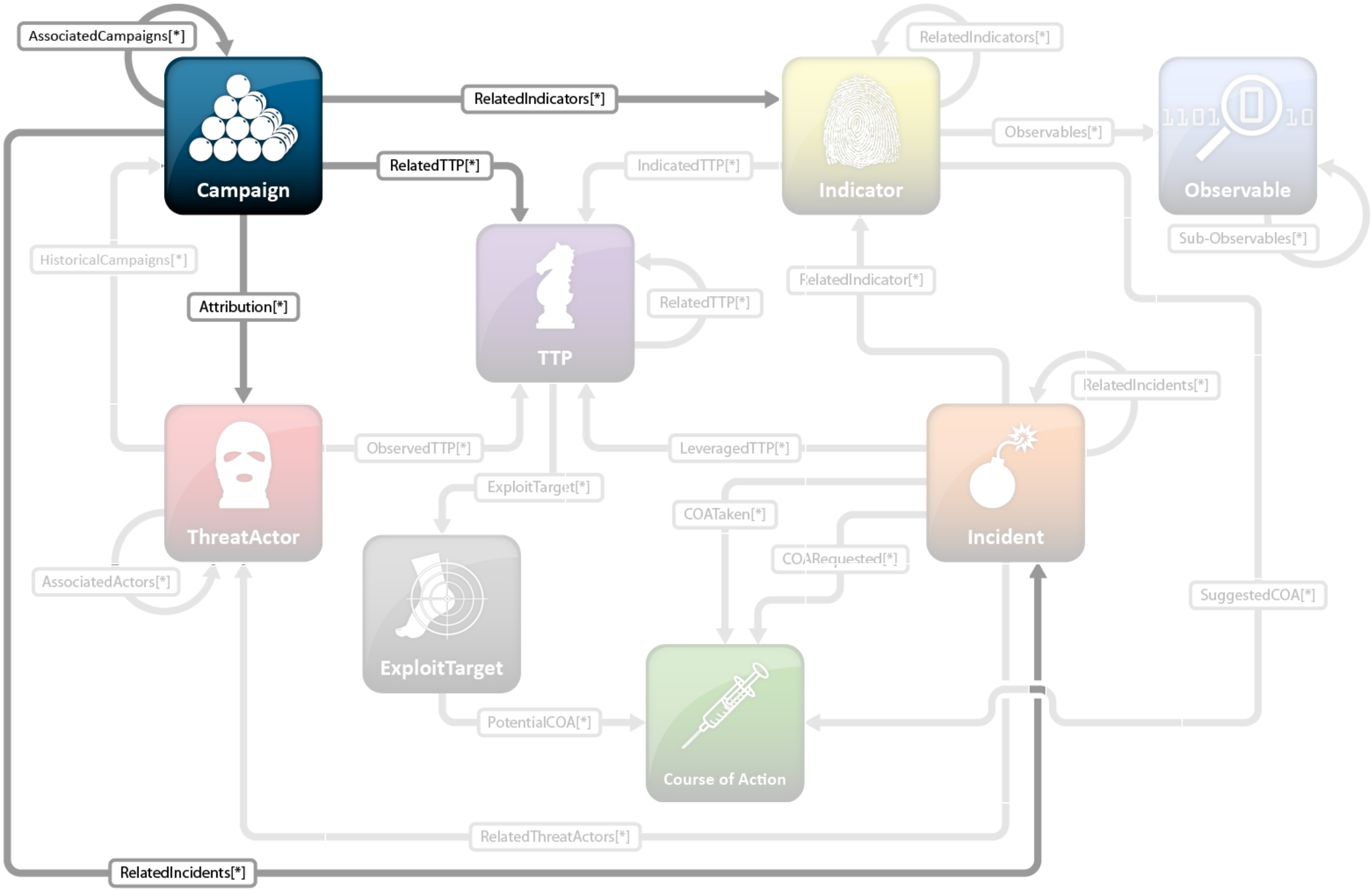
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



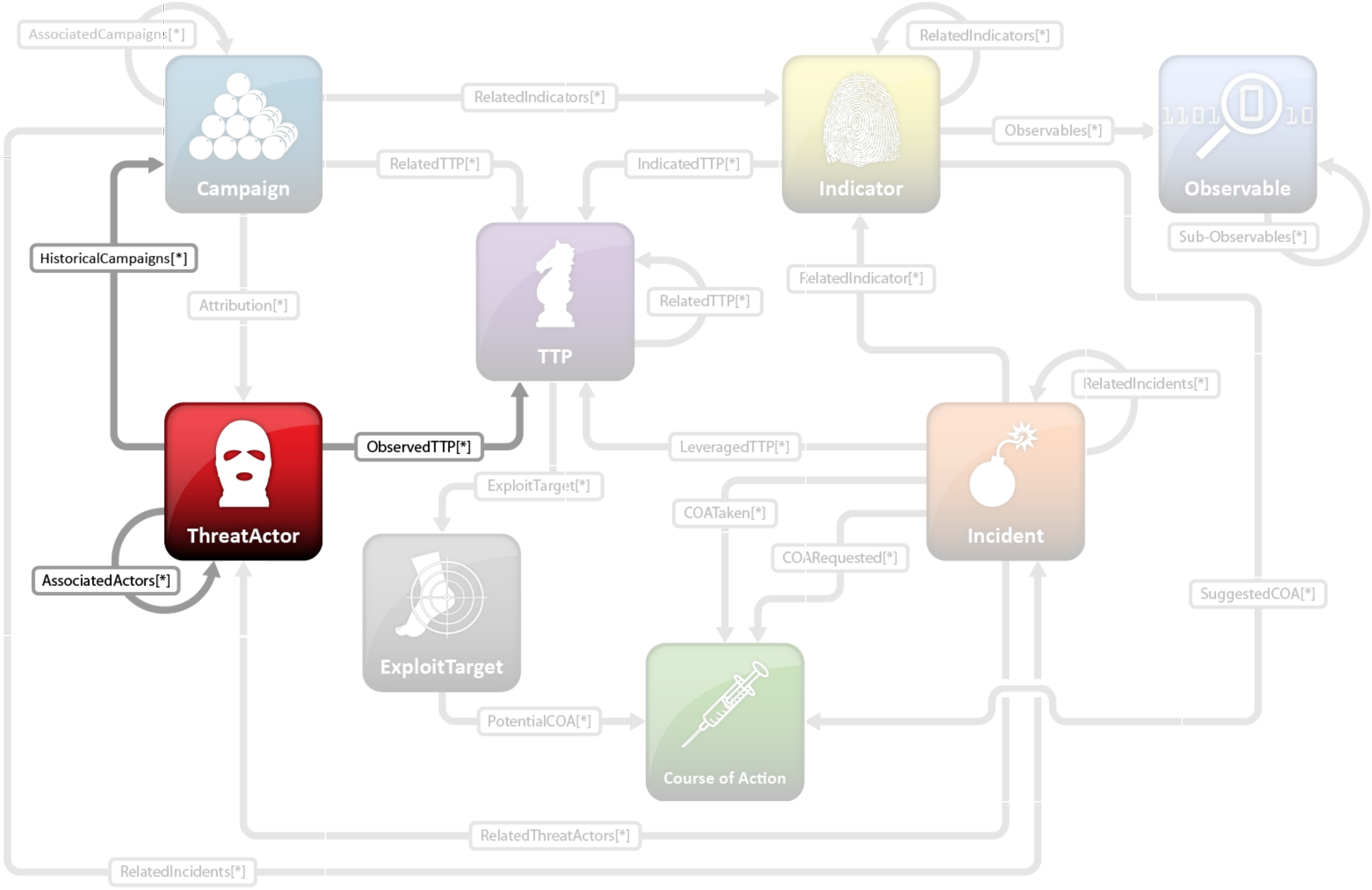
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



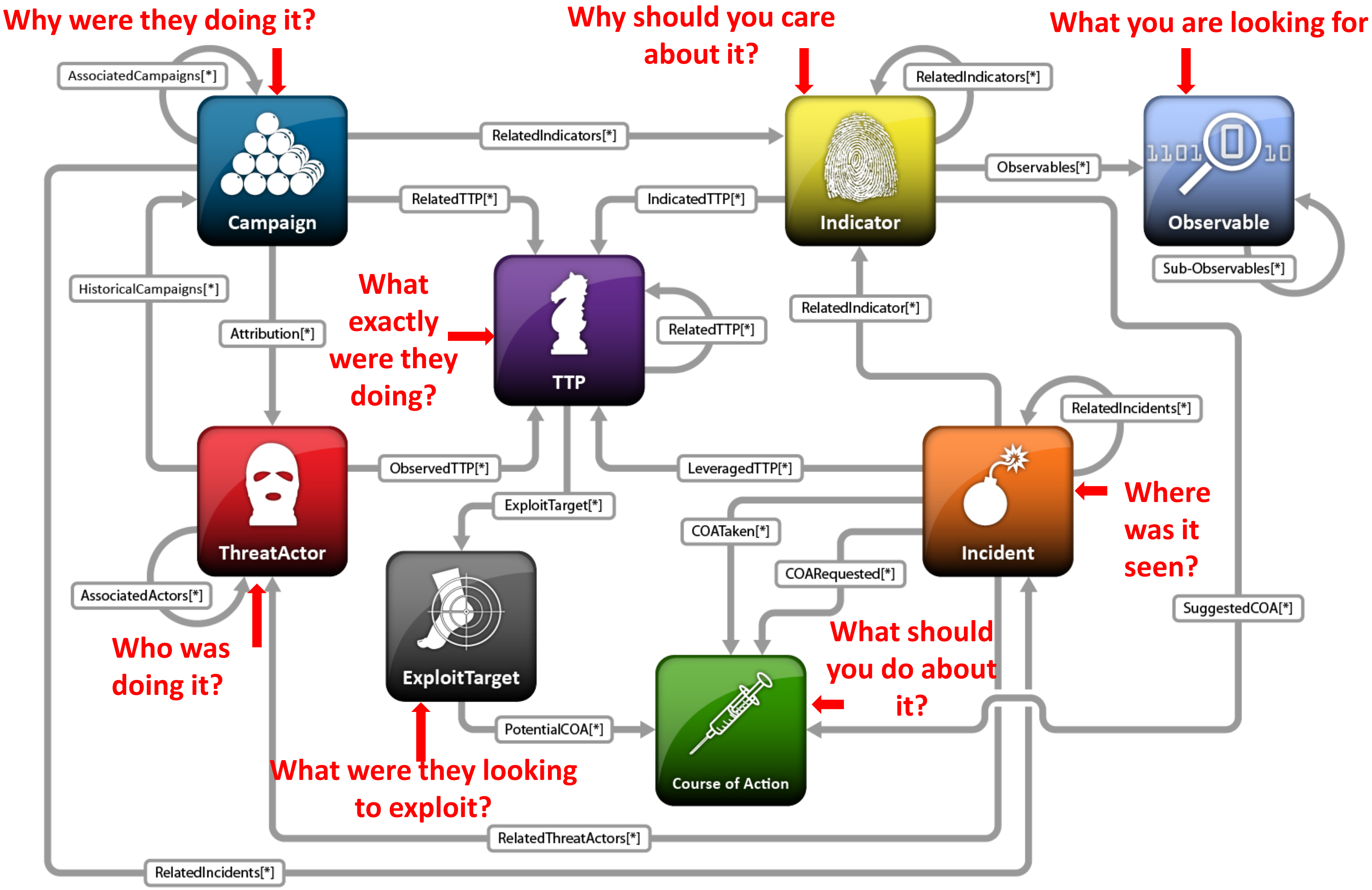
Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



Structured Threat Information eXpression (STIX) v1.0 (DRAFT) Architecture



Why were they doing it?

Why should you care about it?

What you are looking for

What exactly were they doing?

Where was it seen?

What should you do about it?

Who was doing it?

What were they looking to exploit?

Implementations

- Initial implementation has been done in XML Schema
  - Ubiquitous, portable and structured
  - Concrete strawman for community of experts
  - Practical structure for early real-world prototyping and POC implementations
  - Plan to iterate and refine with real-world use
- Next step will be a formal implementation-independent specification
  - Will include guidance for developing XML, JSON, RDF/OWL, or other implementations

Enabling Utilities

- Utilities to enable easier prototyping and usage of the language.

- Utilities consist of things like:
  - Language (Python) bindings for STIX, CybOX, MAEC, etc.
  - High-level programmatic APIs for common needs/activities
  - Conversion utilities from commonly used formats & tools
  - Comparator tools for analyzing language-based content
  - Utilities supporting common use cases
    - E.g. Email_to_CybOX utility supporting phishing analysis & management

- Open communities on GitHub (STIXProject, CybOXProject & MAECProject)

Adoption & Usage

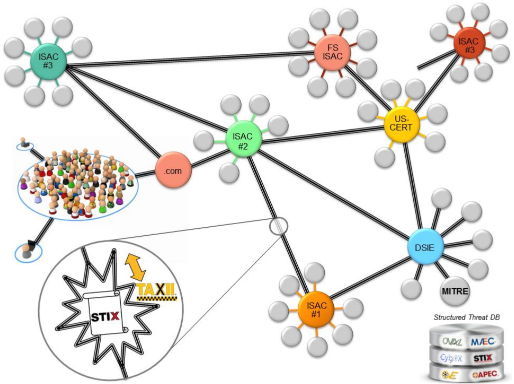
Still in its early stages but already generating extensive interest and initial operational use

TAXII™

Trusted Automated eXchange
of Indicator Information

What is TAXII?

- Trusted Automated eXchange of Indicator Information
- The goal of TAXII is to facilitate the exchange of structured cyber threat information
  - Designed to support existing sharing paradigms in a more automated manner



- TAXII is a set of specifications defining the network-level activity of the exchange
  - Defines services and messages to exchange data
  - Does NOT dictate *HOW* data is handled in the back-end, *WHAT* data is shared or *WHO* it is shared with
  - TAXII is NOT a sharing program

Adoption & Usage

Still in its early stages but already generating extensive interest and initial operational use

TAXII™
Trusted Automated eXchange of Indicator Information
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
U.S. DEPARTMENT OF HOMELAND SECURITY
CRITS
FINANCIAL SERVICES
ISAC

- Actively being considered by several information sharing communities
- Active interest from several large "user" organizations
- Active interest from some service/product vendors

A sampling of some of the organizations contributing to the STIX conversation includes:

THREAT STREAM

Booz | Allen | Hamilton

NORTHROP GRUMMAN

Cyveillance® a QinetiQ Company

CYBERIQ services

WORLD BANK

GE

MANDIANT®

REVERSING LABS

Br Bromium™

NATO OTAN

tripwire

RED SKY® ALLIANCE

USAA®

FINANCIAL SERVICES ISAC

CERT

IID

LOOKINGGLASS

MITRE

GENDARMERIE NATIONALE POLE JUDICIAIRE

LOCKHEED MARTIN

CROWDSTRIKE

incidentLogic

U.S. DEPARTMENT OF HOMELAND SECURITY

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

CYBER²

REN-ISAC

FOREGROUND SECURITY™

ICS-ISAC

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

DTCC

ES ISAC Electricity Sector Information Sharing Analysis Center

Critical Intelligence Intellectual Armor for Critical Infrastructure

VERISIGN™

PUNCH -CYBER ANALYTICS GROUP-

CERT-EU for the EU institutions, bodies and agencies

iSIGHTPARTNERS

NCI Security LLC

G2

Hyatt

STEGOSYSTEMS invisibility integrity immunity

VISA

verizon

GENERAL DYNAMICS

SIEMENS

NIST

RSA CONFERENCE 2013

STIX™ Structured Threat Information eXpression

Current Focus

- Make it easier for people to understand and use STIX
  - Improve documentation
  - Develop supporting utilities
  - Provide collaborative guidance
  - Gather feedback
- Refine and extend the language based on feedback and needs

Phishing Use Case Example

- Currently phishing analysis is very slow and manual
  - Limits the volume of email that can be analyzed
  - Slows ability to respond to high-risk threats
  - Limits the ability to share information in an actionable form
- Structuring the information enables more automation
  - Significantly increase analysis volume
  - Ability to respond to high-risk threats at machine speed
  - Enable active sharing of actionable information
  - Free the human analyst to focus on the “harder” stuff

Potential STIX-enabled Phishing Analysis

1. A suspicious email is received by an individual within organization XXX.

2. The email recipient forwards it to suspicious@XXX.YYY for analysis by the XXX.YYY threat analysis cell.

3. The email received in the suspicious@XXX.YYY Inbox is automatically processed with the **Email_to_CybOX** utility in the background.

   - A comprehensive package of structured CybOX content is generated which characterizes the suspicious email including some derivative automated background analysis.

Email_to_CybOX Structured Output

- The package includes the following Observable Objects with all of the appropriate defined relationships between them:
  - a fully structured representation of the email itself (**CybOX Email_Message object**)
  - for each attachment:
    - a structured capture of the raw file itself (**CybOX Artifact object**)
    - a structured characterization of the properties of the file (**CybOX File object**)
  - for each URL/link embedded in the email itself:
    - a structured capture of the URL (**CybOX URI object**)
    - a structured capture of the domain name of the URL (**CybOX URI object**)
    - a structured capture of the results of a WHOIS lookup performed on the domain name (**CybOX WHOIS object**)
    - a structured capture of a DNS Queries (Type A & AAAA Records) run on the domain name (**CybOX DNSQuery objects**)
    - a structured capture of the DNS Records (Type A & AAAA Record) resulting from the DNS Queries run on the domain name (**CybOX DNSRecord objects**)
    - a structured capture of the resolving IP addresses for the domain name resulting from the DNS Queries (**CybOX Address object**)

Email_Message Object

```
<cybox:Observable id="cybox:observable-6f45ce72-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:object-6dc7fc5a-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Attachments>
            <EmailMessageObj:File xsi:type="FileObj:FileObjectType" object_reference="cybox:object-6dcae276-30c8-11e2-8011-000c291a73d5"/>
          </EmailMessageObj:Attachments>
          <EmailMessageObj:Links>
             <EmailMessageObj:Link type="URL" object_reference="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5“/>
             <EmailMessageObj:Link type="URL" object_reference="cybox:guid-6ec9050e-30c8-11e2-8011-000c291a73d5“/>
           </EmailMessageObj:Links>
          <EmailMessageObj:Header>
            <EmailMessageObj:To>
              <EmailMessageObj:Recipient category="e-mail">
                <AddressObj:Address_Value datatype="String">jsmith@gmail.com</AddressObj:Address_Value>
              </EmailMessageObj:Recipient>
            </EmailMessageObj:To>
            <EmailMessageObj:From category="e-mail">
              <AddressObj:Address_Value datatype="String">jdoe@state.gov</AddressObj:Address_Value>
            </EmailMessageObj:From>
            <EmailMessageObj:Subject datatype="String">Fw:Draft US-China Joint Statement</EmailMessageObj:Subject>
            <EmailMessageObj:Date datatype="DateTime">2011-01-05T12:48:50+08:00</EmailMessageObj:Date>
            <EmailMessageObj:Message_ID datatype="String">
                    CAF=+=fCSNqaNnR=wom=Y6xP09r_wfKjsm0hvY3wJYTGEzGyPkw@mail.gmail.com
            </EmailMessageObj:Message_ID>
          </EmailMessageObj:Header>
          <EmailMessageObj:Optional_Header>
            <EmailMessageObj:Content-Type datatype="String">
                    multipart/mixed; boundary=90e6ba10b0e7fbf25104cdd9ad08
            </EmailMessageObj:Content-Type>
            <EmailMessageObj:MIME-Version datatype="String">1.0</EmailMessageObj:MIME-Version>
            <EmailMessageObj:X-Mailer datatype="String">Microsoft CDO for Windows 2000</EmailMessageObj:X-Mailer>
          </EmailMessageObj:Optional_Header>
```

Email_Message Object (cont.)

```
<EmailMessageObj:Raw_Body datatype="String">

        <![CDATA[  …<!– Raw body content would be inline here → ]]>

</EmailMessageObj:Raw_Body>
<EmailMessageObj:Raw_Header datatype="String">

        <![CDATA[  …<!– Raw header content would be inline here → ]]>

</EmailMessageObj:Raw_Header>
          </cybox:Defined_Object>
          <cybox:Related_Objects>
            <cybox:Related_Object idref="cybox:object-6dcae276-30c8-11e2-8011-000c291a73d5" type="File" relationship="Contains"/>
            <cybox:Related_Object idref="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012" type="Artifact" relationship="Contains"/>
            <cybox:Related_Object idref="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5" type="URL" relationship="Contains"/>
            <cybox:Related_Object idref="cybox:guid-6ec9050e-30c8-11e2-8011-000c291a73d5" type="URL" relationship="Contains"/>
          </cybox:Related_Objects>
        </cybox:Object>
      </cybox:Stateful_Measure>
    </cybox:Observable>
```

Artifact Object

```
<cybox:Observable id="cybox:observable-14ee6790-b83d-44f1-8604-92271efac9bf">
    <cybox:Stateful_Measure>
       <cybox:Object id="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012">
          <cybox:Defined_Object xsi:type="Artifact:ArtifactType" type="File" content_type="application/pdf">
         <Artifact:Hashes>
            <Common:Hash>
               <Common:Type datatype="String">MD5</Common:Type>
               <Common:Simple_Hash_Value datatype="hexBinary">cf2b3ad32a8a4cfb05e9dfc45875bd70</Common:Simple_Hash_Value>
            </Common:Hash>
                 </Artifact:Hashes>
         <Artifact:Packaging is_compressed="false" is_encrypted="false">
            <Artifact:Encoding algorithm="Base64" character_set="iso-8859-1"/>
         </Artifact:Packaging>
         <Artifact:Raw_Artifact>
JVBERi0xLjUNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFuZyhlbi1VUykgL1N0cnVjdFRyZWVSb290IDEwNyAwIFI
vTWFya0luZm88PC9NYXJrZWQgdHJ1ZT4+Pj4NCmVuZG9iag0KMiAwIG9iag0KPDwvVHlwZS9QYWdlcy9Db3VudCAyMC9La
…
<!—The rest of the base64 encoded file content is not included within this document for space concerns. The full content is available in the example file. -->
         </Artifact:Raw_Artifact>
          </cybox:Defined_Object>
          <cybox:Related_Objects>
         <cybox:Related_Object idref="cybox:object-6dcae276-30c8-11e2-8011-000c291a73d5" type="File" relationship="Characterized_By"/>
         <cybox:Related_Object idref="cybox:object-6dc7fc5a-30c8-11e2-8011-000c291a73d5" type="Email Message" relationship="Contained_Within"/>
           </cybox:Related_Objects>
       </cybox:Object>
   </cybox:Stateful_Measure>
</cybox:Observable>
```

File Object

```
<cybox:Observable id="cybox:observable-6f45edbc-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:object-6dcae276-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="FileObj:FileObjectType">
          <FileObj:File_Name datatype="String">Joint_Statement.pdf</FileObj:File_Name>
          <FileObj:File_Extension datatype="String">pdf</FileObj:File_Extension>
          <FileObj:Size_In_Bytes datatype="UnsignedLong">87022</FileObj:Size_In_Bytes>
          <FileObj:Hashes>
            <Common:Hash>
              <Common:Type datatype="String">MD5</Common:Type>
              <Common:Simple_Hash_Value datatype="hexBinary">cf2b3ad32a8a4cfb05e9dfc45875bd70</Common:Simple_Hash_Value>
            </Common:Hash>
          </FileObj:Hashes>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:object-6dc7fc5a-30c8-11e2-8011-000c291a73d5" type="Email Message" relationship="Contained_Within"/>
          <cybox:Related_Object idref="cybox:object-afb6205d-4db6-44de-98d7-37a32ee4b012" type="Artifact" relationship="Characterizes"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

RSA CONFERENCE 2013

URL Object

```
<cybox:Observable id="cybox:observable-6f45f0aa-30c8-11e2-8011-000c291a73d5">
   <cybox:Stateful_Measure>
       <cybox:Object id="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5">
           <cybox:Defined_Object xsi:type="URIObj:URIObjectType" type="URL">
               <URIObj:Value datatype="AnyURI">http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</URIObj:Value>
           </cybox:Defined_Object>
           <cybox:Related_Objects>
               <cybox:Related_Object idref="cybox:guid-6dcb9414-30c8-11e2-8011-000c291a73d5" type="URI" relationship="Contains"/>
               <cybox:Related_Object idref="cybox:object-6dc7fc5a-30c8-11e2-8011-000c291a73d5" type="Email Message" relationship="Contained_Within"/>
           </cybox:Related_Objects>
       </cybox:Object>
   </cybox:Stateful_Measure>
</cybox:Observable>
```

Domain Name Object

```
<cybox:Observable id="cybox:observable-6f45e4fc-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
        <cybox:Object id="cybox:guid-6dcb9414-30c8-11e2-8011-000c291a73d5">
            <cybox:Defined_Object xsi:type="URIObj:URIObjectType" type="Domain Name">
                <URIObj:Value datatype="AnyURI">state.gov</URIObj:Value>
            </cybox:Defined_Object>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="cybox:guid-6eba12f6-30c8-11e2-8011-000c291a73d5" type="WHOIS" relationship="Resolved_To"/>
                <cybox:Related_Object idref="cybox:guid-6eba1dc8-30c8-11e2-8011-000c291a73d5" type="DNS Query" relationship="Properties_Queried_By"/>
                <cybox:Related_Object idref="cybox:guid-6ec1cb36-30c8-11e2-8011-000c291a73d5" type="DNS Record" relationship="Characterized_By"/>
                <cybox:Related_Object idref="cybox:guid-6ec1c8de-30c8-11e2-8011-000c291a73d5" type="IP Address" relationship="Resolved_To"/>
                <cybox:Related_Object idref="cybox:guid-6ec1cdf2-30c8-11e2-8011-000c291a73d5" type="DNS Query" relationship="Properties_Queried_By"/>
                <cybox:Related_Object idref="cybox:guid-6ec8ffaa-30c8-11e2-8011-000c291a73d5" type="DNS Record" relationship="Characterized_By"/>
                <cybox:Related_Object idref="cybox:guid-6ec8fd2a-30c8-11e2-8011-000c291a73d5" type="IP Address" relationship="Resolved_To"/>
                <cybox:Related_Object idref="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5" type="URL" relationship="Extracted_From"/>
                <cybox:Related_Object idref="cybox:guid-6dcb5fda-30c8-11e2-8011-000c291a73d5" type="URL" relationship="Sub-domain_Of"/>
            </cybox:Related_Objects>
        </cybox:Object>
    </cybox:Stateful_Measure>
 </cybox:Observable>
```

DNS Query Object

```
<cybox:Observable id="cybox:observable-6f45fca8-30c8-11e2-8011-000c291a73d5">
  <cybox:Stateful_Measure>
    <cybox:Object id="cybox:guid-6ec1cdf2-30c8-11e2-8011-000c291a73d5">
      <cybox:Defined_Object xsi:type="DNSQueryObj:DNSQueryObjectType" successful="true">
        <DNSQueryObj:Question>
          <DNSQueryObj:QName xsi:type="URIObj:URIObjectType" type="Domain Name">
            <URIObj:Value datatype="AnyURI">state.gov</URIObj:Value>
          </DNSQueryObj:QName>
          <DNSQueryObj:QType datatype="String">AAAA</DNSQueryObj:QType>
          <DNSQueryObj:QClass datatype="String">IN</DNSQueryObj:QClass>
        </DNSQueryObj:Question>
        <DNSQueryObj:Answer_Resource_Records>
          <DNSQueryObj:Resource_Record xsi:type="DNSRecordObj:DNSRecordObjectType" object_reference="cybox:guid-6ec8ffaa-30c8-11e2-8011-00
        </DNSQueryObj:Answer_Resource_Records>
      </cybox:Defined_Object>
      <cybox:Related_Objects>
        <cybox:Related_Object idref="cybox:guid-6dcb9414-30c8-11e2-8011-000c291a73d5" type="URI" relationship="Properties_Queried"/>
        <cybox:Related_Object idref="cybox:guid-6ec8ffaa-30c8-11e2-8011-000c291a73d5" type="DNS Record" relationship="Searched_For"/>
      </cybox:Related_Objects>
    </cybox:Object>
  </cybox:Stateful_Measure>
</cybox:Observable>
```

DNS Record Object

```
<cybox:Observable id="cybox:observable-6f45dbec-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-6ec8ffaa-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="DNSRecordObj:DNSRecordObjectType">
          <DNSRecordObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
            <URIObj:Value datatype="AnyURI">state.gov</URIObj:Value>
          </DNSRecordObj:Domain_Name>
          <DNSRecordObj:IP_Address xsi:type="AddressObj:AddressObjectType" category="ipv6-addr">
            <AddressObj:Address_Value datatype="String">2001:428:d400:4:72:166:186:151</AddressObj:Address_Value>
          </DNSRecordObj:IP_Address>
          <DNSRecordObj:Entry_Type datatype="String">AAAA</DNSRecordObj:Entry_Type>
          <DNSRecordObj:Flags datatype="hexBinary">8180</DNSRecordObj:Flags>
          <DNSRecordObj:Record_Data>id 10546
opcode QUERY
rcode NOERROR
flags QR RD RA
;QUESTION
state.gov. IN AAAA
;ANSWER
state.gov. 5 IN AAAA 2001:428:d400:4:72:166:186:151
;AUTHORITY
;ADDITIONAL</DNSRecordObj:Record_Data>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:guid-6ec1cdf2-30c8-11e2-8011-000c291a73d5" type="DNS Query"
relationship="Searched_For_By"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

IP Address Object

Observable

```
<cybox:Observable id="cybox:observable-6f45f992-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-6ec8fd2a-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="AddressObj:AddressObjectType" category="ipv6-addr">
          <AddressObj:Address_Value datatype="String">2001:428:d400:4:72:166:186:151</AddressObj:Address_Value>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:guid-6dcb9414-30c8-11e2-8011-000c291a73d5" type="URI" relationship="Resolved_To"/>
          <cybox:Related_Object idref="cybox:guid-6ec1cdf2-30c8-11e2-8011-000c291a73d5" type="DNS Query" relationship="Contained_Within"/>
          <cybox:Related_Object idref="cybox:guid-6ec8ffaa-30c8-11e2-8011-000c291a73d5" type="DNS Record" relationship="Contained_Within"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

WHOIS Object

```
<cybox:Observable id="cybox:observable-6f45d6ce-30c8-11e2-8011-000c291a73d5">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-6eba12f6-30c8-11e2-8011-000c291a73d5">
        <cybox:Defined_Object xsi:type="WhoisObj:WhoisObjectType">
          <WhoisObj:Domain_Name xsi:type="URIObj:URIObjectType" type="Domain Name">
            <URIObj:Value datatype="AnyURI">state.gov</URIObj:Value>
          </WhoisObj:Domain_Name>
          <WhoisObj:Status datatype="String">OK</WhoisObj:Status>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:guid-6dcb9414-30c8-11e2-8011-000c291a73d5" type="URI" relationship="Resolved_To"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

Potential STIX-enabled Phishing Analysis (Continued)

4. List of emails submitted to suspicious@XXX.YYY are structured and prioritized (based on reputation analysis or other policy-driven maliciousness characterization) analysis results of the email are presented to the analyst.
    - Automates the first steps of analysis that must be performed on each email and shortens response time for real threats by enabling the analyst to work on likely malicious issues first.

5. Analyst can leverage structured representations to quickly query if this email or similar have been seen before or sent to others within XXX.

6. Analyst reviews suspicious email and any related emails (including shared Indicators), identifies unique characteristics, and captures them in an appropriate Observables (CybOX) pattern.

In this example, the analyst creates a pattern for any email from an email address with the domain name “state.gov” and with a PDF file attached that has a size of 87022 bytes and an MD5 hash= cf2b3ad32a8a4cfb05e9dfc45875bd70.

Observable Pattern

Observable

```
<cybox:Observable id="cybox:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
  <cybox:Stateful_Measure>
     <cybox:Object id="cybox:object-3a7aa9db-d082-447c-a422-293b78e24238">
         <cybox:Defined_Object xsi:type="EmailMessageObj:EmailMessageObjectType">
           <EmailMessageObj:Header>
             <EmailMessageObj:From category="e-mail">
               <AddressObj:Address_Value datatype="String" condition="Contains">@state.gov</AddressObj:Address_Value>
             </EmailMessageObj:From>
           </EmailMessageObj:Header>
         </cybox:Defined_Object>
         <cybox:Related_Objects>
           <cybox:Related_Object type="File" relationship="Contains">
               <cybox:Defined_Object xsi:type="FileObj:FileObjectType">
                      <FileObj:File_Extension datatype="String" condition="Equals">pdf</FileObj:File_Extension>
                      <FileObj:Size_In_Bytes datatype="UnsignedLong" condition="Equals">87022</FileObj:Size_In_Bytes>
                      <FileObj:Hashes>
                             <Common:Hash>
                                    <Common:Type datatype="String" condition="Equals">MD5</Common:Type>
                                    <Common:Simple_Hash_Value datatype="hexBinary" condition="Equals">
                                           cf2b3ad32a8a4cfb05e9dfc45875bd70
                                    </Common:Simple_Hash_Value>
                             </Common:Hash>
                      </FileObj:Hashes>
               </cybox:Defined_Object>
           </cybox:Related_Object>
         </cybox:Related_Objects>
       </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

Create STIX Indicator

```
<TTP:KillChains>
        <TTP:KillChain id="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff" name="LMCO Kill Chain"
definer="LMCO"
reference="http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-
White-Paper-Intel-Driven-Defense.pdf" numberOfPhases="7">
                <stixCommon:KillChainPhase phaseID="stix:TTP-af1016d6-a744-4ed7-ac91-00fe2272185a"
<Indicator:IndicatorType>Phishing Attempt</Indicator:IndicatorType>
<Indicator:Name>"US-China" Phishing Indicator</Indicator:Name>
name="Weaponization" ordinality="2"/>
<Indicator:Description><Common:Text>This is a cyber threat indicator for instances of "US-China"
phishing attempts.</Common:Text></Indicator:Description>
<Indicator:ValidTimePosition>
        <Indicator:start-time>2012-12-01T09:30:47Z</Indicator:start-time>
        <Indicator:end-time>2013-02-01T09:30:47Z</Indicator:end-time>
</Indicator:ValidTimePosition>
defined in the snippet above.-->
    <Indicator:Observable idref="cybox:observable-pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
    </Indicator:Observable>
</Indicator:Observables>
        </TTP:Behavior-AttackPatterns>
</Indicator:IndicatedTTP>
<Indicator:KillChainPhases>
        <Indicator:kill-chain-phase phaseID="stix:TTP-79a0e041-9d5f-49bb-ada4-8322622b162d"
name="Delivery" ordinality="3" killChainID="stix:TTP-af3e707f-2fb9-49e5-8c37-14026ca0a5ff"
killChainName="LMCO Kill Chain"/>
</Indicator:KillChainPhases>
```

If Phishing Lure was Executed, Create a STIX Incident

- Time
  - Granular set of Incident lifecycle timestamps
- Description
- Roles (Reporter, Responder, Coordinator, Victim)
- Affected Assets
- Impact Assessment
- Related Indicators
- Leveraged TTP
- Related Threat Actors
- Intent
- Discovery Method
- Related Incidents
- COA Requested / COA Taken
- Confidence
- Contact
- History

Incident

Potentially Package with Content on Suspected Campaign & ThreatActor

- Campaign
  - Names
  - Intent
  - Related TTPs
  - Related Incidents
  - Related Indicators
  - Attribution
  - Associated Campaigns
  - Confidence
  - Activity
  - Information Source

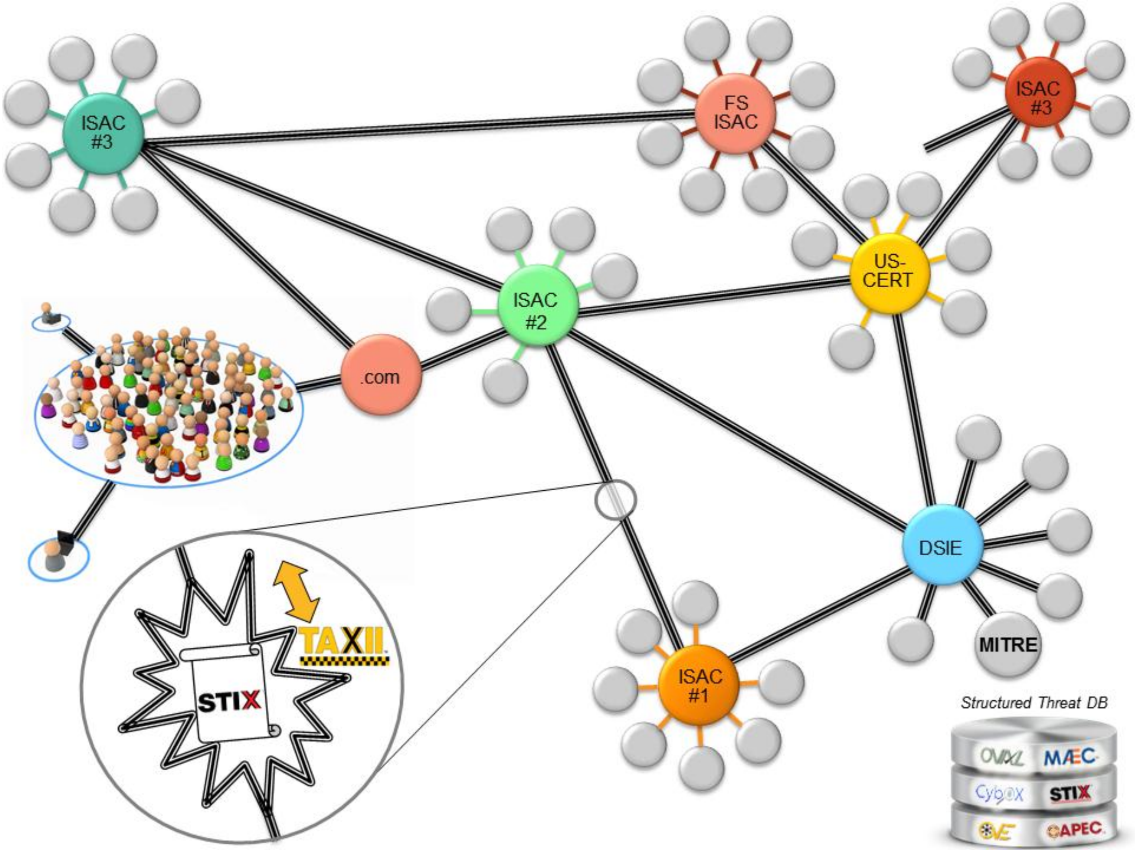
- ThreatActor
  - Identity
  - Intent
  - Observed TTPs
  - Historical Campaigns
  - Associated Actors
  - Handling
  - Confidence
  - Information Source

Sharing Phishing Information

- All of this information can then easily be shared with trusted partners via TAXII

TAXII™

Trusted Automated eXchange of Indicator Information



Where to Learn More

- STIX Website (whitepapers, documentation, schemas, etc.)
  - http://stix.mitre.org
- STIX GitHub site (bindings, APIs, utilities)
  - https://github.com/STIXProject
- STIX Discussion List
  - http://stix.mitre.org/community/registration.html

- TAXII Website (whitepapers, specifications, etc.)
  - http://taxii.mitre.org
- TAXII Discussion List
  - http://taxii.mitre.org/community/registration.html
- TAXII GitHub site (bindings, APIs, utilities, implementations)
  - https://github.com/TAXIIProject

- Questions
  - stix@mitre.org
  - taxii@mitre.org

Orient on the Adversary!

We want you to be part of the conversation.

stix@mitre.org

https://stix.mitre.org

STIX™
Structured Threat Information eXpression

RSΛCONFERENCE2013