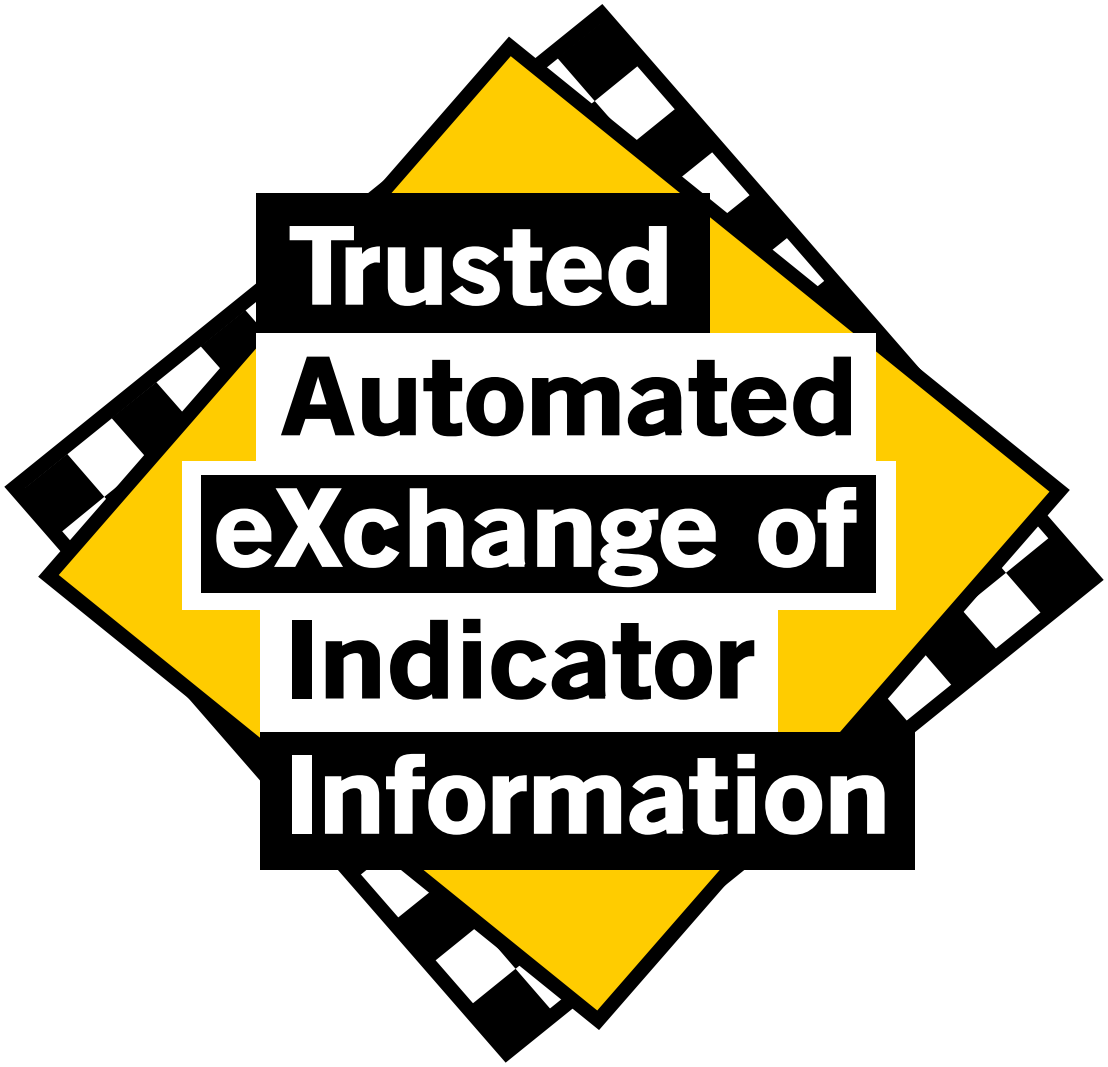


Richard Struse

Deputy Director for Software Assurance

DHS NCSD GCSM

“Information Sharing”

- Means many things to many people – need to be more specific
- Our focus: enabling the exchange of *actionable*, machine-consumable *indicators* of cyber threats
- Goal: empower organizations to easily share:
  - The information ***they choose*** to share,
  - With the organizations ***they choose*** to share with.

Why Share Indicators?

- Goal: Enable the detection, prevention and mitigation of threats in real (or near-real) time
- Empower organizations to achieve improved situational awareness about emerging threats
- Leading to “my detection becomes your prevention”
  - Automating identification, prevention or mitigation ***before*** something bad happens

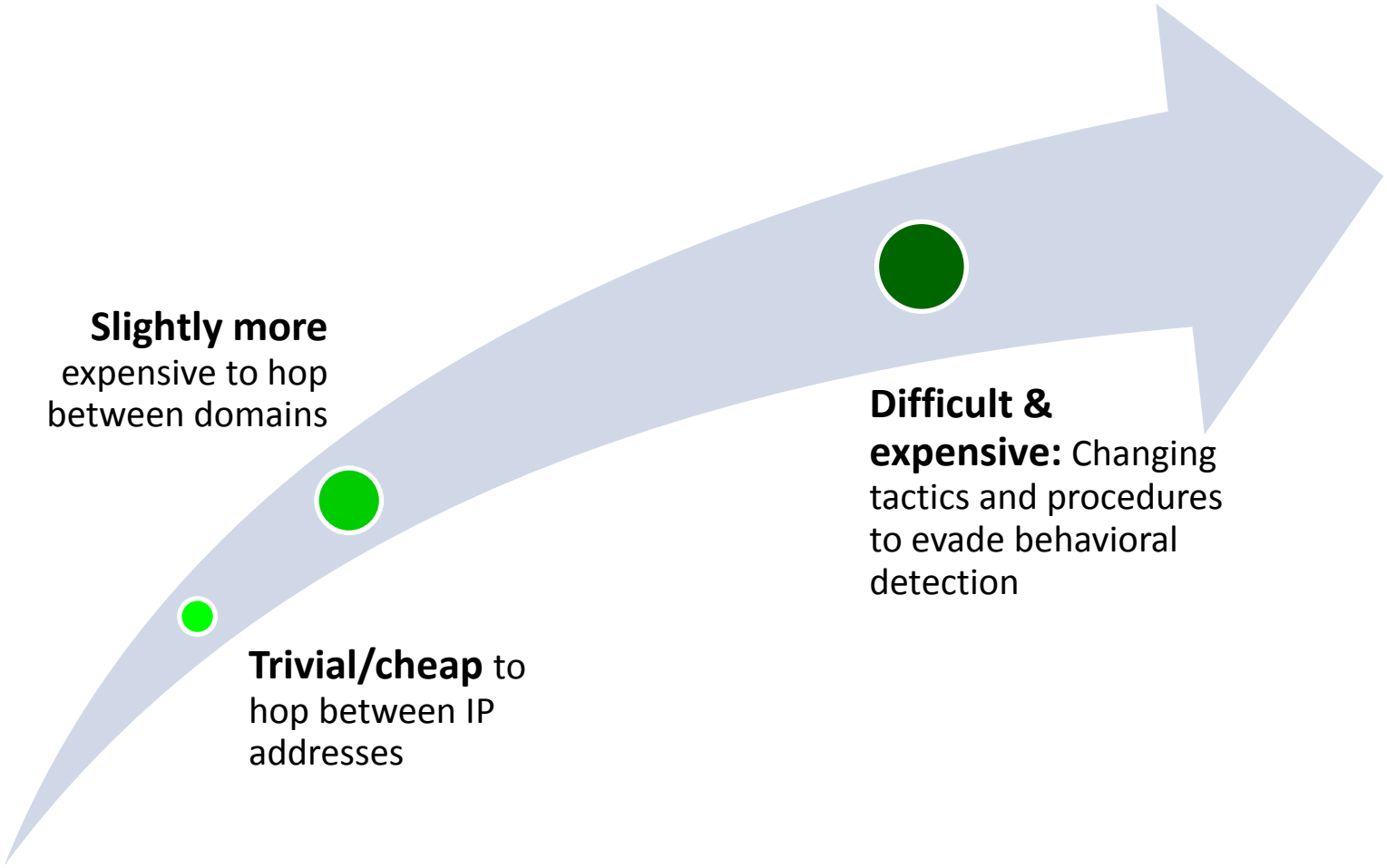
Indicators

- Composite of cyber observables (facts) and contextual information
- Observables: measureable events and stateful properties on systems and networks
  - Examples: network addresses, domain names, file metadata, protocol components (headers, flags, etc.), registry keys, etc.
- Contextual information: source, sensitivity, confidence, impact, relationships, etc.
- What about “actors and objectives?” – Important, but not always part of ***indicators***, per se.

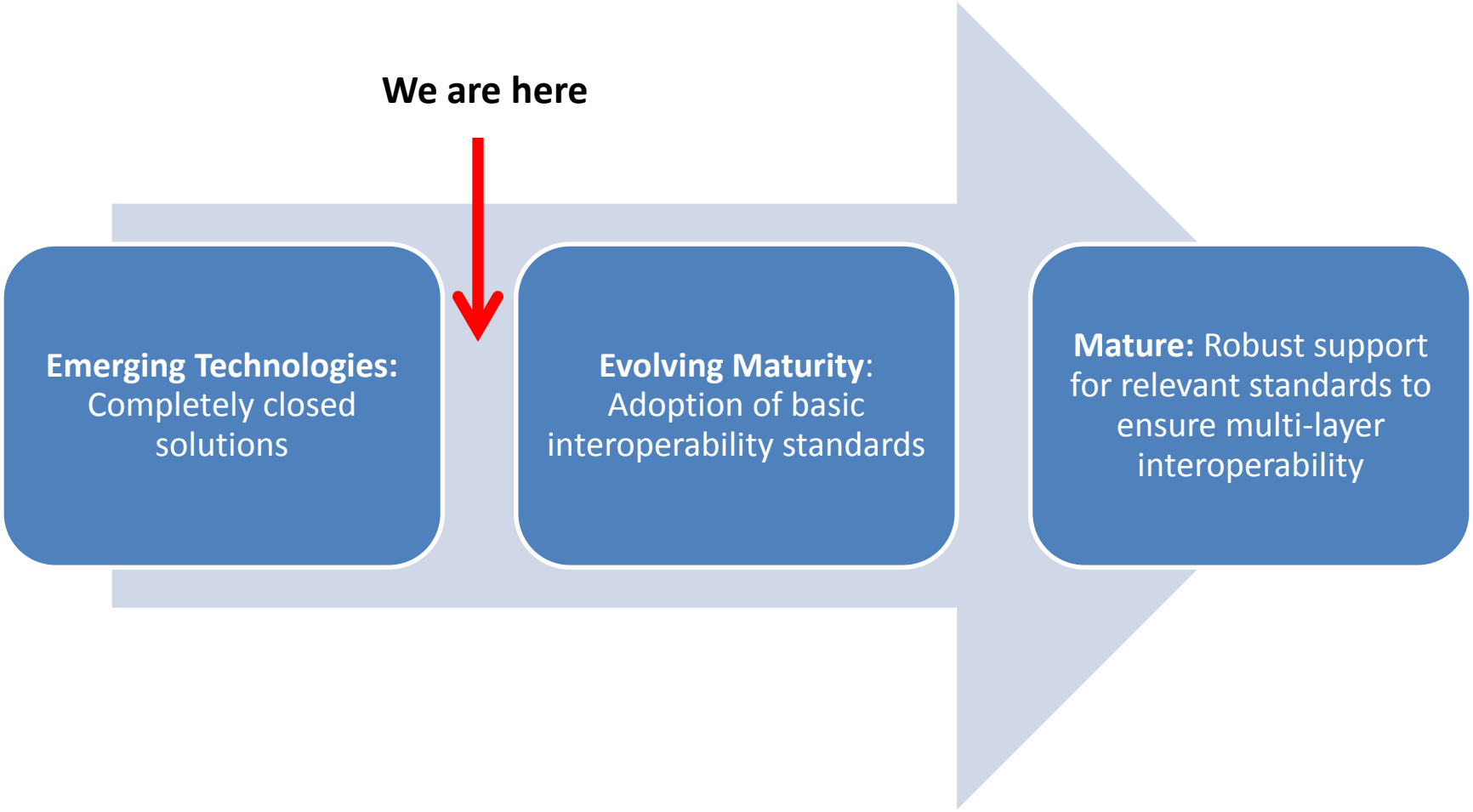
TAXII: Trusted Automated eXchange of Indicator Information

- **Protocol(s)** and **data representations** for indicator exchange
- Ultimate intent is to allow representation and sharing of ***"behavioral indicators"*** in addition to common types such as IP/domain watchlists and hash + size signatures
- Behavioral indicators can express arbitrary combinations and time sequences of observables, resulting in less perishable and more reliable detection techniques
- Force adversaries to expend significantly greater resources to evade detection

Cost to Adversary



Market Evolution: Threat/indicator Sharing



Landscape

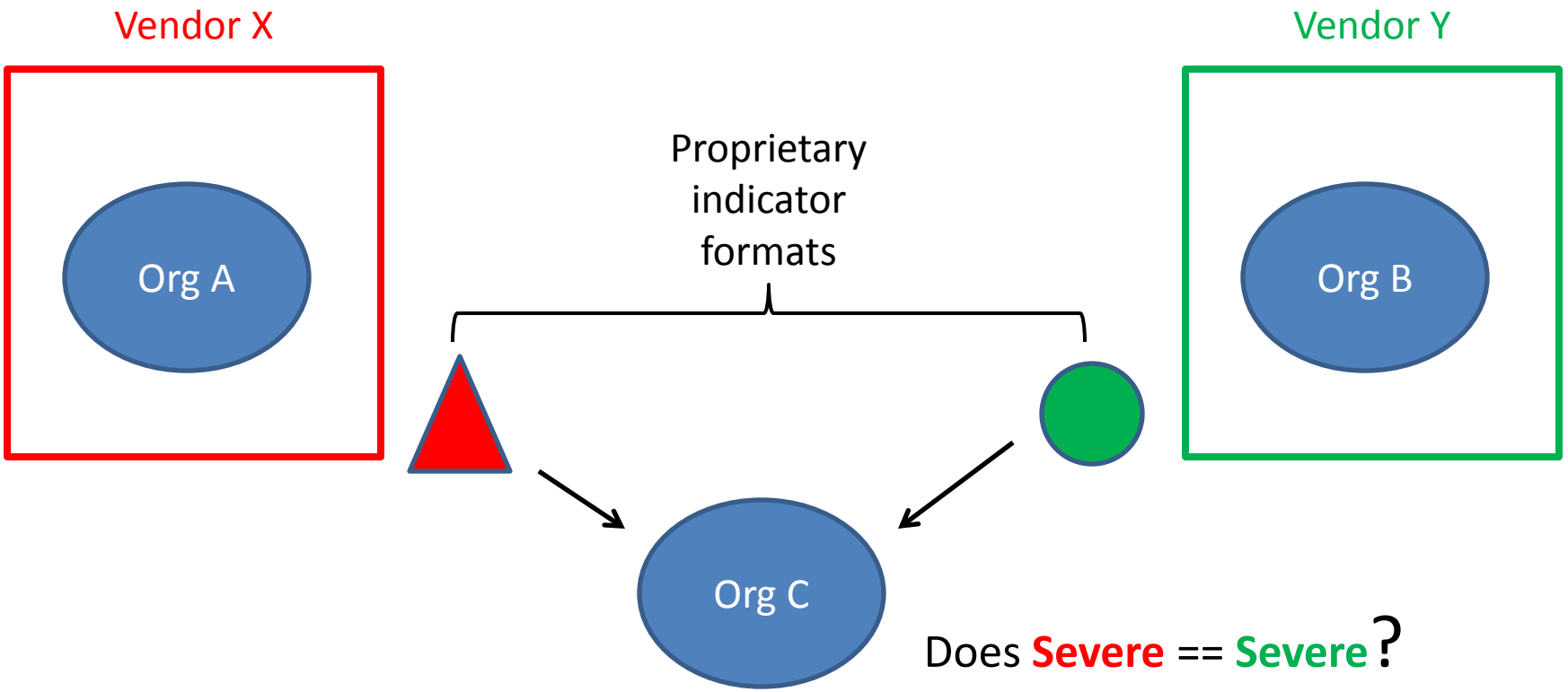
Today:

Some vendors/service providers support automated dissemination of selected indicator information today – *within their solution boundaries*

Our Vision:

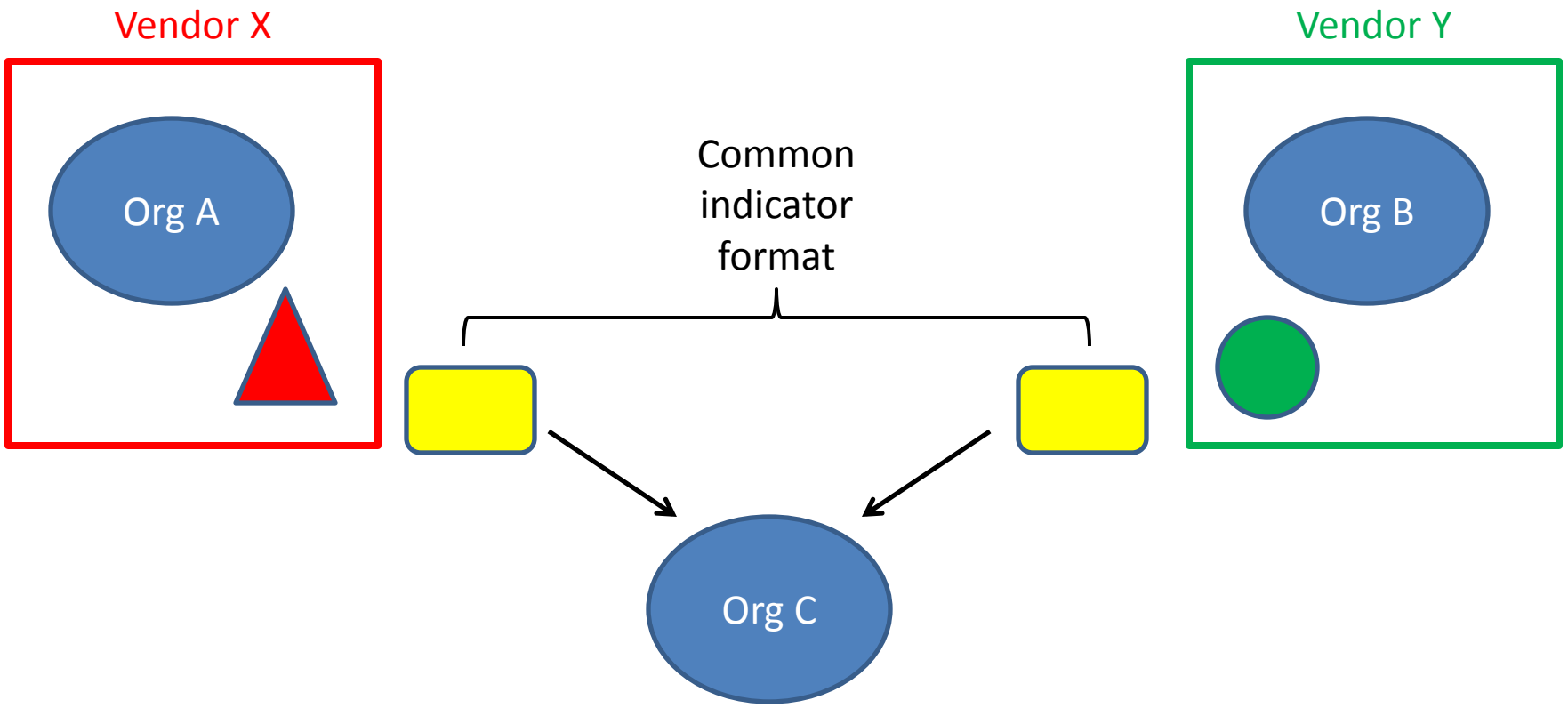
Indicator sharing must grow to cross organizational and technological boundaries – no one vendor covers 100% of the market

Sharing Challenges



- Org C must understand *each* format in use and try to map across formats – sacrificing time and potentially losing information
- Duplication of effort at each organization in the exchange is expensive and does not scale

Enabling Cross-Vendor Sharing



- Org C only needs to understand one format – no need to map and no information loss
- Each vendor maps their internal representations to the common format *once* – efficient and scalable

Limited Scope

TAXII will specify

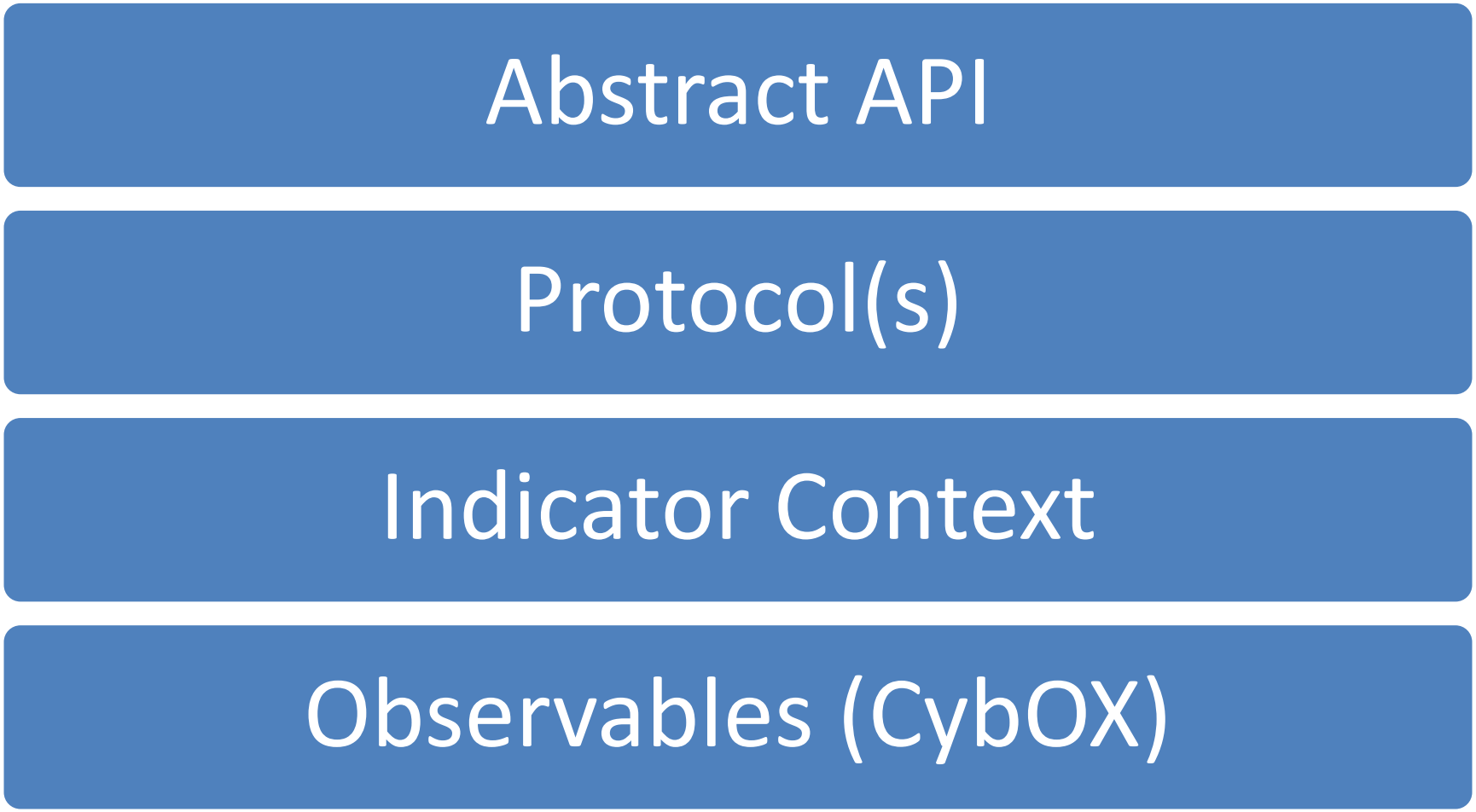
- Data representations for indicators and observables
- Protocol(s) for exchanging indicators securely

These areas remain open for experimentation, innovation and tailoring

TAXII will NOT Specify

- Collection – how indicators are obtained or generated
- Analytics – how indicators are scored or evaluated
- Process – how an indicator is employed or shared with others
- Mitigation – how indicators are used to protect assets
- Internal representations

TAXII: High-level Architecture



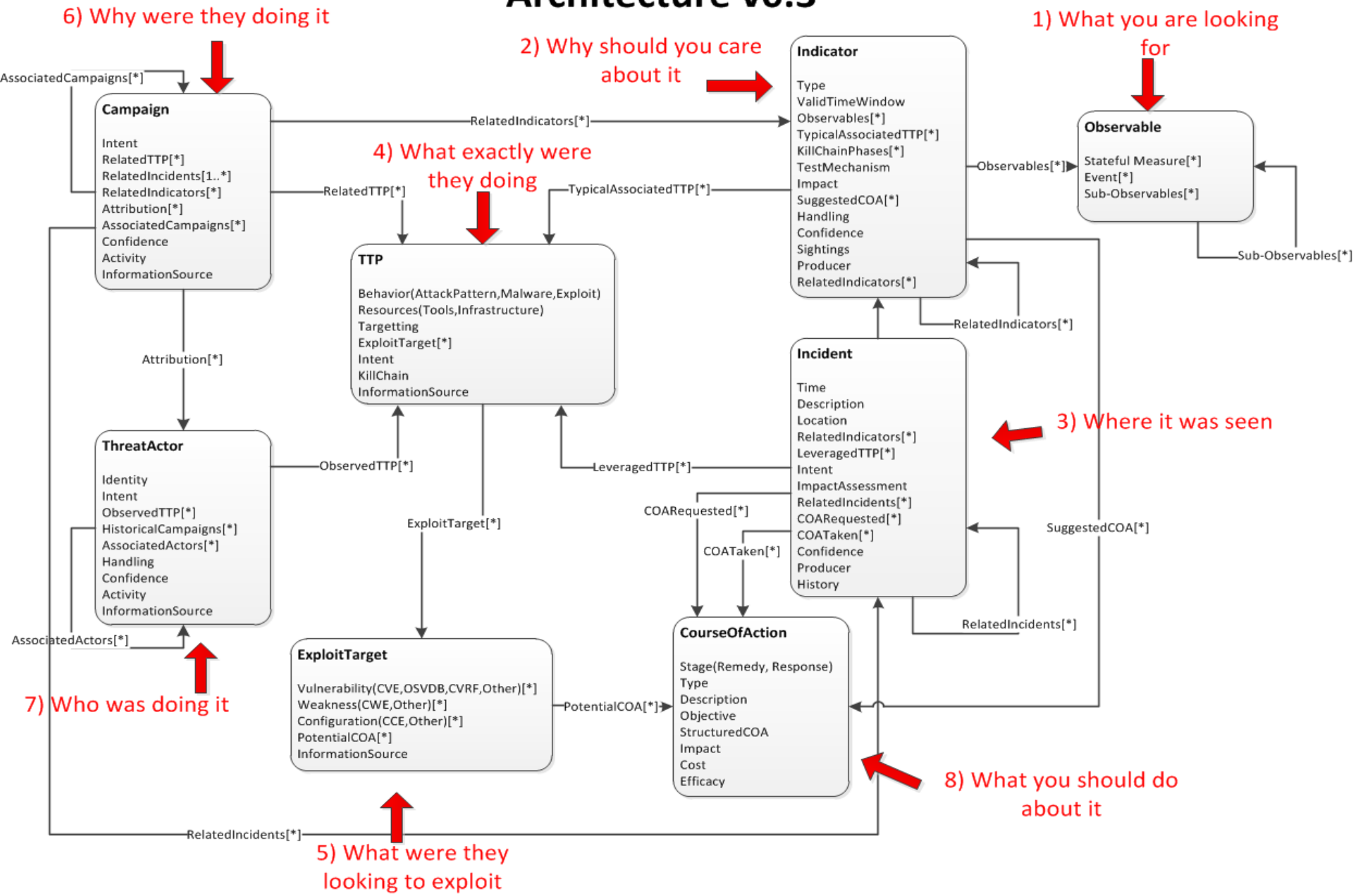
The Structured Threat Information eXpression (STIX)

- STIX is a language for the specification, capture, characterization and communication of cyber threat information.
- Use cases include:
  - Analyzing cyber threats
  - Specifying indicator patterns for cyber threat
  - Managing cyber threat response activities
  - Sharing cyber threat information

STIX (continued)

- Unifying architecture tying together a diverse set of cyber threat information including:
  - Cyber Observables
  - Indicators
  - Incidents
  - Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, targeting, etc.)
  - Exploit Targets (e.g., vulnerabilities and weaknesses)
  - Courses of Action (e.g., incident response or vulnerability/weakness remedies)
  - Cyber Attack Campaigns
  - Cyber Threat Actors

Structured Threat Information eXpression (STIX) Architecture v0.3



CybOX: Cyber Observable eXpression

- DHS-sponsored, MITRE-led community-defined specification for ‘facts’ in the cyber domain
- Designed to be extensible by the community
- Version 1.0 (draft) release: April 17
- Formal specification independent of representation
- XML binding defined, additional bindings can be added (e.g. JSON)
- cybox.mitre.org

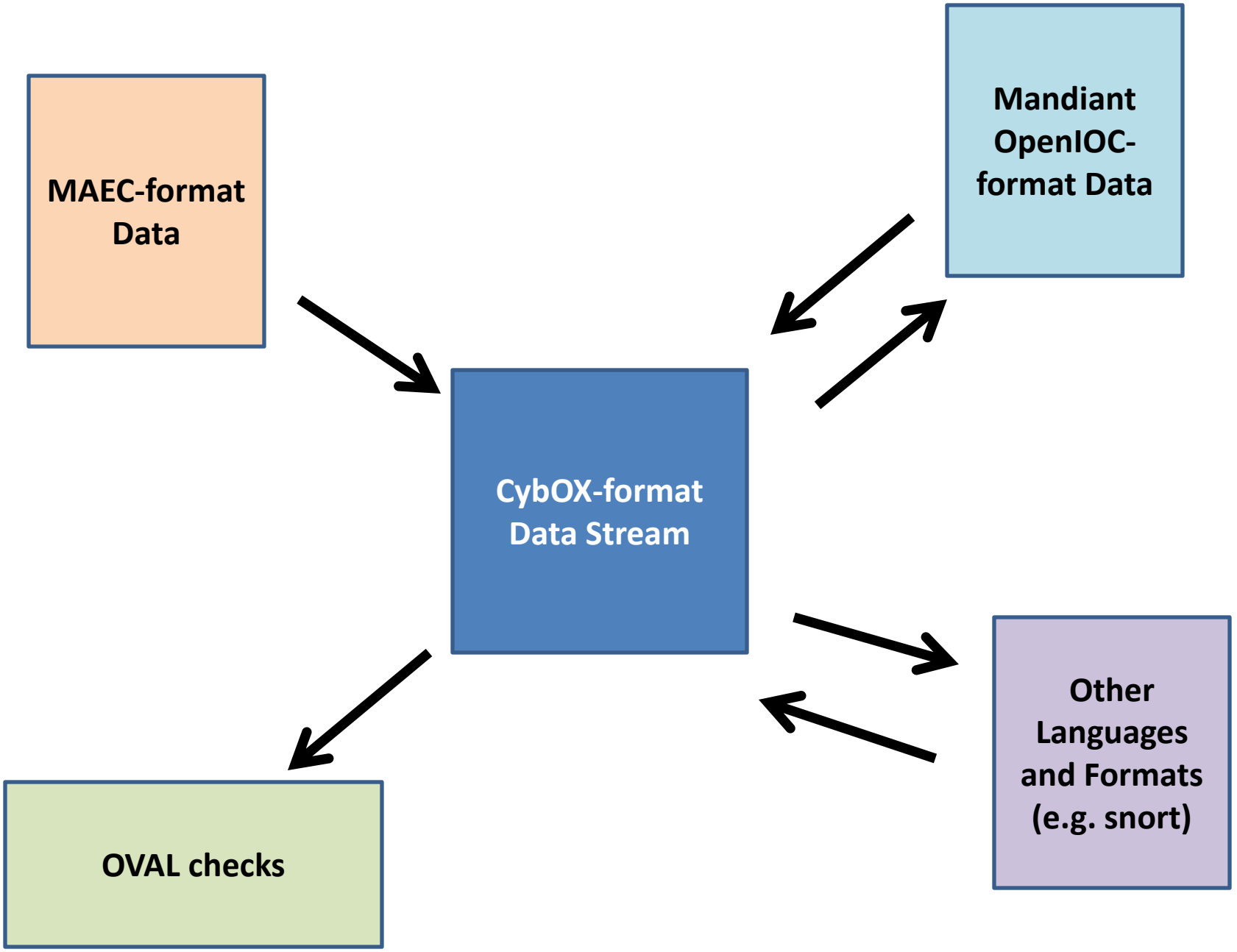
CybOX - Expressivity

- Large number of objects defined and is user-extensible
- Each object has a rich set of (optional) elements
- Object patterns can be expressed as arbitrary Boolean expressions using AND, OR, NOT
- Comparisions supported include relational operators, InSet, InRange, regexes

CybOX v1.0 Objects

- Account
- Address
- Disk
- Disk Partition
- DNS Entry
- DNS Cache
- Email Message
- File
- GUI
- GUI Dialog Box
- GUI Window
- Library
- Linux Package
- Memory
- Mutex
- Network Connection
- Network Flow
- Network Route
- Network Subnet
- Network Packet
- Pipe
- Port
- Process
- Product
- Semaphore
- Service
- Socket
- System
- Unix File
- Unix Network Route
- Unix Pipe
- Unix Process
- Unix User Account
- Unix Volume
- URI
- User Account
- User Session
- Volume
- Win Computer Account
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Executable File
- Win File
- Win Kernel
- Win Kernel Hook
- Win Handle
- Win Mailslot
- Win Mutex
- Win Pipe
- Win Network Route
- Win Network Share
- Win Prefetch
- Win Process
- Win Registry
- Win Semaphore
- Win Service
- Win System
- Win System Restore
- Win Task
- Win Thread
- Win User Account
- Win Volume
- Win Waitable Timer
- X509 Certificate

(more on the way)


MAEC-format Data
Mandiant OpenIOC-format Data
CybOX-format Data Stream
OVAL checks
Other Languages and Formats (e.g. snort)

CybOX: Resources

- Resources (released under New BSD license)
  - Snort -> CybOX
  - OpenIOC -> CybOX and CybOX -> OpenIOC
  - CybOX -> OVAL
  - Full set of Python bindings for CybOX
  - Email -> CybOX parsing tool

CybOX in Action: Spear phishing Example

Suspected Spear phishing email:

From: Jon Doe <jdoe@yahoo.com>
Sent: Tuesday, June 19, 2012 5:21 AM
To: Robert Smith <rsmith@megacorp.com>
Subject: Completed Analysis
Attachments: AnalysisSummary.exe.doc

Attached is the summary for the analysis that you requested. This is CONFIDENTIAL so do not share with anyone outside the group. The full summary can be found here:
http://www.consultingservize.net/archives/Analysis.pdf

Regards,
Jonathan Doe
Senior Analyst
Consulting Services, LLC

The email is run through the email-to-CybOX parser to generate a *complete* representation of the email, including attachments and embedded links

CybOX Representation of Email Headers

```
</cybox:Observable>
  <cybox:Observable id="cybox:observable-ff7819ac-c217-11e1-b047-0024e82077cd">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-ff7816b4-c217-11e1-b047-0024e82077cd">
        <cybox:Defined_Object xsi:type="EmailMessageObj:EmailMessageObjectType">
          <EmailMessageObj:Attachments>
            <EmailMessageObj:File xsi:type="FileObj:FileObjectType" object_reference="cybox:guid-ff77d2bc-
    c217-11e1-b047-0024e82077cd"/>
          </EmailMessageObj:Attachments>
          <EmailMessageObj:Header>
            <EmailMessageObj:To>
              <EmailMessageObj:Recipient category="e-mail">
                <AddressObj:Address_Value datatype="String">rsmith@megacorp.com
                </AddressObj:Address_Value>
              </EmailMessageObj:Recipient>
            </EmailMessageObj:To>
            <EmailMessageObj:From category="e-mail">
              <AddressObj:Address_Value datatype="String">jdoe@yahoo.com
              </AddressObj:Address_Value>
            </EmailMessageObj:From>
            <EmailMessageObj:Subject datatype="String">Completed Analysis
            </EmailMessageObj:Subject>
            <EmailMessageObj:Date datatype="DateTime">2012-06-19T05:21:07-07:00
            </EmailMessageObj:Date>
            <EmailMessageObj:Message_ID
    datatype="String">20120619052107.7fce262a4747103829365740aac88c24.65fb2854aa.wbe@email04.secure
    server.net
            </EmailMessageObj:Message_ID>
          </EmailMessageObj:Header>
```

CybOX Representation of Email Headers (cont)

<EmailMessageObj:Optional_Header>
<EmailMessageObj:Content-Type datatype="String">multipart/mixed; boundary="=_3e7b6dc86e97030872156d0ed4b813b0“
</EmailMessageObj:Content-Type>
<EmailMessageObj:MIME-Version datatype="String">1.0
</EmailMessageObj:MIME-Version>
<EmailMessageObj:X-Originating-IP category="ipv4-addr">
<AddressObj:Address_Value datatype="String">**67.32.219.198**
</AddressObj:Address_Value>
</EmailMessageObj:X-Originating-IP>
</EmailMessageObj:Optional_Header>
<EmailMessageObj:Raw_Body datatype="String"><![CDATA[<html>
<head>
</head>
<body>Attached is the summary for the analysis that you requested. This is CONFIDENTIAL so do not share with anyone outside the group.
The full summary can be found here: http://www.consultingservize.net/archives/Analysis.pdf

Regards,
Jonathan Doe
Senior Analyst
Consulting Services, LLC
</body></html>]]></EmailMessageObj:Raw_Body>
</cybox:Defined_Object>
</cybox:Object>
</cybox:Stateful_Measure>
</cybox:Observable>
</cybox:Observables>

CybOX Representation of Email Embedded Links

```
<cybox:Observable id="cybox:guid-ff78208c-c217-11e1-b047-0024e82077cd">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-ff7814fc-c217-11e1-b047-0024e82077cd">
        <cybox:Defined_Object xsi:type="URIObj:URIObjectType" type="URL">
          <URIObj:Value datatype="AnyURI">
          http://www.consultingservize.net/archives/Analysis.pdf
          </URIObj:Value>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:guid-ff7816b4-c217-11e1-b047-0024e82077cd"
    type="Email Message" relationship="Contained_Within"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

CybOX Representation of Email Attachment

```
<cybox:Observable id="cybox:guid-ff781d80-c217-11e1-b047-0024e82077cd">
    <cybox:Stateful_Measure>
      <cybox:Object id="cybox:guid-ff77d2bc-c217-11e1-b047-0024e82077cd">
        <cybox:Defined_Object xsi:type="FileObj:FileObjectType">
          <FileObj:File_Name datatype="String">AnalysisSummary.exe.doc</FileObj:File_Name>
          <FileObj:Size_In_Bytes datatype="UnsignedLong">92672</FileObj:Size_In_Bytes>
          <FileObj:Hashes>
            <Common:Hash>
              <Common:Type datatype="String">MD5</Common:Type>
              <Common:Simple_Hash_Value datatype="hexBinary">
                  181aea20e3f50b5d0560f6f926943436</Common:Simple_Hash_Value>
            </Common:Hash>
            <Common:Hash>
              <Common:Type datatype="String">SHA1</Common:Type>
              <Common:Simple_Hash_Value datatype="hexBinary">
                  d406fee7f297b3248d3a965051931dc95d5cf927</Common:Simple_Hash_Value>
            </Common:Hash>
          </FileObj:Hashes>
        </cybox:Defined_Object>
        <cybox:Related_Objects>
          <cybox:Related_Object idref="cybox:guid-ff7816b4-c217-11e1-b047-0024e82077cd"
              type="Email Message" relationship="Contained_Within"/>
        </cybox:Related_Objects>
      </cybox:Object>
    </cybox:Stateful_Measure>
  </cybox:Observable>
```

Indicator Context Layer

- Cyber Observables = ‘Facts’
- Indicator Context = ‘Opinions’
- Includes
  - Confidence assessments/scores
  - Severity assessments/scores
  - Sensitivity/sharing restrictions

Protocols and APIs

- Intent is to define a basic set of abstract APIs
- Define bindings to specific implementations:
  - e.g. SOAP over HTTP/TLS
- Considering re-use of various existing protocols

TAXII: Value Proposition

For users: Better ***management of risk*** by seamlessly integrating comprehensive threat intelligence from partners, providers, ISACs, and government

For vendors: Deliver greater ***value to customers*** by tapping more diverse sources of data at little or no cost, increasing solution effectiveness and utility

For the nation: Enhance ***trust in cyberspace*** through improved situational awareness, accelerating the identification, prevention and mitigation of threats

Questions?

Richard Struse
Deputy Director
Software Assurance
National Cyber Security Div.

U.S. Department of Homeland Security
National Protection & Programs Directorate

richard.struse@dhs.gov

Homeland Security

thank you.