Trusted Automated eXchange of Indicator Information

Richard Struse
DHS

Sean Barnum
MITRE

STIX™

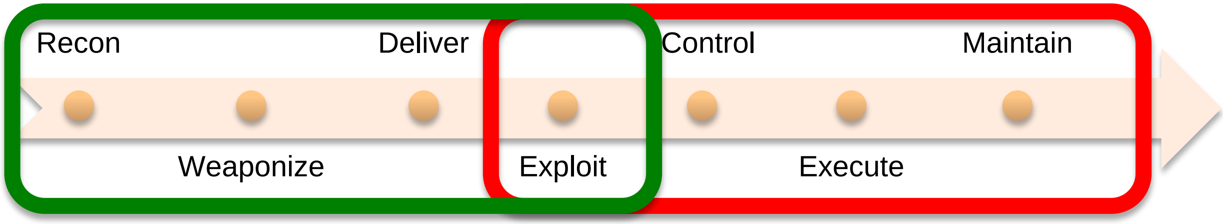
Structured Threat Information eXpression

MITRE

Diverse and evolving threats

Balance inward & outward focus

Proactive & reactive actions


Recon

Deliver

Control

Maintain

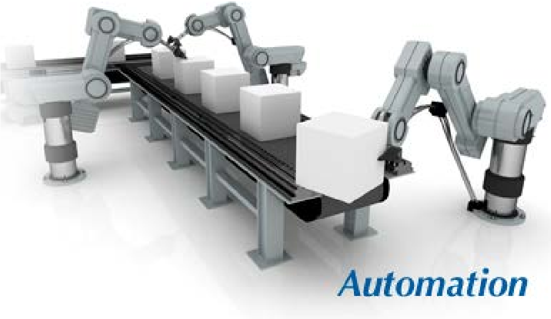
Weaponize

Exploit

Execute

Need for holistic threat intelligence

Information sharing



MITRE

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 indicator sharing is human-to-human exchanges of unstructured descriptions of potential indicators

Often conducted via web-based portals or encrypted email.

A more recent trend is the machine-to-machine transfer of relatively simple sets of indicator data

STIX aims to extend indicator sharing to enable management and exchange of significantly more expressive sets of indicators as well as other full-spectrum cyber threat information.

Evolution of Standardized Representations for Threat

CVE	**Vulnerabilities**
CWE	**Weaknesses**
CAPEC	**Attack Patterns**
MAEC	**Malware Behavior**
CybOX	**Cyber Observables** ← Based on
?	**Threat Indicators** →

IDXWG community of Threat Intel and Incident Response experts begins working on defining a standard representation for cyber threat indicators

What is an Indicator?

Community iterated on scope

Defined Indicator scope as a part of broader cyber threat information architecture

Structured threat information architecture evolved into STIX

MITRE

What is STIX?

Language

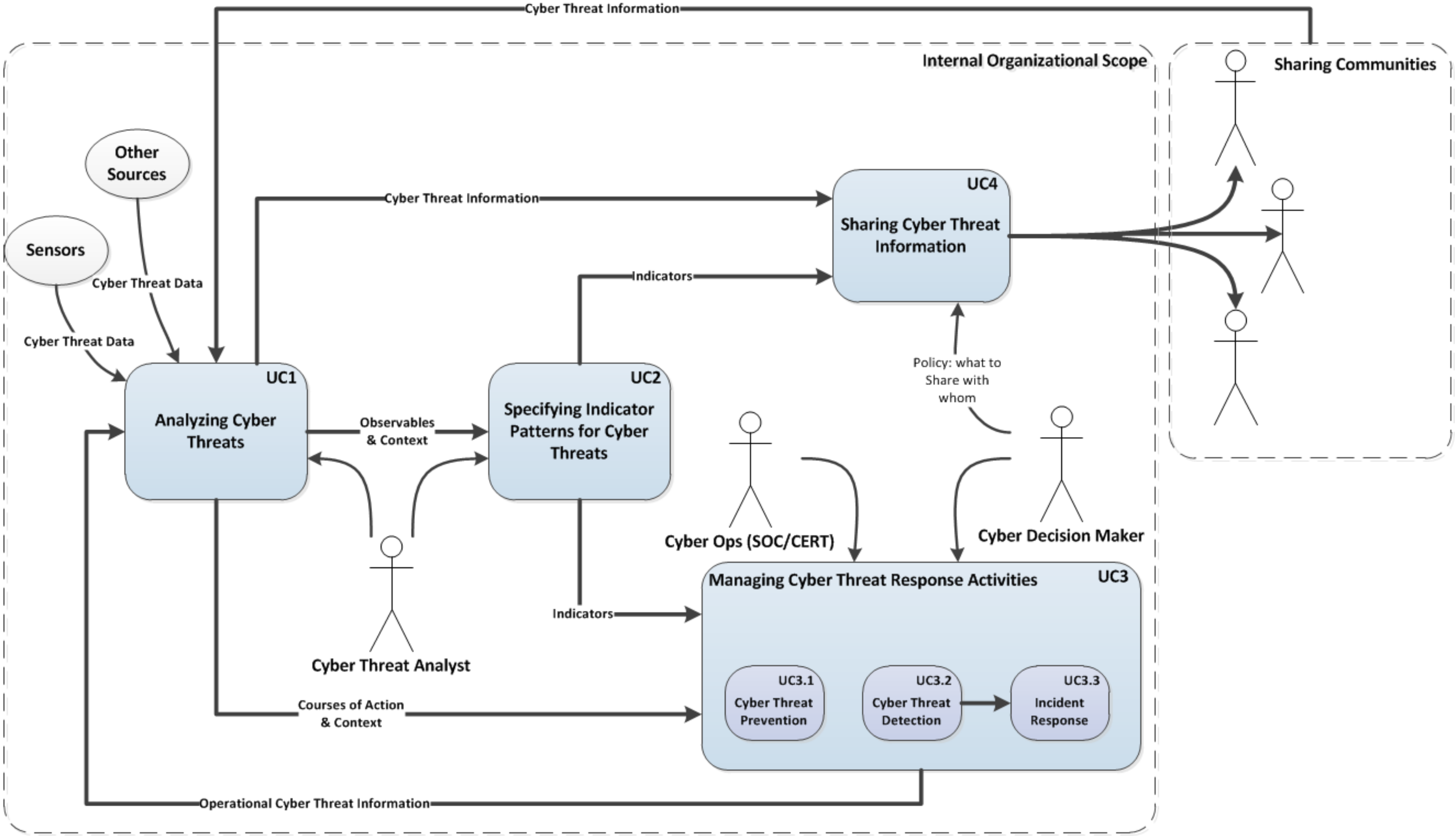
Specify Capture Characterize Communicate

Cyber Threat Information

Community-driven

Consistency Clarity Support automation

STIX Use Cases



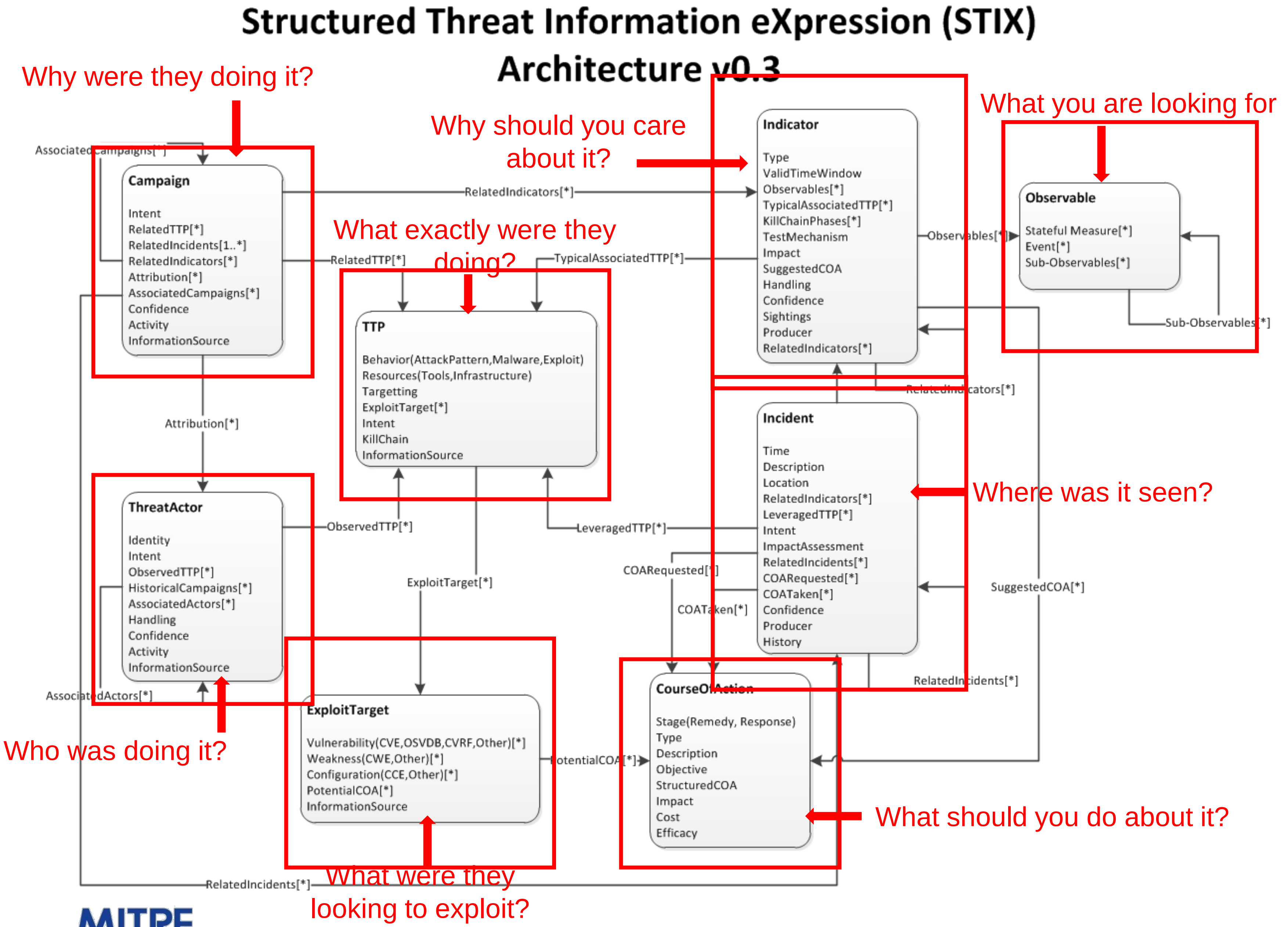
- STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.

MITRE

STIX Guiding Principles

- Expressivity
- Integrate rather than Duplicate
- Flexibility
- Extensibility
- Automatability
- Readability

STIX Architecture



Structured Threat Information eXpression (STIX) Architecture v0.3

Why were they doing it?

Campaign
Intent
RelatedTTP[*]
RelatedIncidents[1..*]
RelatedIndicators[*]
Attribution[*]
AssociatedCampaigns[*]
Confidence
Activity
InformationSource

Why should you care about it?

Indicator
Type
ValidTimeWindow
Observables[*]
TypicalAssociatedTTP[*]
KillChainPhases[*]
TestMechanism
Impact
SuggestedCOA
Handling
Confidence
Sightings
Producer
RelatedIndicators[*]

What you are looking for

Observable
Stateful Measure[*]
Event[*]
Sub-Observables[*]

What exactly were they doing?

TTP
Behavior(AttackPattern,Malware,Exploit)
Resources(Tools,Infrastructure)
Targetting
ExploitTarget[*]
Intent
KillChain
InformationSource

Incident
Time
Description
Location
RelatedIndicators[*]
LeveragedTTP[*]
Intent
ImpactAssessment
RelatedIncidents[*]
COARequested[*]
COATaken[*]
Confidence
Producer
History

Where was it seen?

ThreatActor
Identity
Intent
ObservedTTP[*]
HistoricalCampaigns[*]
AssociatedActors[*]
Handling
Confidence
Activity
InformationSource

Who was doing it?

ExploitTarget
Vulnerability(CVE,OSVDB,CVRF,Other)[*]
Weakness(CWE,Other)[*]
Configuration(CCE,Other)[*]
PotentialCOA[*]
InformationSource

What were they looking to exploit?

CourseOfAction
Stage(Remedy, Response)
Type
Description
Objective
StructuredCOA
Impact
Cost
Efficacy

What should you do about it?

MITRE

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
- Once stable it will be abstracted into an implementation-independent specification.
  - Support other implementations such as semantic web (RDF/OWL), JSON-centric, protobuf, etc.

Adoption & Usage

Still early and immature but already generating extensive interest and initial operational use

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

- Being investigated/considered by several public/public, public/private and private/private information sharing communities
- Active interest from several large “user” organizations
- Active interest from some service/product vendors

MITRE

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

CYBERIQ services

WORLD BANK

FINANCIAL SERVICES ISAC

MANDIANT®

PUNCH -CYBER ANALYTICS GROUP-

NATO OTAN

tripwire

RED SKY® ALLIANCE

USAA®

MITRE

LOOKINGGLASS

CERT

Booz | Allen | Hamilton

LOCKHEED MARTIN

CrowdStrike

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBER2

REN-ISAC

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

DTCC.

VERISIGN

G2

STEGOSYSTEMS invisibility integrity immunity

ICS-ISAC

NCI Security LLC

GENERAL DYNAMICS

IID

verizonbusiness

NIST

Orient on the Adversary!

We want you to be part of the conversation.

Website and community collaboration support coming soon!

stix@mitre.org

https://msm.mitre.org/docs/STIX-Whitepaper.pdf

STIX™
Structured Threat Information eXpression

MITRE

“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.

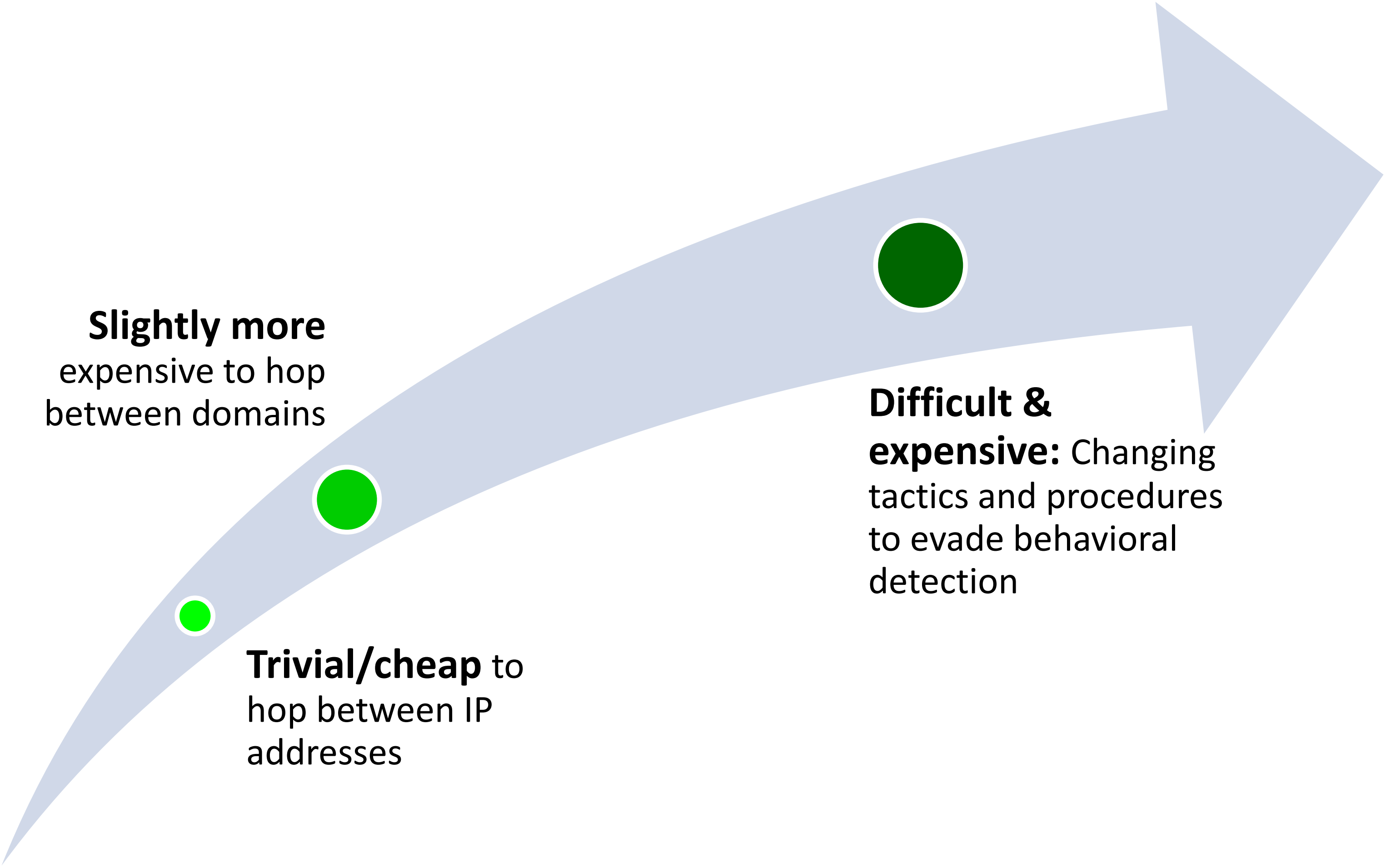
Why Share Indicators?

- 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

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

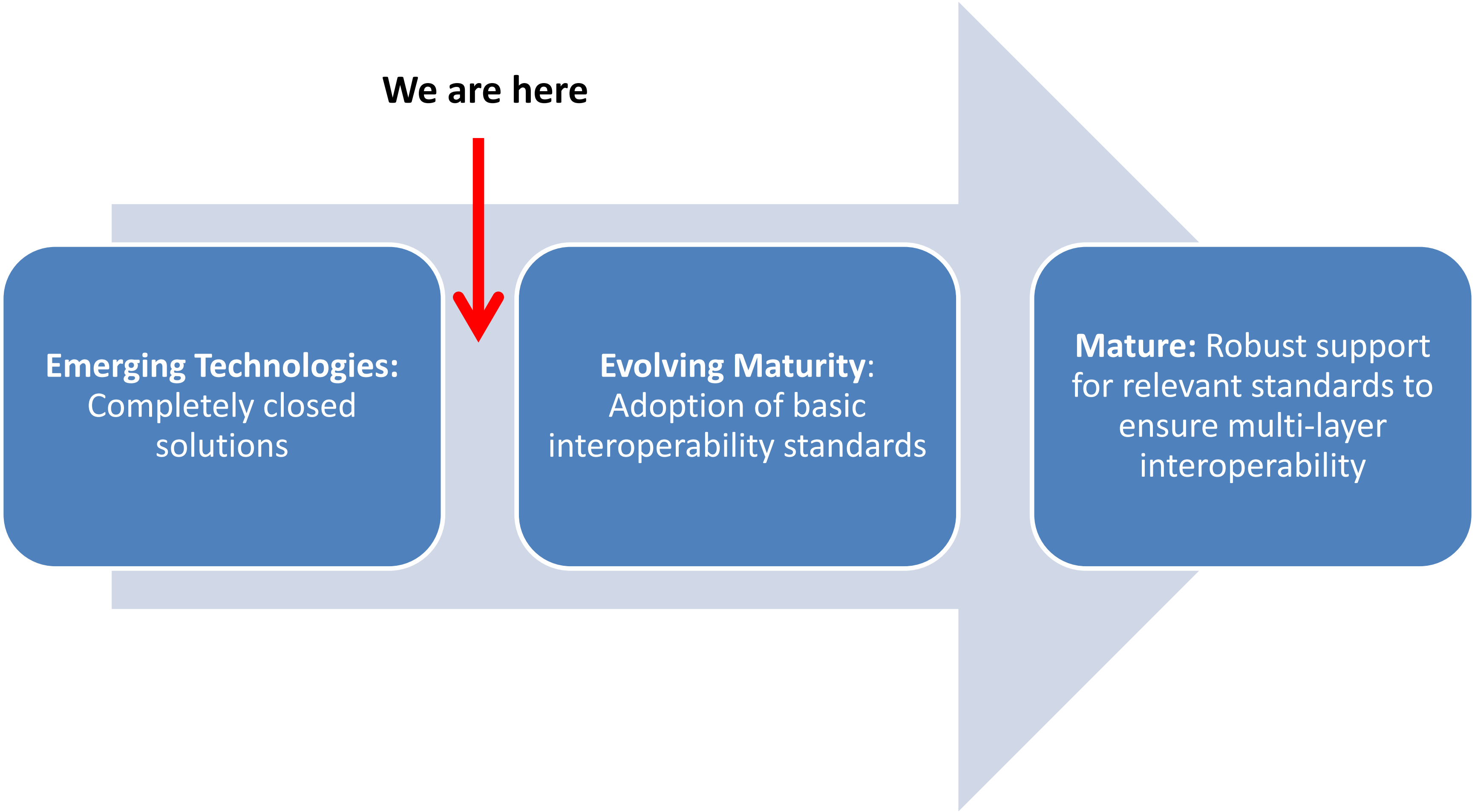


Trivial/cheap to hop between IP addresses

Slightly more expensive to hop between domains

Difficult & expensive: Changing tactics and procedures to evade behavioral detection

Market Evolution: Threat/indicator Sharing



We are here

Emerging Technologies: Completely closed solutions

Evolving Maturity: Adoption of basic interoperability standards

Mature: Robust support for relevant standards to ensure multi-layer interoperability

Landscape

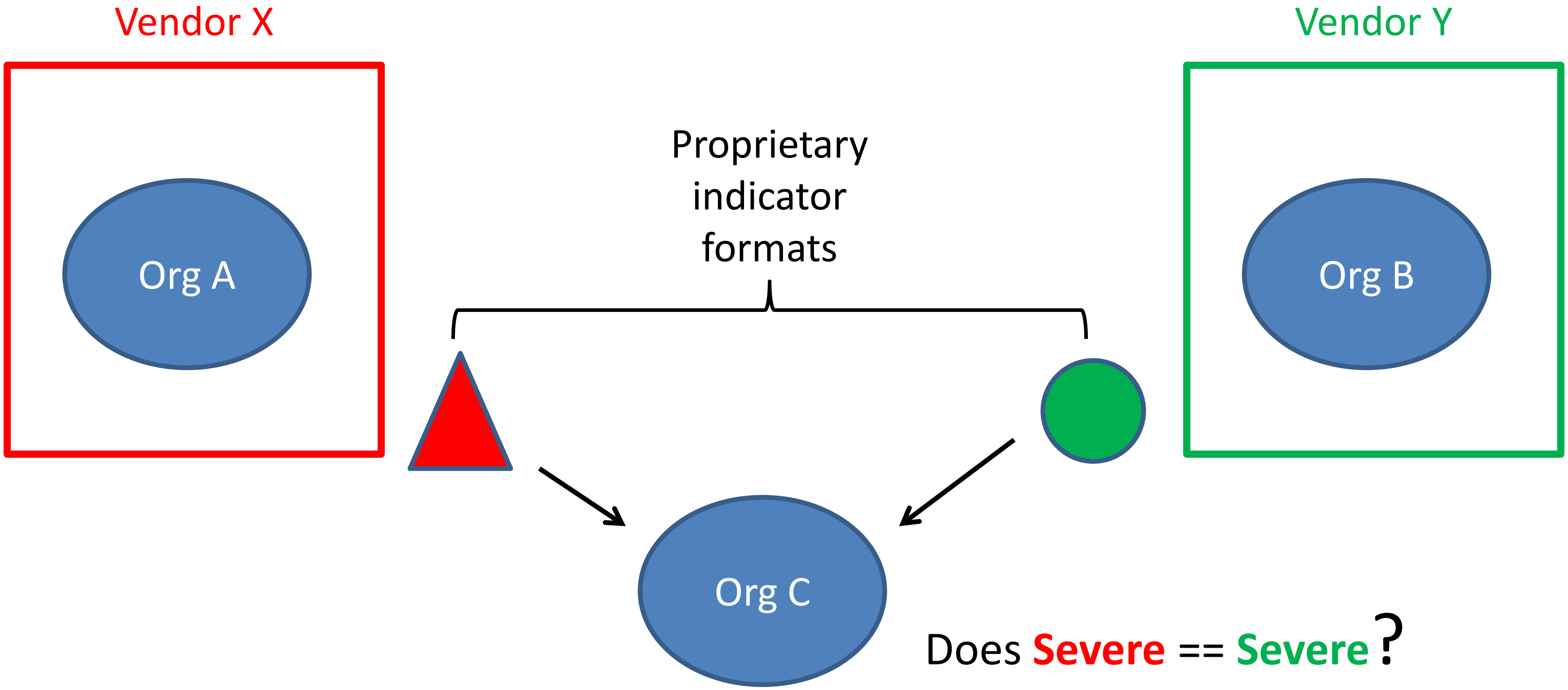
Today:

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



Vendor X

Org A

Proprietary indicator formats

Vendor Y

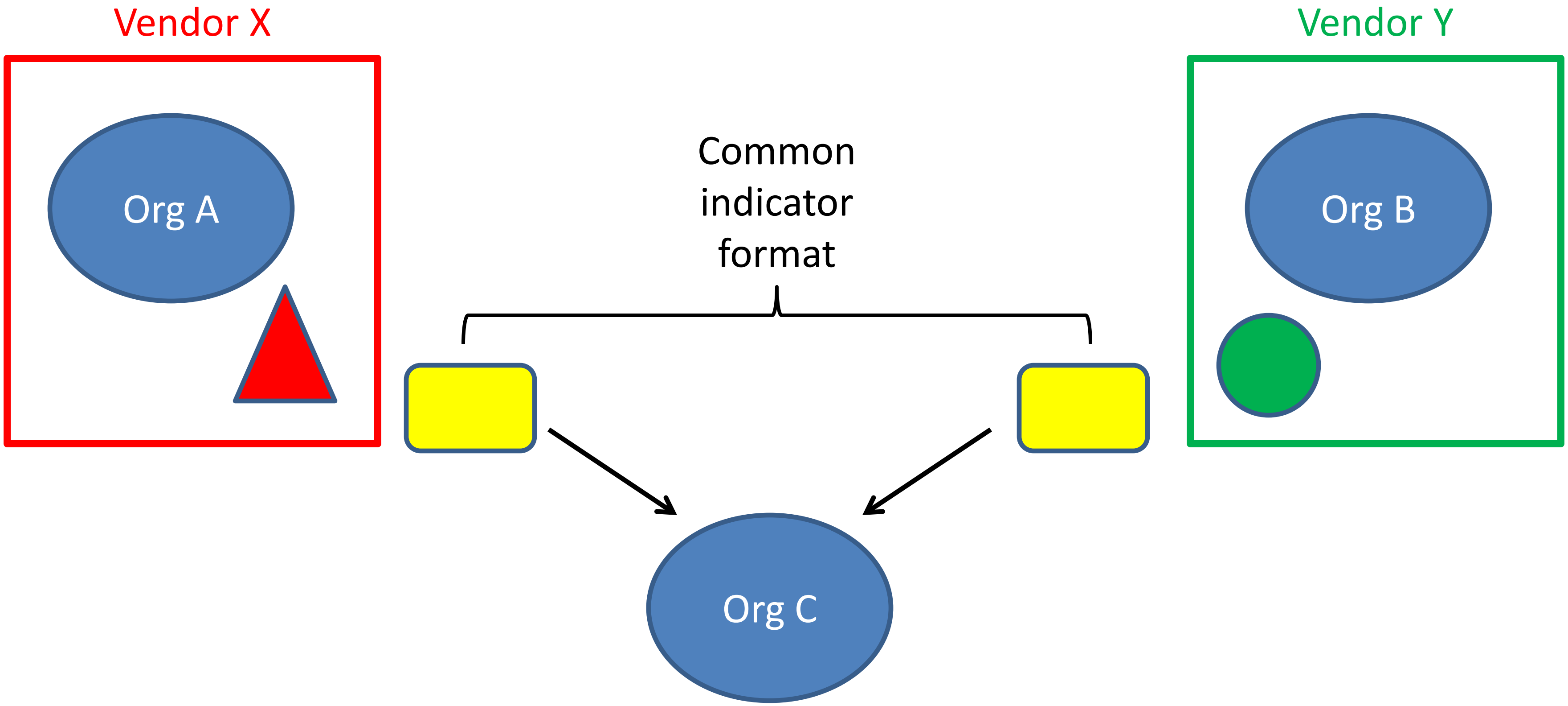
Org B

Org C

Does **Severe** == **Severe**?

- 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

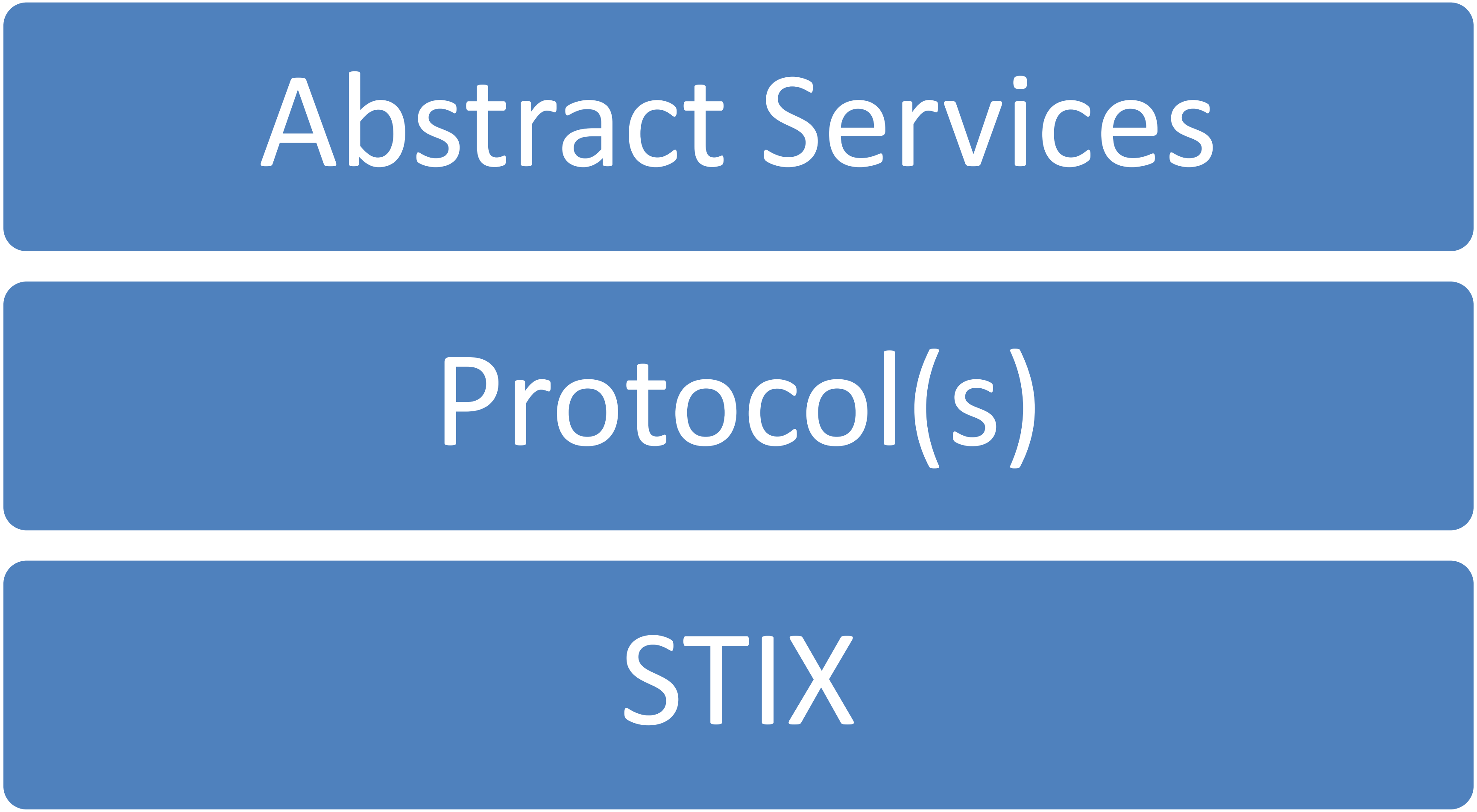
- Data representations for indicators and observables
- Protocol(s) for exchanging indicators securely

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

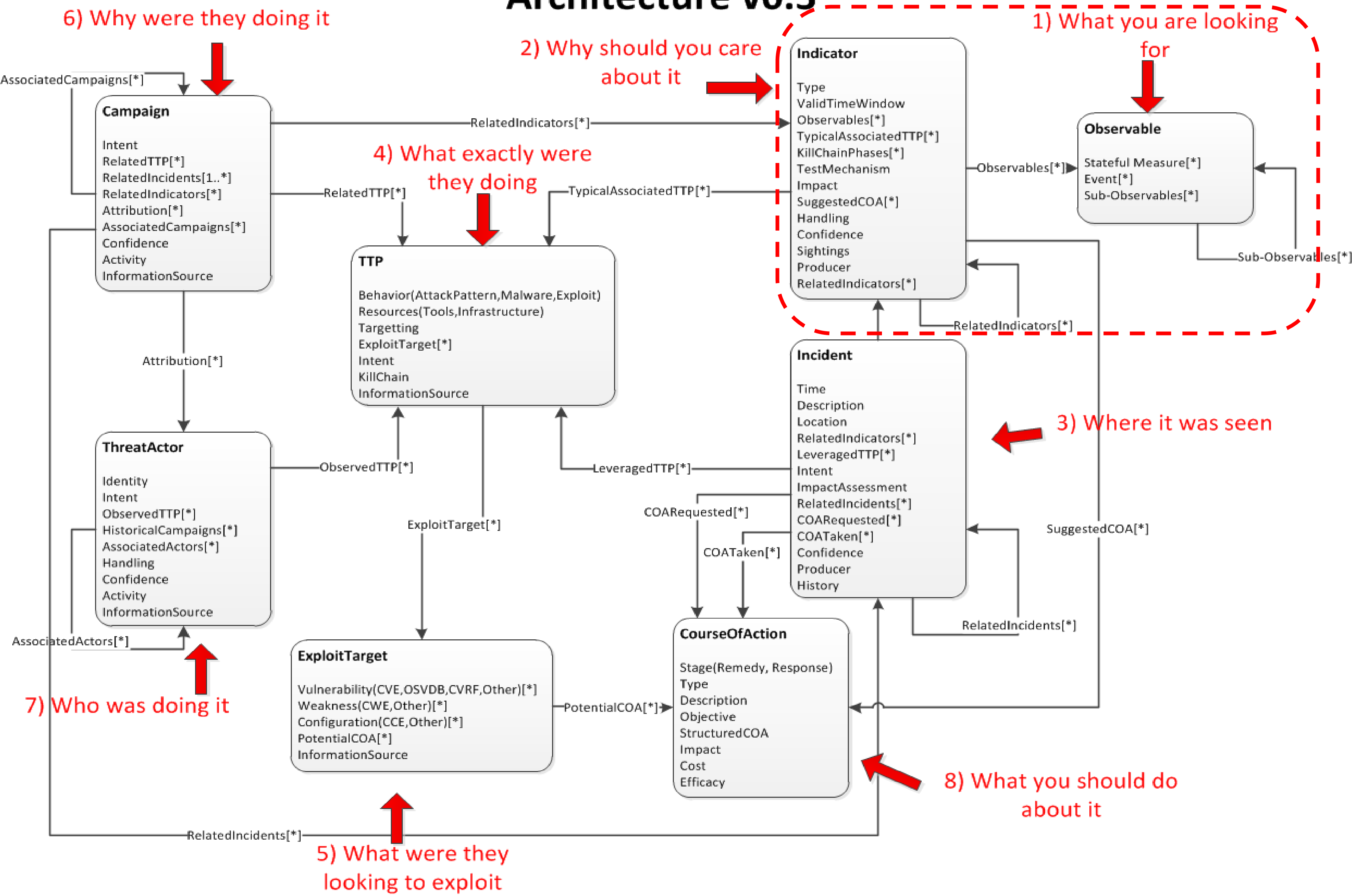


Abstract Services

Protocol(s)

STIX

Structured Threat Information eXpression (STIX) Architecture v0.3



1) What you are looking for

2) Why should you care about it

3) Where it was seen

4) What exactly were they doing

5) What were they looking to exploit

6) Why were they doing it

7) Who was doing it

8) What you should do about it

Indicator

Type
ValidTimeWindow
Observables[*]
TypicalAssociatedTTP[*]
KillChainPhases[*]
TestMechanism
Impact
SuggestedCOA[*]
Handling
Confidence
Sightings
Producer
RelatedIndicators[*]

Observable

Stateful Measure[*]
Event[*]
Sub-Observables[*]

Campaign

Intent
RelatedTTP[*]
RelatedIncidents[1..*]
RelatedIndicators[*]
Attribution[*]
AssociatedCampaigns[*]
Confidence
Activity
InformationSource

TTP

Behavior(AttackPattern,Malware,Exploit)
Resources(Tools,Infrastructure)
Targetting
ExploitTarget[*]
Intent
KillChain
InformationSource

Incident

Time
Description
Location
RelatedIndicators[*]
LeveragedTTP[*]
Intent
ImpactAssessment
RelatedIncidents[*]
COARequested[*]
COATaken[*]
Confidence
Producer
History

ThreatActor

Identity
Intent
ObservedTTP[*]
HistoricalCampaigns[*]
AssociatedActors[*]
Handling
Confidence
Activity
InformationSource

ExploitTarget

Vulnerability(CVE,OSVDB,CVRF,Other)[*]
Weakness(CWE,Other)[*]
Configuration(CCE,Other)[*]
PotentialCOA[*]
InformationSource

CourseOfAction

Stage(Remedy, Response)
Type
Description
Objective
StructuredCOA
Impact
Cost
Efficacy

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

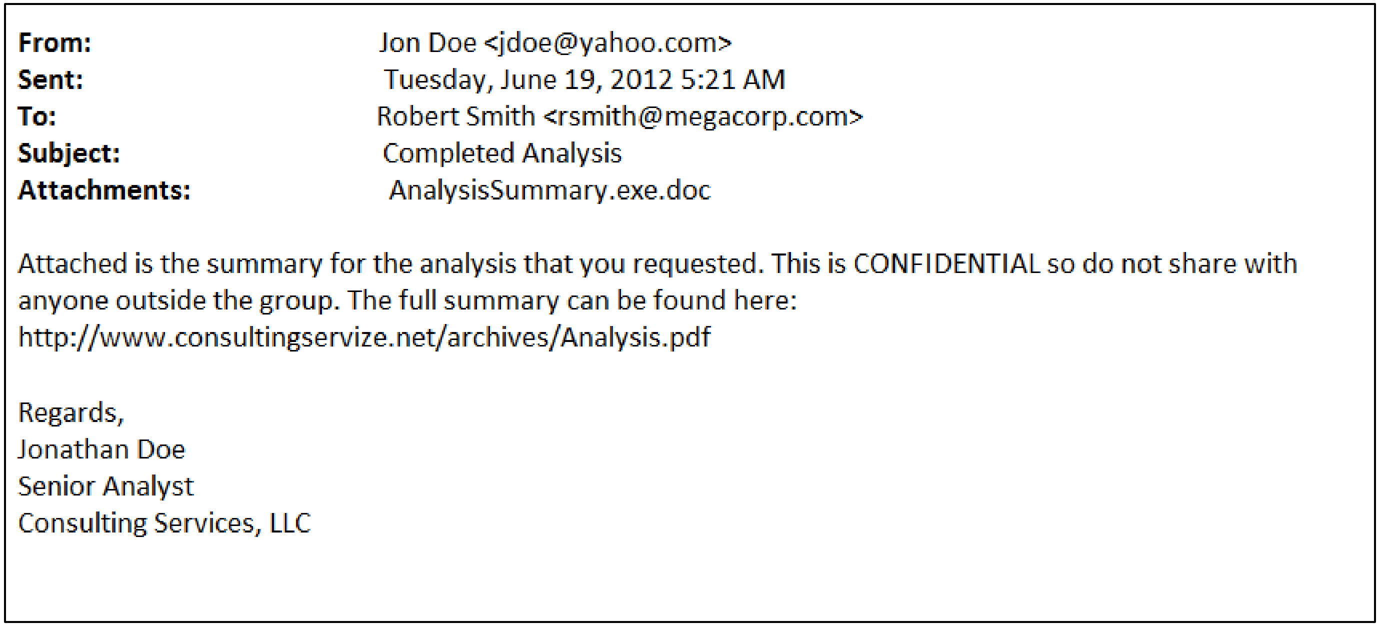
(more on the way)

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

```xml
</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.secureserver.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>
```

STIX-Indicator Context Layer

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

Services and Protocols

- Intent is to define a basic set of abstract Services
- Define bindings to specific implementations:
  - – e.g. RESTful interface

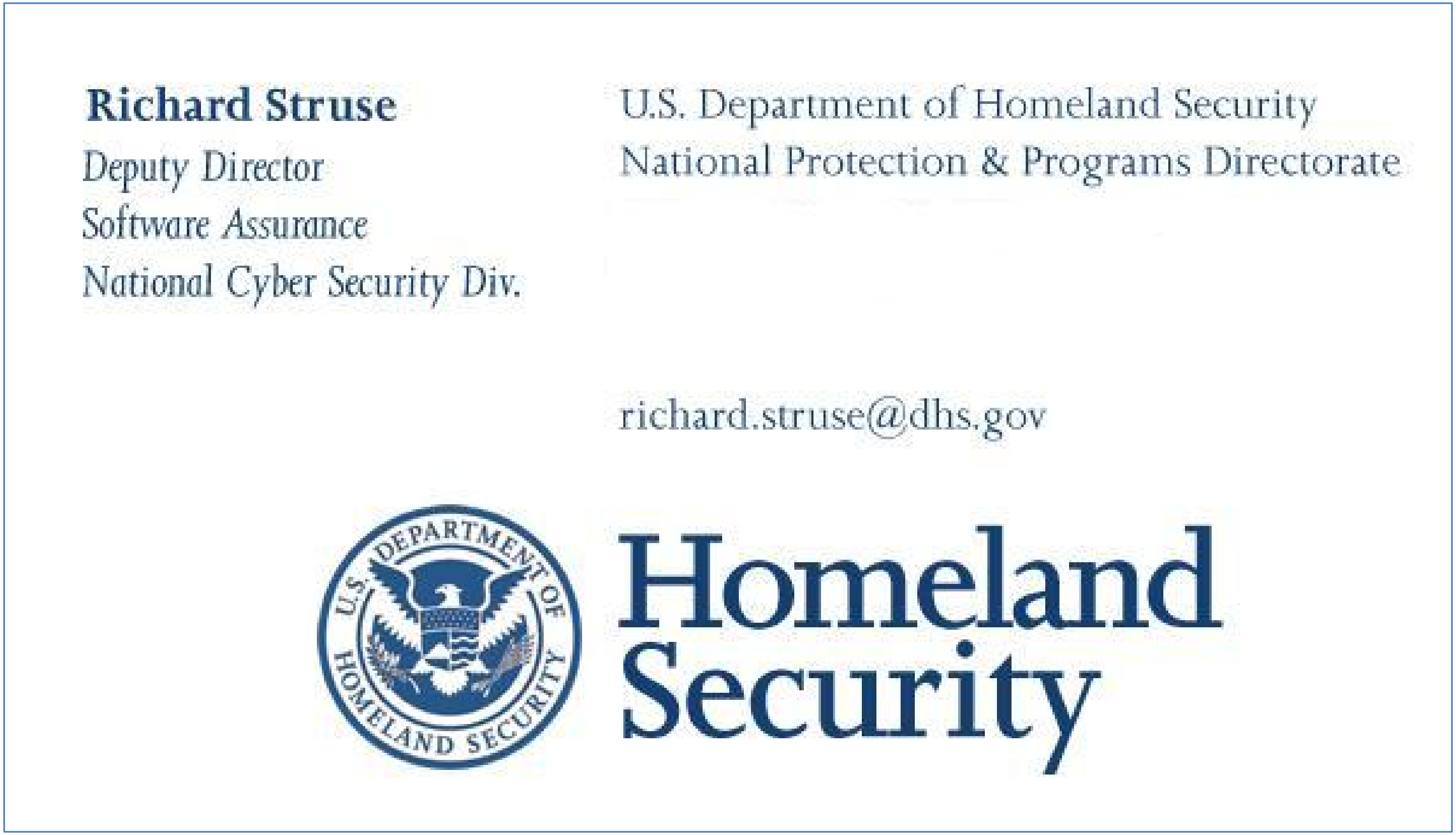
TAXII: Value Proposition

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.