STIX & TAXII

Analyzing and Sharing Cyber Threat Intelligence

What are STIX and TAXII?

A language for modeling and representing cyber threat intelligence.

A protocol for exchanging cyber threat intelligence.

STIX and TAXII are International Standards

- **STIX and TAXII were developed by DHS and MITRE in conjunction with major collaboration partners from:**
  - US Government
  - Financial Sector
  - Critical Infrastructure Sector
  - International industry and government

- **As of 2015, both have transitioned to OASIS in the newly formed Cyber Threat Intelligence Technical Committee**

OASIS
Advancing open standards for the information society

Homeland Security

Structured Threat Information Expression

A language for modeling and representing cyber threat intelligence.

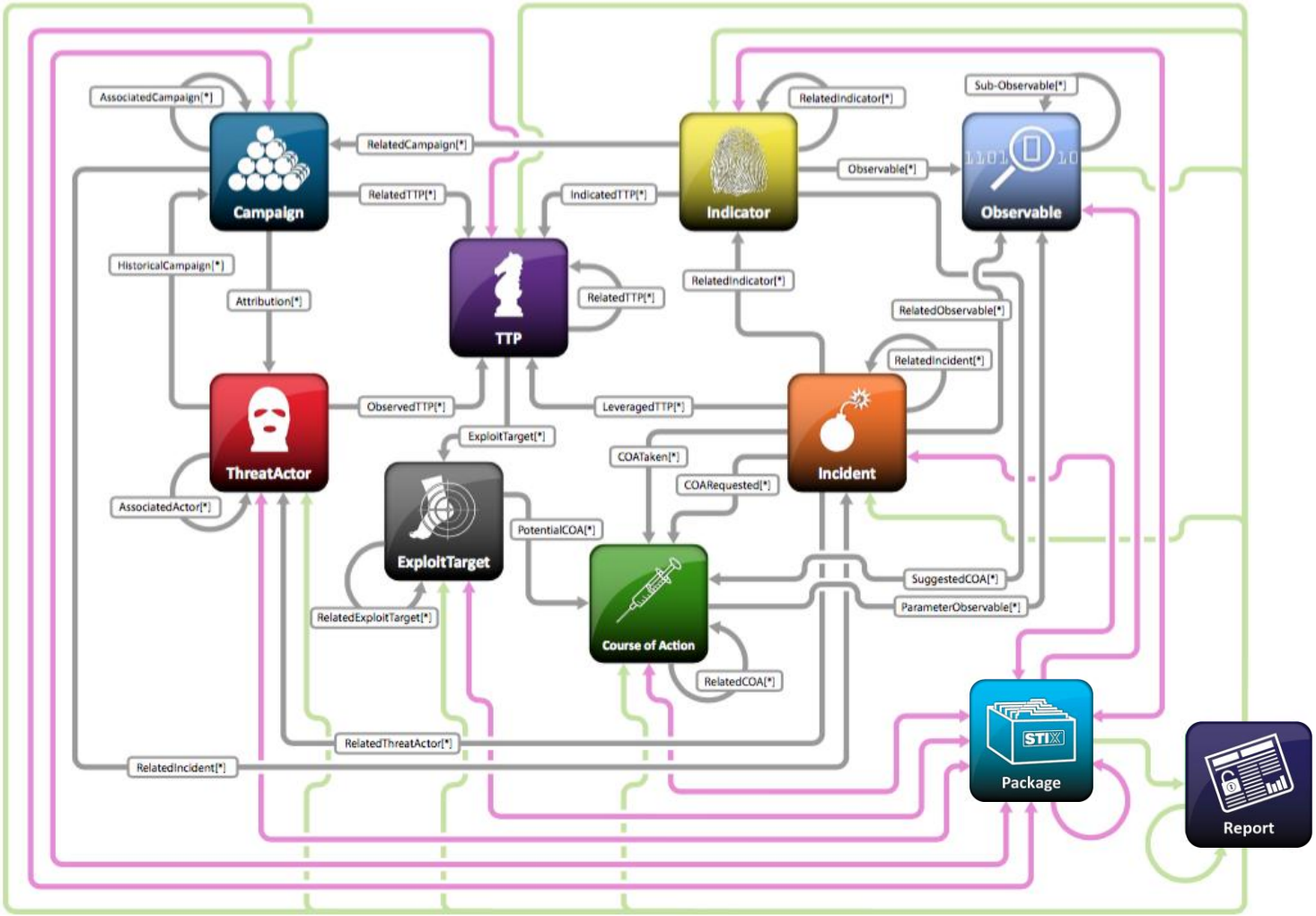
- Structured language for automation
- Designed for sharing and analysis
- Active community of developers and analysts
- International standard in OASIS

Homeland Security

Current Status

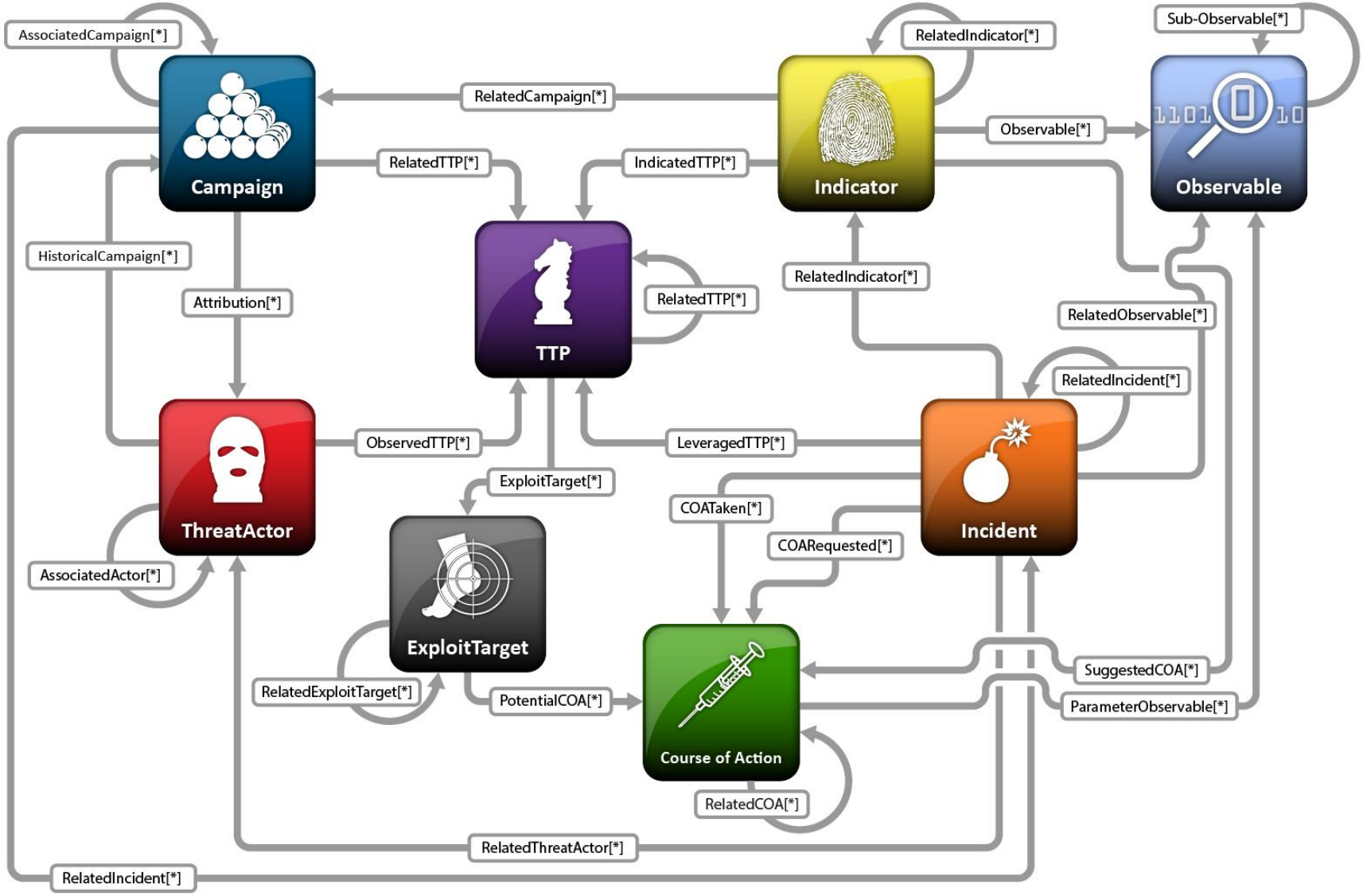
- **STIX 1.2 is the latest published version**
  - Published by DHS/MITRE
  - XML Schemas
- **STIX 1.2.1 will be published by OASIS**
  - Nearly identical to STIX 1.2
  - Will include text specifications, UML, and XML schemas
- **STIX 2.0 is currently in development**
  - JSON-based
  - Published by OASIS
  - Will include more comprehensive text specifications and UML

STIX 1.2 Architecture



Homeland Security

STIX 1.2 Architecture - ZOOM



Observable

Instances of **events and objects** that **have been seen** in cyberspace
(and)
Patterns for **events and objects** that **might be seen** in cyberspace

Observable

- 90+ Object Types
  - Files (names, hashes, …)
  - Addresses (IP, e-mail, domains, …)
  - E-mails (subject, sender, attachments, ...)
  - Registry Keys
- Patterning support
  - Wildcards
  - Compositional logic
- Events (e.g. File A downloads File B)

Examples

IP	192.168.1.4
Hash	d99a74fbe169e3eba0…
Traffic	192.168.1.4 -> 10.10.1.1

Filename Pattern	File/File_Name [Contains] bad.exe
Email Regex	Email/Subject [Matches] BAD.+STUFF

XML

IP Address:

```
<cybox:Observable id="example:observable-c8c32b6e-2ea8-51c4-6446-7f5218072f27">
    <cybox:Object id="example:object-d7fcce87-0e98-4537-81bf-1e7ca9ad3734">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
            <AddressObject:Address_Value>198.51.100.2</AddressObject:Address_Value>
        </cybox:Properties>
    </cybox:Object>
</cybox:Observable>
```

Email Subject Pattern:

```
<indicator:Observable id="example:Observable-e9926796-6b52-463c-8be1-0ab66e9adb1c">
    <cybox:Object id="example:EmailMessage-38afa5c9-ef26-4948-928b-0230521c67b7">
        <cybox:Properties xsi:type="EmailMessageObj:EmailMessageObjectType">
            <EmailMessageObj:Header>
                <EmailMessageObj:Subject
                  condition="StartsWith">[IMPORTANT] Please Review Before</EmailMessageObj:Subject>
            </EmailMessageObj:Header>
        </cybox:Properties>
    </cybox:Object>
</indicator:Observable>
```

Indicator

Pattern* for **something you might see**
and
what it means if you see it

- *Patterns* are represented using CybOX
- *What it means* is represented via a TTP or Campaign
- Also includes context, such as potential courses of action, timeframes, and likely impact

Homeland Security

Examples

C2	1.2.3.x = C2 for Actor Z
Malware	h99a74… = PIVY v423
Phishing	E-mail from x@x = phishing

XML

```
<stix:Indicators>
    <stix:Indicator id="example:indicator-a932fcc6-e032-176c-126f-cb970a5a1ade" xsi:type='indicator:IndicatorType'
    timestamp="2014-05-08T09:00:00.000000Z">
        <indicator:Title>File hash for Poison Ivy variant</indicator:Title>
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash Watchlist</indicator:Type>
        <indicator:Observable id="example:Observable-7d6f87bb-b4cd-42dd-b655-72557e9ea79f">
            <cybox:Object id="example:File-91040dc2-28d8-4925-bfe8-6b50d300afe1">
                <cybox:Properties xsi:type="FileObj:FileObjectType">
                    <FileObj:Hashes>
                        <cyboxCommon:Hash>
                            <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                            <cyboxCommon:Simple_Hash_Value condition="Equals">ef537f25...</cyboxCommon:Simple_Hash_Value>
                        </cyboxCommon:Hash>
                    </FileObj:Hashes>
                </cybox:Properties>
            </cybox:Object>
        </indicator:Observable>
        <indicator:Indicated_TTP>
            <stixCommon:TTP idref="example:ttp-e610a4f1-9676-eab3-bcc6-b2768d58281a" />
        </indicator:Indicated_TTP>
    </stix:Indicator>
</stix:Indicators>
```

Incident

Information about a cybersecurity **investigation** or **incident.**

- Victim identity
- Impacted assets and business functions
- Attribution to a threat actor or campaign
- Leveraged TTPs (malware, attack patterns, etc)
- Indicators that detected it
- Exploit targets that were used to gain entry
- Times and actions

Examples

Basic	System XYZ has PIVY
APT	Systems 3,4,7 owned by ACME, Inc. have malware. APT31 is suspected.

XML

```
<stix:Incident id="example:incident-8236b4a2-abe0-4b56-9347-288005c4bb92" timestamp="2014-11-18T23:40:08.061362+00:00"
xsi:type='incident:IncidentType' version="1.2">
    <incident:Title>Breach of Cyber Tech Dynamics</incident:Title>
    <incident:Time>
        <incident:Initial_Compromise precision="second">2012-01-30T00:00:00</incident:Initial_Compromise>
        <incident:Incident_Discovery precision="second">2012-05-10T00:00:00</incident:Incident_Discovery>
        <incident:Restoration_Achieved precision="second">2012-08-10T00:00:00</incident:Restoration_Achieved>
        <incident:Incident_Reported precision="second">2012-12-10T00:00:00</incident:Incident_Reported>
    </incident:Time>
    <incident:Description>Intrusion into enterprise network</incident:Description>
    <incident:Reporter>
        <stixCommon:Description>The person who reported it</stixCommon:Description>
        <stixCommon:Identity id="example:Identity-cd64aaa6-b1c0-4026-8ea1-14ff5a19e5fb">
            <stixCommon:Name>Sample Investigations, LLC</stixCommon:Name>
        </stixCommon:Identity>
        <stixCommon:Time>
            <cyboxCommon:Produced_Time>2014-03-11T00:00:00</cyboxCommon:Produced_Time>
        </stixCommon:Time>
    </incident:Reporter>
    <incident:Victim id="example:Identity-dd8637b7-51b4-48f0-9e3c-a2b23b3a2dd7">
        <stixCommon:Name>Cyber Tech Dynamics</stixCommon:Name>
    </incident:Victim>
    <incident:Impact_Assessment>
        <incident:Effects>
            <incident:Effect xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial Loss</incident:Effect>
        </incident:Effects>
    </incident:Impact_Assessment>
    <incident:Confidence timestamp="2014-11-18T23:40:08.061379+00:00">
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
    </incident:Confidence>
</stix:Incident>
```

Homeland Security

Tactics, Techniques, and Procedures (TTP)

HSSEDI™

Adversary behavior and resources, including **malware**, **attack patterns**, **exploits**, **infrastructure**, **tools**, **personas**, & **targeting.**

- Includes information about intended effect
- Malware is extensible via MAEC
- Though all used through the TTP construct, should only be used individually
  - i.e. do not combine one TTP with both a malware instance and an attack pattern

Homeland Security

TTP

Examples

Malware	PIVY Variant
Attack	SQL Injection
Targeting	Retail Sector
Infrastructure	C2 Server = 1.23.4.5

XML: Malware

```
<stix:TTP xsi:type="ttp:TTPType" id="example:ttp-7d9fe1f7-429d-077e-db51-92c70b8da45a">
  <ttp:Title>Poison Ivy Variant v4392-acc</ttp:Title>
  <ttp:Behavior>
    <ttp:Malware>
      <ttp:Malware_Instance xsi:type="stix-maec:MAEC4.1InstanceType">
        <ttp:Type xsi:type="stixVocabs:MalwareTypeVocab-1.0">Remote Access Trojan</ttp:Type>
        <ttp:Name>Poison Ivy Variant v4392-acc</ttp:Name>
        <stix-maec:MAEC id="example:package-2fb96bef-1b11-436e-af4a-15588ac3198b" schema_version="2.1">
          <!-- MAEC Content Here -->
          <maecPackage:Malware_Subjects>
            <maecPackage:Malware_Subject id="example:Subject-57cd4839-436e-1b11-af4a-15588ac3198b">
              <maecPackage:Malware_Instance_Object_Attributes>
              </maecPackage:Malware_Instance_Object_Attributes>
            </maecPackage:Malware_Subject>
          </maecPackage:Malware_Subjects>
        </stix-maec:MAEC>
      </ttp:Malware_Instance>
    </ttp:Malware>
  </ttp:Behavior>
</stix:TTP>
```

TTP

XML: Targeting

```
<stix:TTPs>
    <stix:TTP xsi:type="ttp:TTPType" id="example:ttp-4fde045a-b25f-f035-e8d0-29c9d5130cd9"
      timestamp="2014-05-08T09:00:00.000000Z">
        <ttp:Title>Victim Targeting: Customer PII and Financial Data</ttp:Title>
        <ttp:Victim_Targeting xsi:type="ttp:VictimTargetingType">
            <ttp:Targeted_Information xsi:type="stixVocabs:InformationTypeVocab-1.0">Information Assets - Customer
            PII</ttp:Targeted_Information>
            <ttp:Targeted_Information xsi:type="stixVocabs:InformationTypeVocab-1.0">Information Assets - Financial
            Data</ttp:Targeted_Information>
        </ttp:Victim_Targeting>
    </stix:TTP>
</stix:TTPs>
```

Homeland Security

Exploit Target

Vulnerabilities, **weaknesses**, and **misconfigurations** in infrastructure that make it vulnerable to attack

- Includes references to CVE, CCE, and CWE
  - Extension for CVRF
- Like TTP, only use it for one at a time

Examples

Vulnerability Heartbleed (CVE-2014-0160)

Weakness Improper String Handling (CWE-89)

ExploitTarget

XML

```
<stix:Exploit_Targets>
    <stixCommon:Exploit_Target xsi:type="et:ExploitTargetType"
      id="example:et-48a276f7-a8d7-bba2-3575-e8a63fcd488"
      timestamp="2014-05-08T09:00:00.000000Z">
        <et:Title>Javascript vulnerability in MSIE 6-11</et:Title>
        <et:Vulnerability>
            <et:CVE_ID>CVE-2013-3893</et:CVE_ID>
        </et:Vulnerability>
    </stixCommon:Exploit_Target>
</stix:Exploit_Targets>
```

Homeland Security

Campaign

HSSEDI™

Pattern of ongoing activity with a **common purpose or goal**

- Pattern of ongoing activity is primarily via relationships
  - Incidents
  - Indicators
  - TTPs
- Includes intended effect
- Distinct from threat actor

Homeland Security

Examples

APT	Campaign against U.S. industry
Crime	Campaign against systems at big box retailers

Campaign

XML

```
<stix:Indicators>
    <stix:Indicator id="example:indicator-c43a0a05-e8d2-4f64-ae37-3f3fb153f8d9" timestamp="2014-09-09T19:58:39.608000+00:00"
    xsi:type='indicator:IndicatorType' negate="false" version="2.1.1">
        <indicator:Title>IP Address for known C2 Channel</indicator:Title>
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
        <indicator:Observable id="example:Observable-f1712715-9bcd-404a-bf47-76504cf1232c">
            <cybox:Object id="example:Address-c4d21d91-2bea-4b19-ac53-c513f1b1bc51">
                <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
                    <AddressObj:Address_Value condition="Equals">10.0.0.0</AddressObj:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </indicator:Observable>
        <indicator:Related_Campaigns>
            <indicator:Related_Campaign>
                <stixCommon:Campaign idref="example:Campaign-b549a58c-afd9-4847-85c3-5be13d56d3cc"
                timestamp="2014-09-09T19:58:39.609000+00:00" />
            </indicator:Related_Campaign>
        </indicator:Related_Campaigns>
    </stix:Indicator>
</stix:Indicators>
<stix:Campaigns>
    <stix:Campaign id="example:Campaign-b549a58c-afd9-4847-85c3-5be13d56d3cc" timestamp="2014-09-09T19:58:39.609000+00:00"
    xsi:type='campaign:CampaignType' version="1.2">
        <campaign:Title>Operation Omega</campaign:Title>
    </stix:Campaign>
</stix:Campaigns>
```

Homeland Security

Threat Actor

HSSEDI™

Information about threat actor **groups** and **individuals**

- Includes:
  - Extensive identity information via OASIS CIQ
  - Assessments of maturity, intent, and resources
- Distinct from campaign

Homeland Security

Examples

Individual	KDZ-23, Amateur/Crime
Group	APT1, APT
ID Info	Nationality: American

ThreatActor

XML

```
<stix:Threat_Actor id="example:threatactor-dfaa8d77-07e2-4e28-b2c8-92e9f7b04428" timestamp="2014-11-19T23:39:03.893348+00:00"
  xsi:type='ta:ThreatActorType' version="1.2">
    <ta:Title>Disco Team Threat Actor Group</ta:Title>
    <ta:Identity id="example:Identity-733c5838-34d9-4fbf-949c-62aba761184c" xsi:type='stix-ciqidentity:CIQIdentity3.0InstanceType'>
        <ExtSch:Specification xmlns:ExtSch="http://stix.mitre.org/extensions/Identity#CIQIdentity3.0-1">
          <xpil:PartyName xmlns:xpil="urn:oasis:names:tc:ciq:xpil:3">
            <xnl:OrganisationName xmlns:xnl="urn:oasis:names:tc:ciq:xnl:3" xnl:Type="CommonUse">
              <xnl:NameElement>Disco Team</xnl:NameElement>
            </xnl:OrganisationName>
            <xnl:OrganisationName xmlns:xnl="urn:oasis:names:tc:ciq:xnl:3" xnl:Type="UnofficialName">
              <xnl:NameElement>Equipo del Discoteca</xnl:NameElement>
            </xnl:OrganisationName>
          </xpil:PartyName>
          <xpil:Addresses xmlns:xpil="urn:oasis:names:tc:ciq:xpil:3">
            <xpil:Address>
              <xal:Country xmlns:xal="urn:oasis:names:tc:ciq:xal:3">
                <xal:NameElement>United States</xal:NameElement>
              </xal:Country>
              <xal:AdministrativeArea xmlns:xal="urn:oasis:names:tc:ciq:xal:3">
                <xal:NameElement>California</xal:NameElement>
              </xal:AdministrativeArea>
            </xpil:Address>
          </xpil:Addresses>
          <xpil:ElectronicAddressIdentifiers xmlns:xpil="urn:oasis:names:tc:ciq:xpil:3">
            <xpil:ElectronicAddressIdentifier>disco-team@stealthemail.com</xpil:ElectronicAddressIdentifier>
            <xpil:ElectronicAddressIdentifier>facebook.com/thediscoteam</xpil:ElectronicAddressIdentifier>
          </xpil:ElectronicAddressIdentifiers>
          <xpil:Languages xmlns:xpil="urn:oasis:names:tc:ciq:xpil:3">
            <xpil:Language>Spanish</xpil:Language>
          </xpil:Languages>
        </ExtSch:Specification>
    </ta:Identity>
</stix:Threat_Actor>
```

Homeland Security

Course of Action

Preventative or reactive **responses to threat activity**

- Includes:
  - Assessments of cost, efficacy, etc.
  - Structured COA to represent machine-readable courses of action
- Often used from incident or indicator
  - Incident to represent

Examples

Preventative	Install patch MSKB-234
Reactive	Clean the box and rebuild

XML

```
<stix:Course_Of_Action id="example:coa-495c9b28-b5d8-11e3-b7bb-000c29789db9" xsi:type='coa:CourseOfActionType' version="1.2">
    <coa:Title>Block traffic to PIVY C2 Server (10.10.10.10)</coa:Title>
    <coa:Stage xsi:type="stixVocabs:COAStageVocab-1.0">Response</coa:Stage>
    <coa:Type xsi:type="stixVocabs:CourseOfActionTypeVocab-1.0">Perimeter Blocking</coa:Type>
    <coa:Objective>
        <coa:Description>Block communication between the PIVY agents and the C2 Server</coa:Description>
        <coa:Applicability_Confidence>
            <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
        </coa:Applicability_Confidence>
    </coa:Objective>
    <coa:Parameter_Observables cybox_major_version="2" cybox_minor_version="1" cybox_update_version="0">
        <cybox:Observable id="example:Observable-356e3258-0979-48f6-9bcf-6823eecf9a7d">
            <cybox:Object id="example:Address-df3c710c-f05c-4edb-a753-de4862048950">
                <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
                    <AddressObj:Address_Value>10.10.10.10</AddressObj:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </coa:Parameter_Observables>
    <coa:Impact>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">Low</stixCommon:Value>
        <stixCommon:Description>This IP address is not used for legitimate hosting so there should be no operational impact.</stixCommon:Description>
    </coa:Impact>
    <coa:Cost>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">Low</stixCommon:Value>
    </coa:Cost>
    <coa:Efficacy>
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
    </coa:Efficacy>
</stix:Course_Of_Action>
```

Report

A collection of content **related to a single subject**

- Includes:
  - References to the content included in the report
  - Title, description, author, and other metadata
- Used to represent ”analysis reports” and other types of threat reports

Examples

Major Report	Mandiant's APT1 Report
Standard Report	IB-4232

XML

```
<stix:Report timestamp="2015-05-07T14:22:14.760467+00:00"
    id="example:Report-ab11f431-4b3b-457c-835f-59920625fe65" xsi:type='report:ReportType' version="1.0">
    <report:Header>
        <report:Title>Report on Adversary Alpha's Campaign against the Industrial Control Sector</report:Title>
        <report:Intent xsi:type="stixVocabs:ReportIntentVocab-1.0">Campaign Characterization</report:Intent>
        <report:Description>Adversary Alpha has a campaign against the ICS sector!</report:Description>
    </report:Header>
    <report:Campaigns>
        <report:Campaign idref="example:campaign-1855cb8a-d96c-4859-a450-abb1e7c061f2"
          xsi:type='campaign:CampaignType'/>
    </report:Campaigns>
</stix:Report>
```

Homeland Security

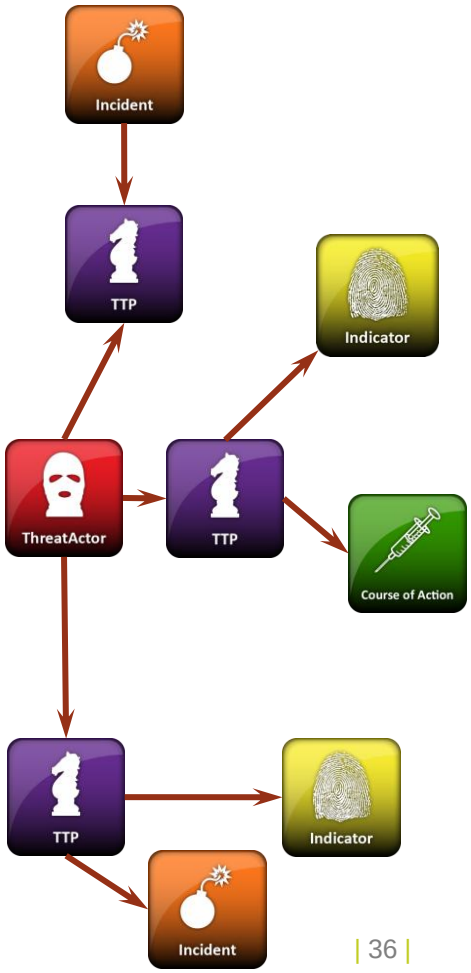
Example: Retailer Malware

You're a threat analyst at a major retailer, STB, Inc.

One of your front line employees complains about weird errors. Upon **investigating**, IT finds **BP.trojan** on their system.

Your CTI system pulls up a report from US-CERT attributing that variant to **Ugly Duckling.** They also indicate that **BlackPOS** is often used by that actor and give a **file hash** and **response options**.

Your investigation with that data uncovers several more infestations. Additionally, you discover a new variant of **BlackPOS** with a different **hash**.



Homeland Security

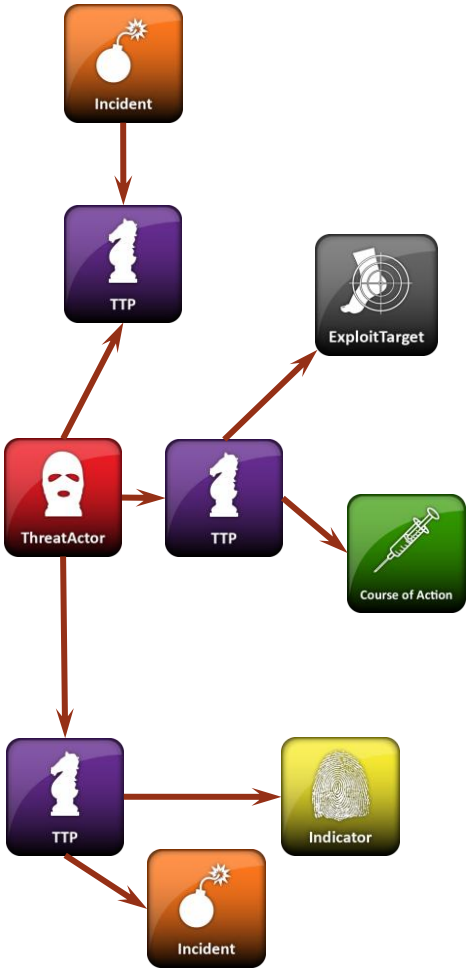
Information Sharing

What do you share?

STIX lets you choose what to share

…and what not to share

…and lets you relate it all together



Homeland Security

Trusted, Automated Exchange of Indicator Information

HSSEDI™

- Automated machine-to-machine sharing over HTTP
- Supports a wide variety of sharing models
- Active community of developers and analysts
- Becoming international standard in OASIS

A protocol for exchanging cyber threat intelligence.

Homeland Security

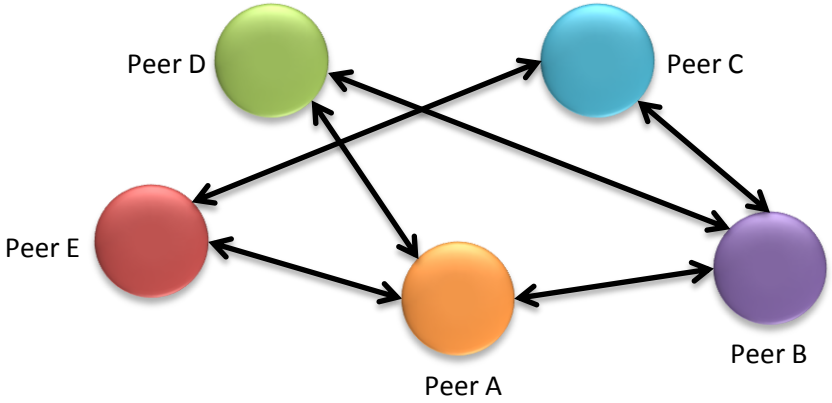
What is TAXII?

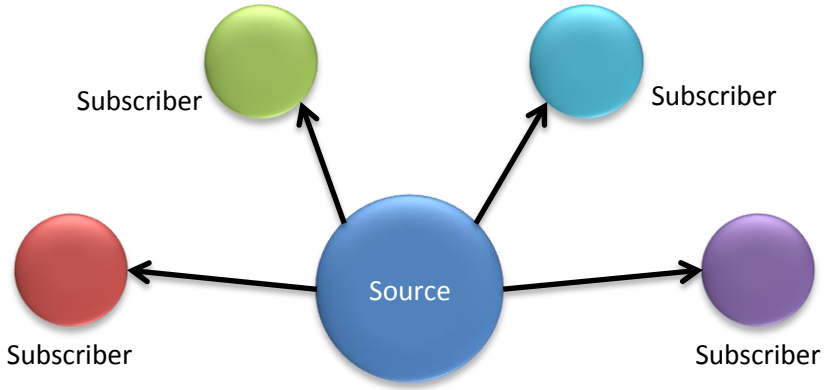
- **Standardizes exchange of cyber threat information**
- **A set of specifications any software can implement**

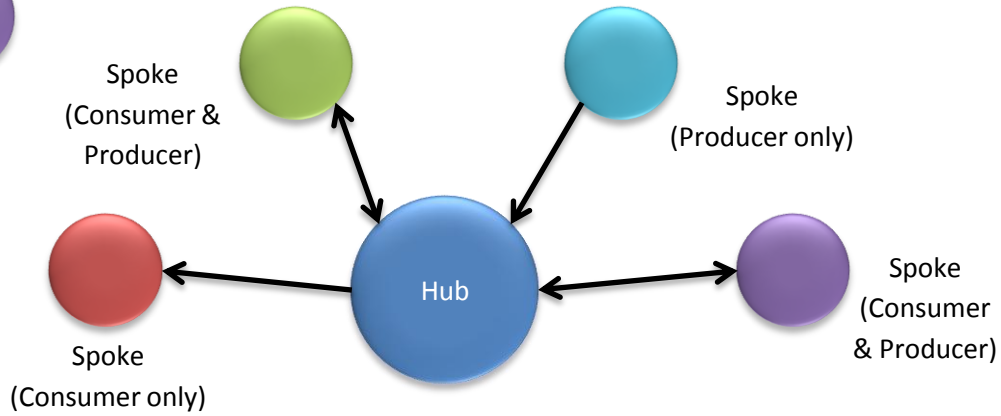
- **TAXII is NOT**
  - A specific sharing program
    - but sharing programs can use it
  - Software
    - but software can use it to share information
  - Mandate particular trust agreements or sharing
    - instead, use it to share what *you* want with the parties *you* choose

Flexible Sharing Models

- **Most sharing models are variants of these three basic models**
  - TAXII can support participation in any of these models or multiple models simultaneously







Homeland Security

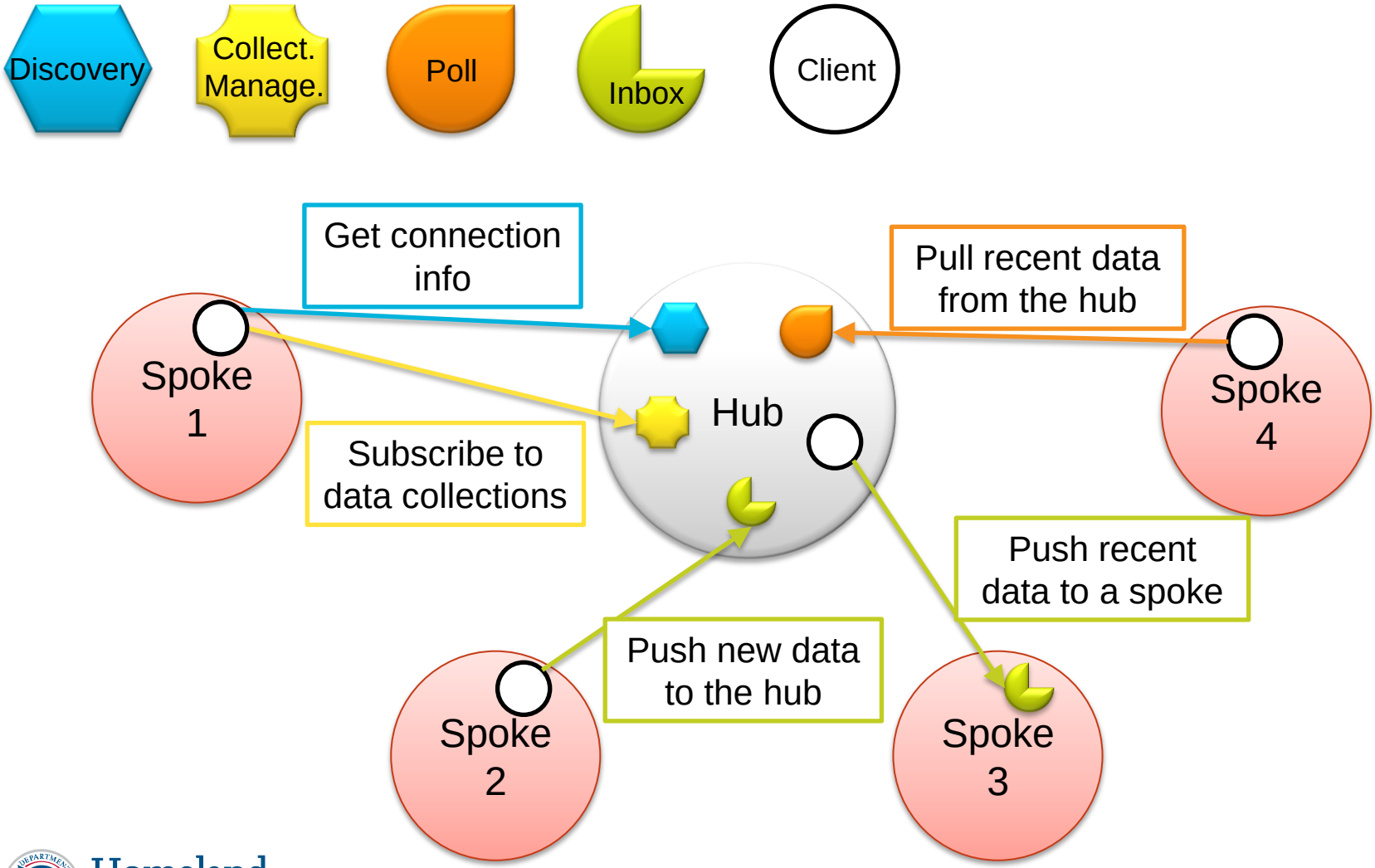
TAXII Features

- **Minimal requirements imposed on data consumers**
  - Does not require data consumers to field internet services or establish a particular security capability
- **Minimal data management requirements on data producers**
  - Does not require use of particular data management technologies or constrain how producers manage access to their data
- **Flexible sharing model support**
  - Does not force a particular sharing model on users
- **Appropriately secure communication**
  - Supports multiple security mechanisms without forcing adoption of unnecessary measures
- **Push and Pull content dissemination**
  - Users can exchange data using either or both models
- **Flexible protocol and message bindings**
  - Does not require a particular network protocol or message format

TAXII Services

- **TAXII defines four Services**
  - Discovery – A way to learn what services an entity supports and how to interact with them
  - Collection Management – A way to learn about and request subscriptions to Data Collections
  - Inbox – A way to receive pushed content (push messaging)
  - Poll – A way to request content (pull messaging)
- **Each service is optional – implement only the ones you wish**
  - You can have multiple instances of each service
- **Services can be combined in different ways for different sharing models**

Hub & Spoke Example



STIX & TAXII

Analyzing and Sharing Cyber Threat Intelligence

Homeland Security