BLUE COAT®

Security
Empowers
Business

EVOLUTION OF CYBER THREAT INTELLIGENCE

BRET JORDAN CISSP

Director of Security Architecture and Standards

ENISA 2015-02-24

Evolution of Cyber Threat Intelligence

BLUE COAT

- About me
  - Bret Jordan
  - 20+ years in network security
    - Worked in everything from academia, large enterprise, small startups, and now in the vendor space
  - Hold several certifications including:
    - CISSP, GCIH, GREM, GAWN
  - I currently work at Blue Coat Systems where I head up advanced security architecture and standards
    - I came to Blue Coat through the Solera Networks acquisition
  - Active participant on the STIX/TAXII working group
    - Not with a corporate agenda, I get to leave my Blue Coat hat off
    - Helping to guide architectural development of global standards in threat intelligence sharing through active engagement with community

Evolution of Cyber Threat Intelligence

BLUE COAT

- Today I want to talk briefly about the evolution of cyber threat intelligence
  - Specifically, the future of cyber threat intelligence
  - Possible implementations
  - Challenges associated with sharing threat data
  - Risk of the status quo

Evolution of Cyber Threat Intelligence

BLUE COAT

- I believe, we all get the general idea
  - We need an ecosystem where **actionable cyber threat information is shared automatically** across technology verticals and public / private sectors in near real-time to address the ever increasing cyber threat landscape

But How Do We Do This?

The Future of Cyber Threat Intelligence

BLUE COAT

- Over the years the security community and various vendors have proposed several solution to this problem with mixed levels of success, those proposed solutions, to name a few, are:

  - IODEF
    - 2007
    - Incident Object Description and Exchange Format
  - CIF
    - 2009, Educause
    - Collective Intelligence Framework
  - VERIS
    - 2010, Verizon
    - Vocabulary for Event Recording and Incident Sharing
  - OpenIOC
    - 2011, Mandiant
  - MILE
    - 2011
    - Managed Incident Lightweight Exchange
  - OTX
    - 2012, Alien Vault
    - Open Threat Exchange

The Future of Cyber Threat Intelligence

BLUE COAT

- And recently, as of 2013, a new and very promising solution was introduced by the MITRE Corporation
- This solution has quickly gained world-wide support from financial services, CERTS, vendors, governments, industrial control systems, and enterprise users
- This solution is called STIX and TAXII, or as I refer to it
  - "STIX and all of its children"

The Future of Cyber Threat Intelligence

BLUE COAT

- The STIX family includes the following standards giving it a richness and completeness not found with other solutions

- Structured Threat Information Expression (STIX)

- Cyber Observable Expression (CybOX)

- Malware Attribute Enumeration & Characterization (MAEC)

- Common Attack Pattern Enumeration & Classification (CAPEC)

- Open Vulnerability Assessment Language (OVAL)

- Trusted Automated Exchange of Indicator Information (TAXII)

So what is STIX and why is it relevant?

The Future of Cyber Threat Intelligence

BLUE COAT

- First off, STIX is a language for the characterization and communication of cyber threat intelligence
  - Current language bindings are in XML with APIs in Python
  - JSON bindings are forth coming in Python and Golang

- While STIX is NOT a product, process, database, program, or tool, it does support
  - Strategic, operational and tactical cyber intelligence, not just technical cyber defense
  - It also offers a **machine consumable representation** with a consistent expression of that threat information

The Future of Cyber Threat Intelligence

BLUE COAT

- It is important to note that STIX and all of its children, including TAXII were developed openly with strong participation from an **international community** of financial services, governments, vendors, and industry stakeholders

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

The Future of Cyber Threat Intelligence

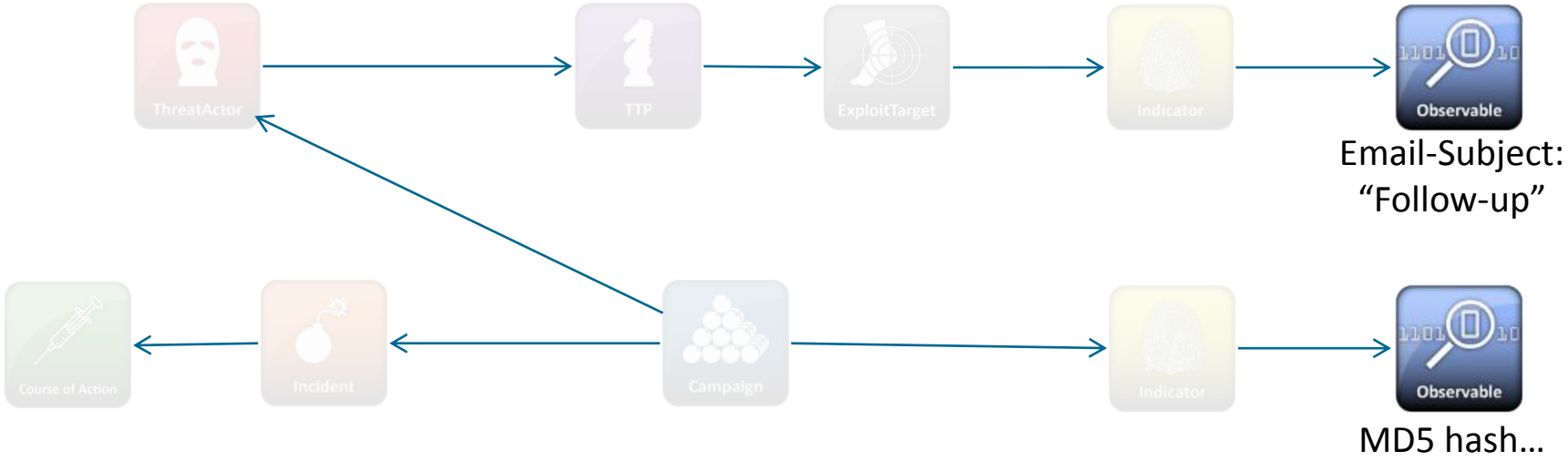
BLUE COAT

- There are 6 idioms in STIX, and they answer questions like:
  - How to describe the threat?
  - How to spot the indicator?
  - Where was this seen?
  - What exactly were they doing and how?
  - What were they looking to exploit?
  - Why were they doing it?
  - Who is responsible for this threat?
  - What can I do about it?

Lets quickly look at each of these Idioms

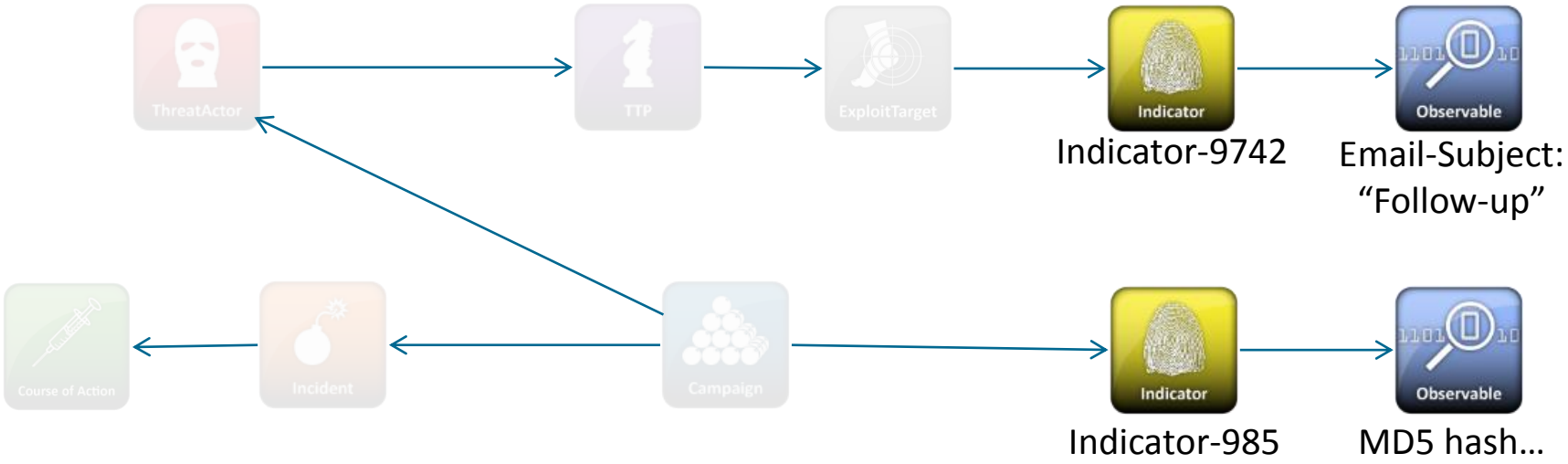
STIX Idioms

- Cyber Observables
  - Identifies the specific patterns observed (either static or dynamic)
  - Examples
    - An incoming network connection from a particular IP address
    - Email subject line
    - MD5 / SHA1 hash of a file

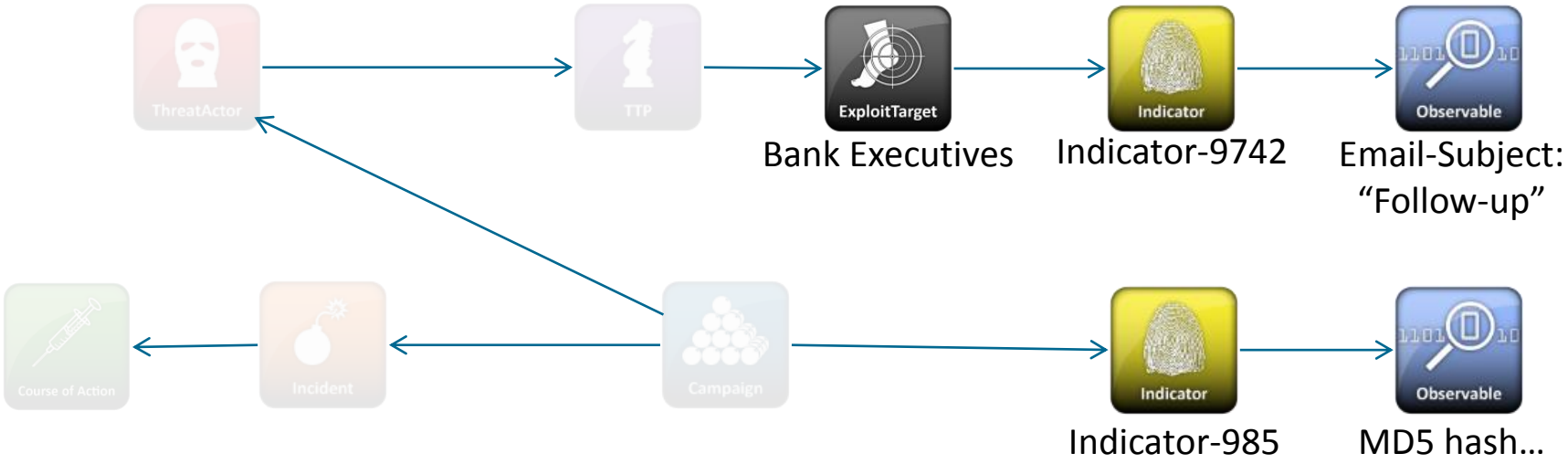


STIX Idioms

- Indicators
  - Identifies contextual information about observables
  - Examples
    - If network traffic is seen from a particular range of IP addresses it indicates a DDoS attack
    - If a file is seen with a particular SHA256 hash it indicates the presence of Poison Ivy

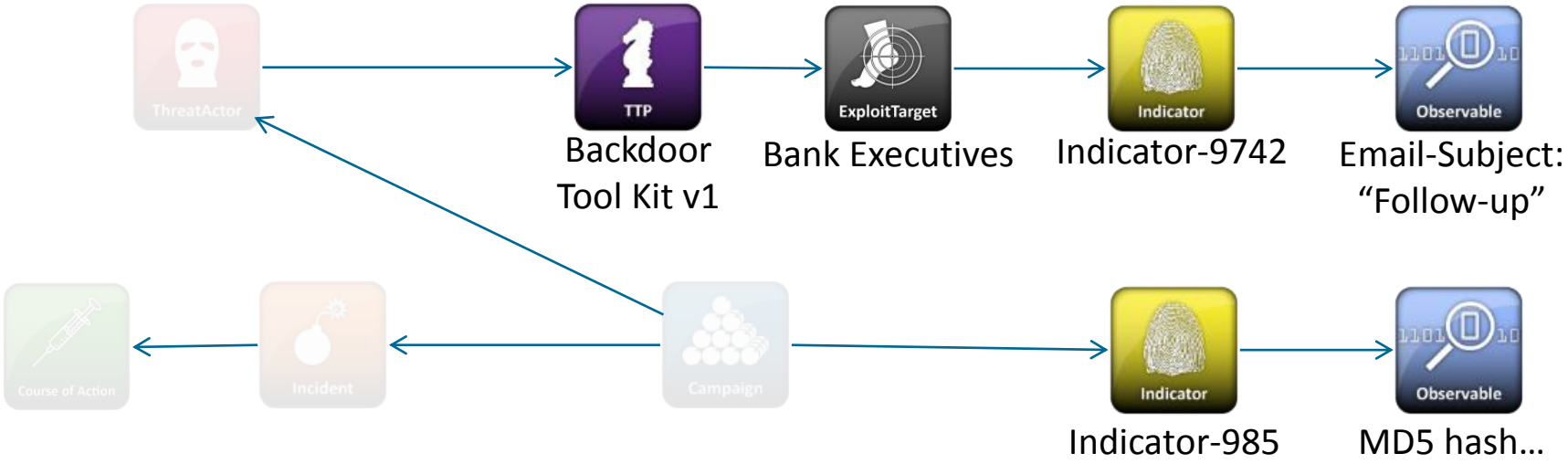


- Exploit Targets
  - Identify vulnerabilities or weaknesses that may be targeted and exploited by the TTP of a Threat Actor
  - Examples
    - A particular MongoDB configuration that leads to a vulnerability in the management console



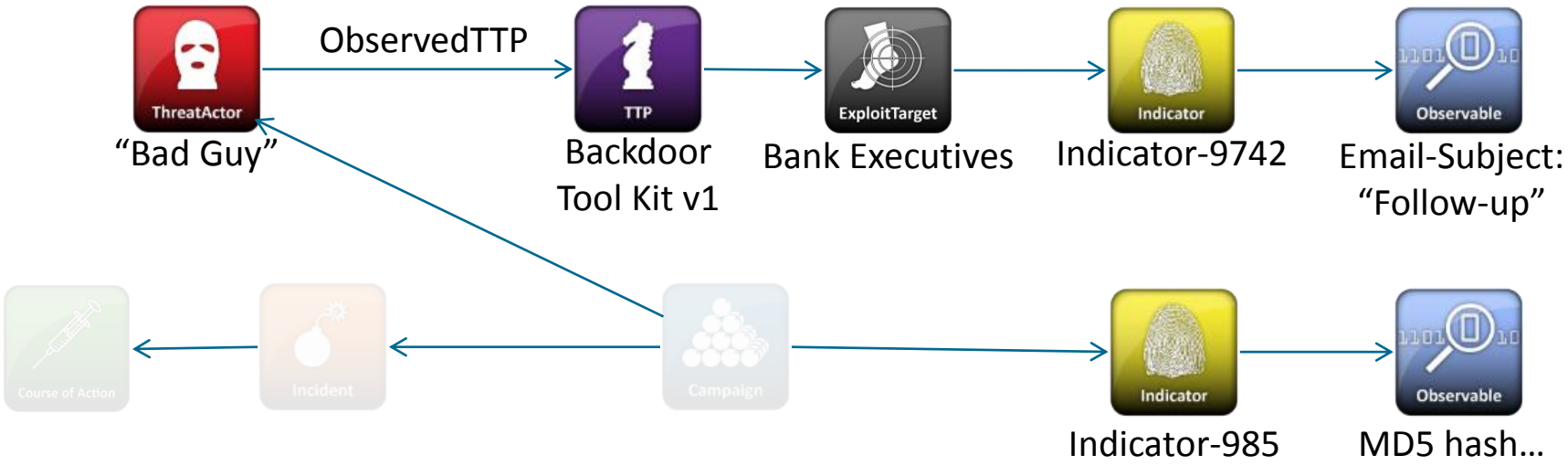
STIX Idioms

- TTPs (Tactics, Techniques, and Procedures)
  - Are the behaviors or modus operandi of cyber adversaries (e.g. what do they do, what do they use, and who and what do they target)
  - Examples
    - Particular range of IP address used for their command and control (C2) infrastructure



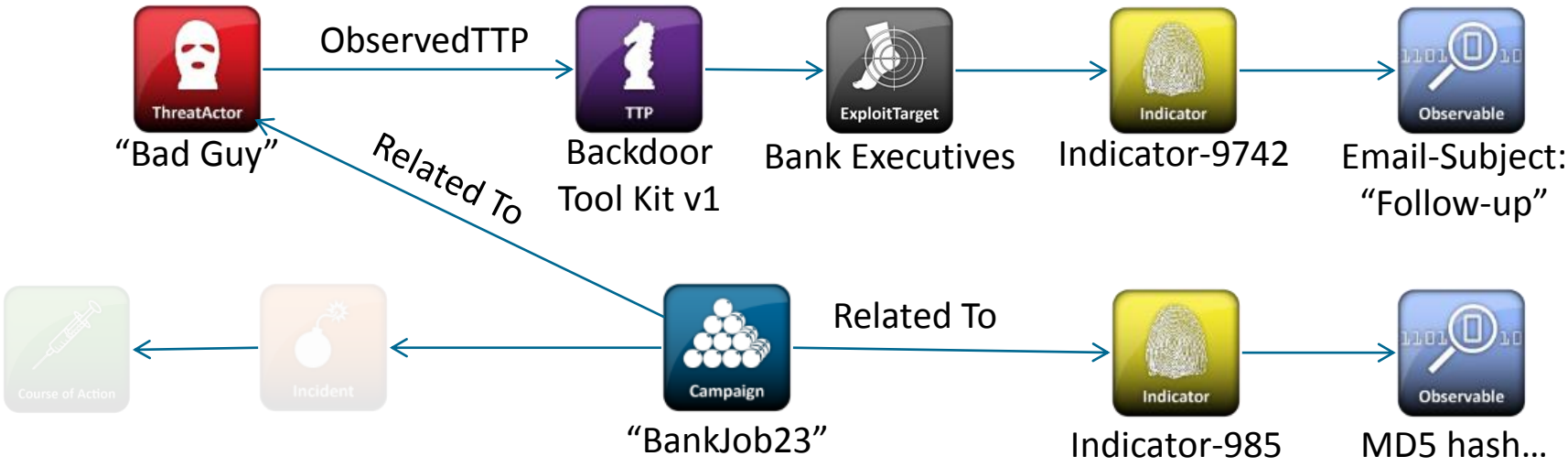
STIX Idioms

- Threat Actors
  - Identifies the characterizations of malicious actors (or adversaries) representing a threat, based on previously observed behavior
  - Examples
    - Assertions that the Threat Actor is also known by the names Comment Crew, Comment Group and Shady Rat



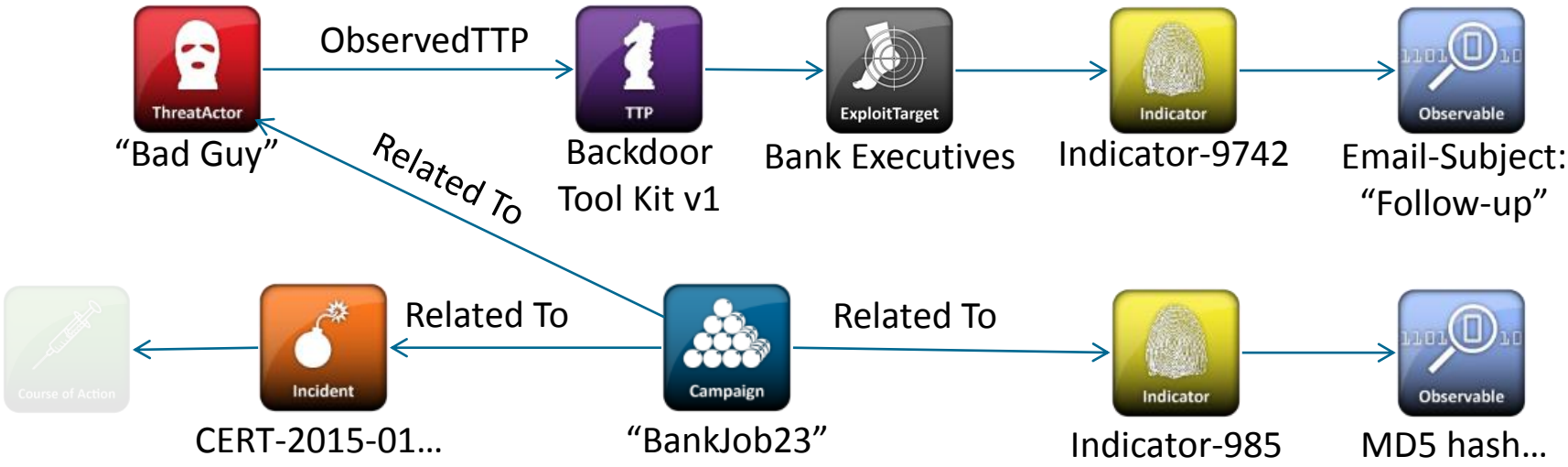
STIX Idioms

- Campaigns
  - Is the perceived instances of the Threat Actors pursuing specific targets
  - Examples
    - Asserted attribution to particular Threat Actors with ties to organized crime



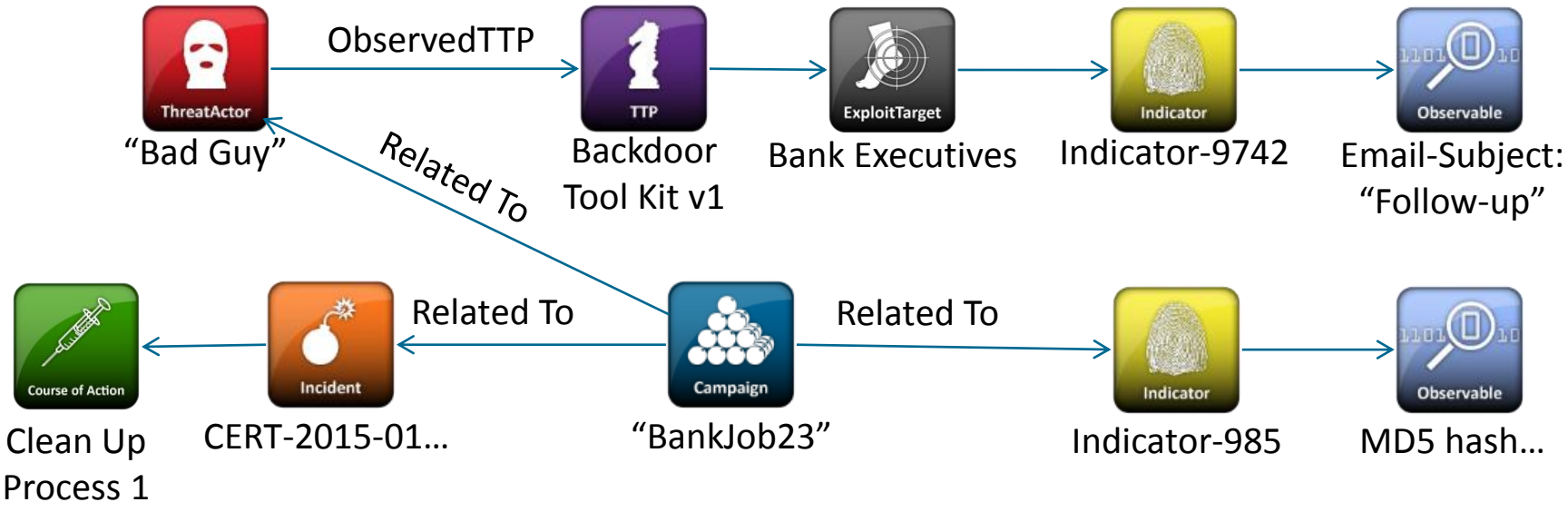
STIX Idioms

- Incidents
  - These are the specific security events affecting an organization along with information discovered during the incident response
  - Examples
    - A laptop assigned to John was found on 2/10/15 to be infected with Zeus using a specific range of IPs for C2.



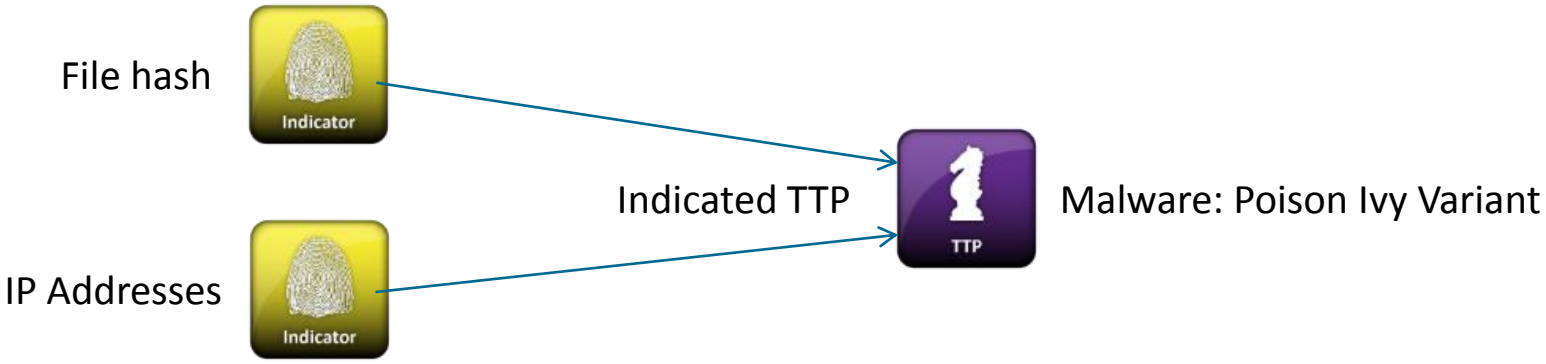
BLUE COAT

- Course of Actions
  - Here is where we can enumerate specific actions aimed to address or mitigate the potential impact of an Incident
  - Examples
    - Block outgoing network traffic to 218.77.79.34
    - Remove malicious files and regkeys and reboot the system



BLUE COAT

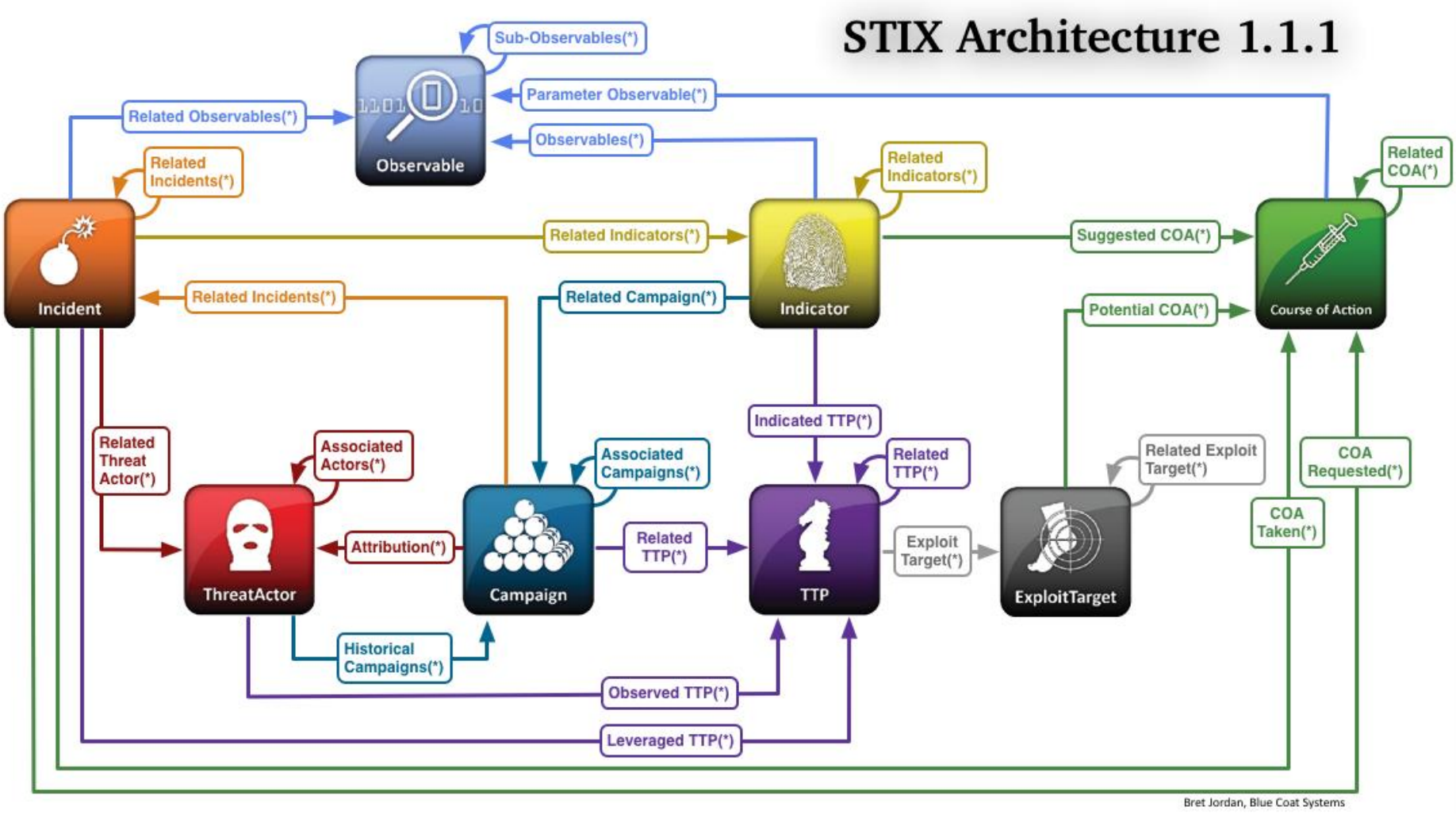
- With all of these idioms, it is important to note that STIX makes use of idref based relationships
  - This allows reuse of all of the Idioms in other STIX packages or even by other users




```
<indicator:Observable id="example:observable-b4ae4ea6-8ce2-41e8-8102-9eb437440e4e">
    <cybox:Object id="example:object-5e46abd0-818e-46a7-aca9-0a403030f1b9">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
            <FileObj:Hashes>
```

The Future of Cyber Threat Intelligence

BLUE COAT



So what is TAXII?

The Future of Cyber Threat Intelligence

BLUE COAT

- TAXII is a set of services for exchanging cyber threat information
  - TAXII is NOT a product, process, database, program, or tool
  - TAXII does NOT mandate any particular trust agreements or sharing models
    - Share only what you want and with whom choose

- The TAXII specification is an open community effort to address the operational needs of effectively sharing cyber threat intelligence with a diverse community
  - Existing standards did not solve the problem
  - Developed with strong participation from an international community of governments and industry stakeholders
  - **It is in operational use today**

The Future of Cyber Threat Intelligence

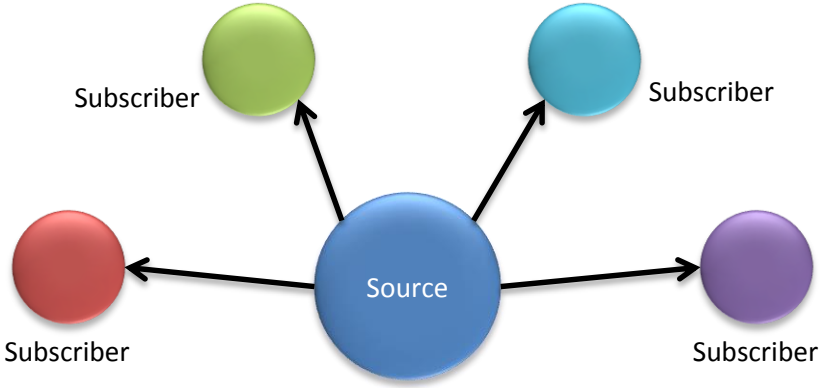
BLUE COAT

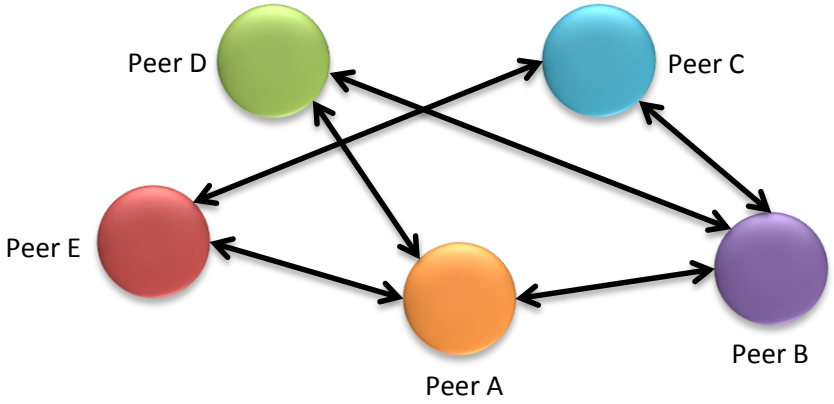
- TAXII defines four services for its operation
  - Discovery Service
  - Inbox Service
  - Poll Service
  - Collection Management Service

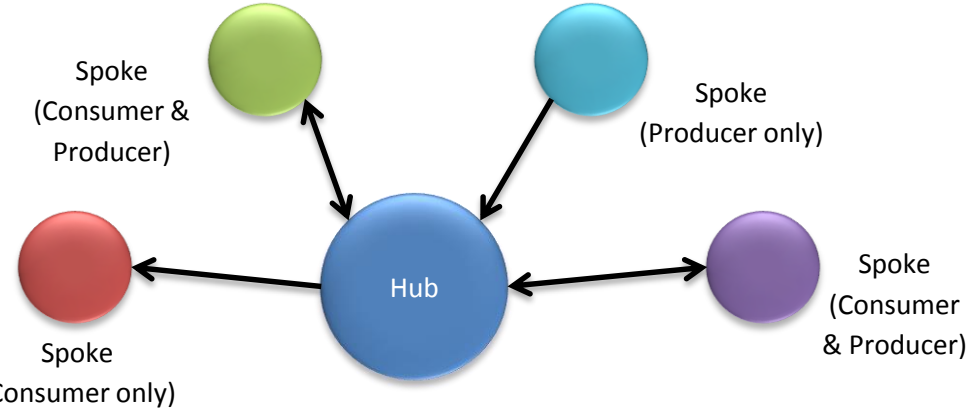
- Each service is optional

- Services can be combined in different ways for different types of sharing models and to address different needs

- The three sharing models TAXII supports are
  - Publisher (push)
  - Subscriber (pull)
  - Mesh (p2p)



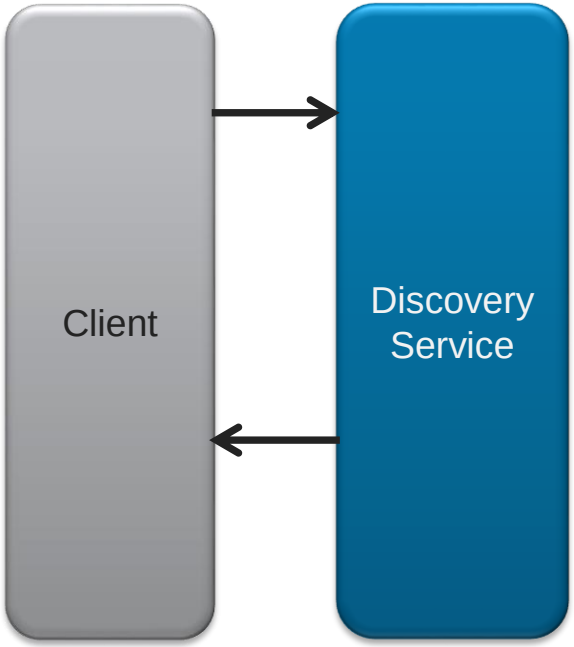




Source: MITRE

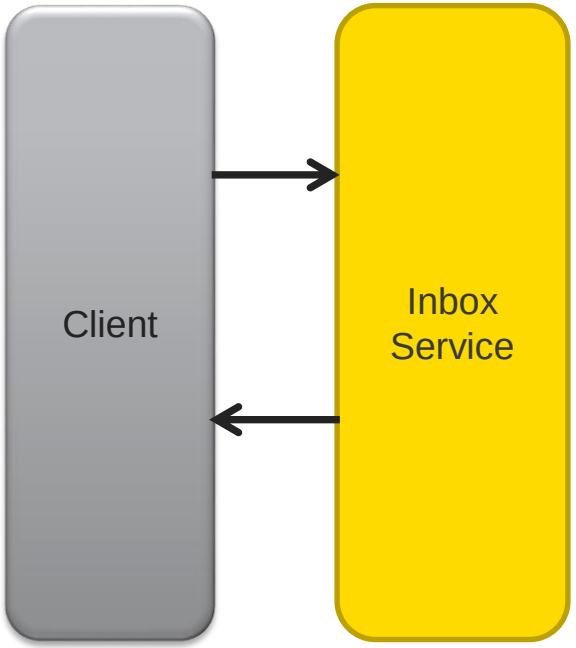
- TAXII Discovery Service
  - Allows clients to discover what TAXII services are currently being offered by a server

- Example
  - Client sends a Discovery Request
    - The Discovery Request does not have any parameters
  - Server responds with a Discovery Response that lists the TAXII Services being offered
    - This data includes service type (e.g., Inbox), address, description, etc.



- TAXII Inbox Service
  - Is hosted by data consumers to receive pushed content
    - Basically a listener for incoming content

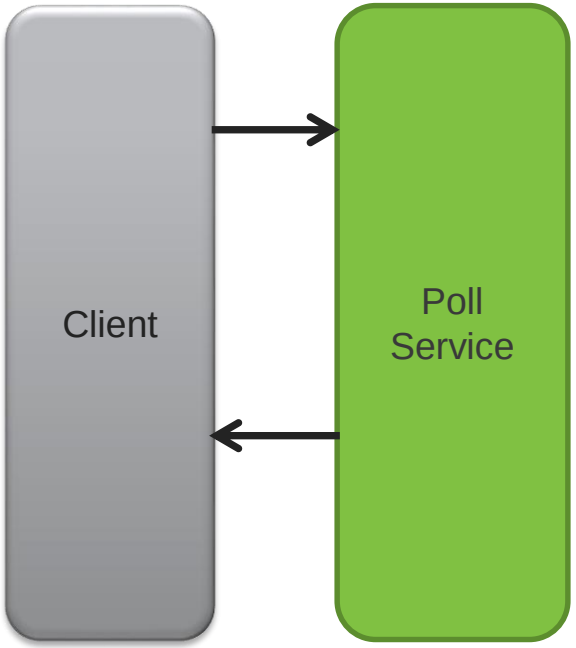
- Example
  - Client sends an Inbox Message containing 0 or more content blocks
  - Server responds with a Status Message (indicating either success or an error condition)



BLUE COAT

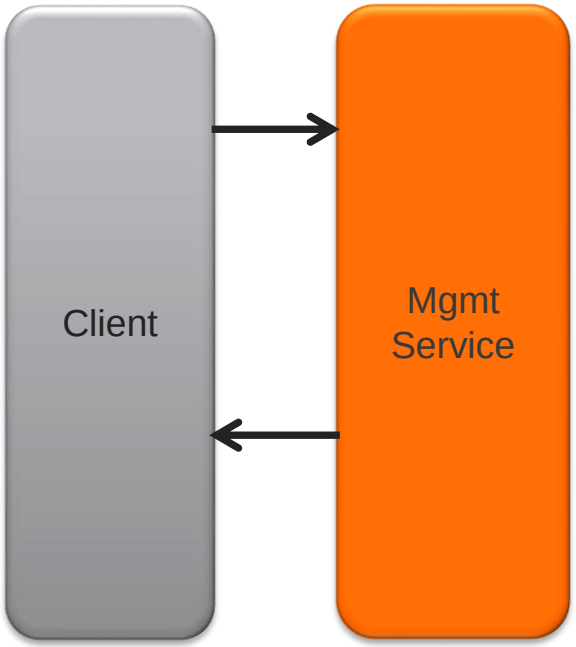
- TAXII Poll Service
  - This is hosted by data producers to allow consumers to poll data
  - Consumers request updates relative to a TAXII data collection

- Example
  - Client sends Poll Request (contains Data Collection name, optional query, etc)
  - Server responds with a Poll Response containing 0 or more content blocks or a status message

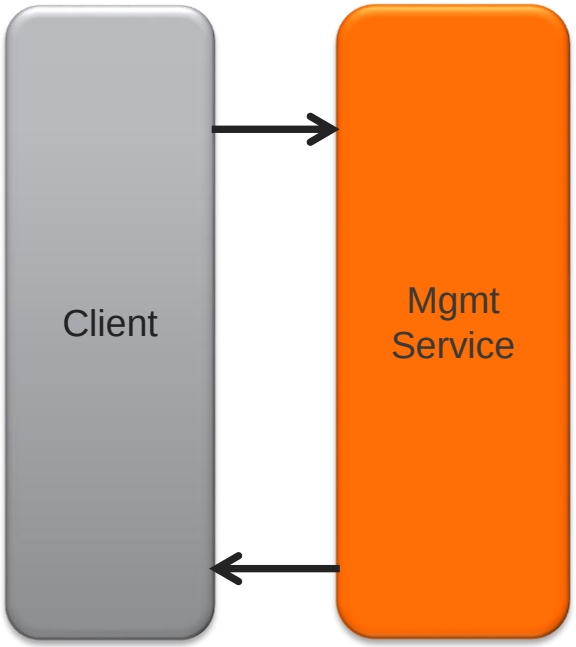


- TAXII Management Service
  - This is hosted by data producers to provide information on Data Collections and/or process Subscriptions
  - Can offer one or both of the two message exchanges
  - Does not specify the process for deciding whether to allow the requested action to occur nor how the action should be processed
    - This just deals with arranging subscriptions, not the actual data dissemination

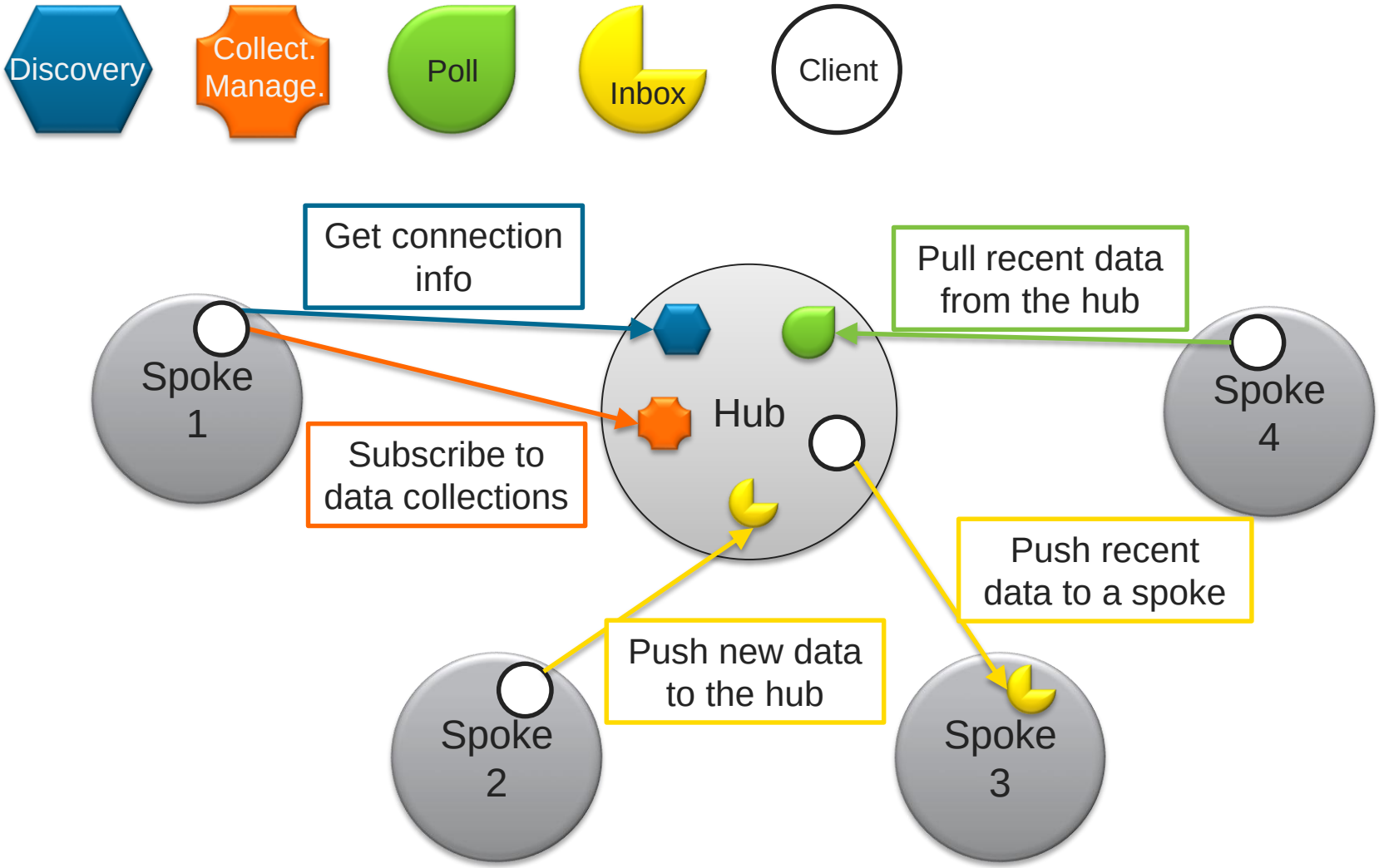
- Example 1
  - Client sends a Collection Information Request
    - No parameters
  - Server responds with a Collection Information Response listing
    - Data collections and descriptions
    - How to access data and a status message.



- Example 2
  - Client sends a Manage Collection Subscription Request
    - Requesting a status, create, cancel, pause, or resume action on a subscription
    - Requests can include a query
  - Server responds with a Manage Collection Subscription Response or Status Message
    - Note this just deals with arranging subscriptions, not actual data dissemination



The Future of Cyber Threat Intelligence



The Future of Cyber Threat Intelligence

BLUE COAT

- Things that the specification does not define
  - Out of band agreements on sharing
  - How to perform authentication for your data
  - Authorization / subscription management
  - Which protocol to use
    - Current bindings for HTTP / HTTPS but it is not restricted to HTTP

CHALLENGES

with sharing threat data

Challenges With Sharing Threat Data

BLUE COAT

- Requirements
  - Need a production worthy high performance TAXII server and client
    - Current options
      - Proof of concept YETI project (Python / Django)
      - Proof of concept Java client
      - FS-ISAC's Soltra Edge
      - A lot of work being done here, but no "FreeRADIUS" yet
  - Decide what type of data you will share and with whom
    - STIX Profiles can help
    - Some data may not be appropriate to share without sufficient sanitization, so you will need a process to do that
      - STIX Profiles can help with this too
  - What type of sharing models will you allow?
    - How much do you trust those you will be sharing with

Challenges With Sharing Threat Data

BLUE COAT

- Requirements (cont.)
  - What are you going to do / can you do with the data?
    - Consume / use internally
    - Republish, become a warehouse
    - Enrich with other data sources, fill in the gaps
    - Correlate data
    - Provide intelligence on the data itself
      - I believe this to be one of the most fascinating ideas, imagine…..
  - Setup sharing agreements, work with your legal department
  - Agree to handling and marking of sensitive data and what people can then do with it.
  - Provide authentication of services

Challenges With Sharing Threat Data

BLUE COAT

- Lets assume for a minute that we can all agree on a standard and all the technical problems associated with that standard get resolved.

- There are still a lot of challenges to be overcome as the **real problems are not technical** but procedural, operational, and legal

Challenges With Sharing Threat Data

BLUE COAT

- These are the types of sharing models that most people will participate in, as I see it:
  - Open Source Intelligence (OSI) provider
    - Similar what we have today with URL blacklist and things like VirusTotal
    - Limited to Indicators, Observables, and basic Course of Action
  - Subscription based private intelligence
    - This is usually found in the vendor space and may be tied to products and subscription fees
  - Open sharing within a restricted ecosystems
    - Financial services, industrial control systems, governments, vendor alliances

Challenges With Sharing Threat Data

BLUE COAT

- Actually using the data to get value
  - We need to stop just talking about it
- Managing trust and reliability
  - How do you know if these systems or the data is trust worthy?
  - Knowing if the threat intelligence repos have been poisoned
- Chain of custody
  - Know all of the parties involved with that piece of threat intelligence
  - Protect anonymity from sources that can not be named
- Privacy
  - Lots of seemingly benign data can tell you a lot, how do we protect user

Challenges With Sharing Threat Data

BLUE COAT

- Restrictions on enrichment, collaboration and sharing
  - No one has the full picture
  - Only share what you want and with whom you want
  - Making sure it does not spread beyond your comfort level
- Keep your hands off my data
  - Controlling what people do with your data if you share it
- Mixing public and private sectors
- Who really owns the data
  - How do you guarantee a retraction and deletion of previously sent data
- How do you do X, Y, and Z
  - Sightings, the like or the +1 of Facebook like tools

Challenges With Sharing Threat Data

BLUE COAT

- Speed
  - Most current cyber intelligence delivery methods are manual and human-to-human
  - Most are unstructured and reside in lists or in IPS signatures
- Lack of vendor buy in
  - Vendors wanting everything and sharing nothing
  - Vendor to vendor product communication
    - Just imagine….
- Liabilities Issues
  - Defamation of character if you mesh the physical world with the cyber and get your assertions wrong
  - Exposing your capabilities

Challenges With Sharing Threat Data

- In the end, legal council may still say NO with reasons of
  - Government legal restrictions
  - Fear of being sued
    - Need immunity to litigation
  - Contractual agreements with customers and providers

Source / Subscriber Walkthrough

Source / Subscriber Walkthrough

- Goals for sharing in source subscriber model
  - A vendor (the source) wants to publish threat alerts as information becomes available
  - Customers (subscribers) can pay to receive these daily updates
  - There may be multiple levels of access depending on contract negotiations
  - Currently, customers log into the vendor web site to view updates in a manual way, the desire is for this to be automated

Source / Subscriber Walkthrough

- Step 1: Vendor organizes data records into TAXII Data Collections
  - Decides on a “contract level” for the collections
    - Many records will be present in all collections, but some fields may be removed before dissemination depending on their contract and their subscription level
  - All Data Collections are Data Feeds
    - The vendor wants the data to be ordered so that consumers can request only the most recent data
  - Access to a feed contingent upon the purchasing of a contract

Source / Subscriber Walkthrough

- Step 2: Vendor labels all data within each TAXII Data Feed with a timestamp
  - Decides to use the time of posting as that timestamp
    - More than one data record may have the same timestamp – not a problem
    - A single record could have the same timestamp in all of the data feeds – not a requirement

Source / Subscriber Walkthrough

BLUE COAT

- Step 3: Vendor implements a TAXII Collection Management Service to handle
  - Collection Information Requests
    - Lists available collections
    - Explain what information is provided via each collection (i.e., contract levels)
    - References to the site where one can purchase needed contracts
  - Collection Management Requests
    - Forward management requests to the back-end for comparison to purchased contracts

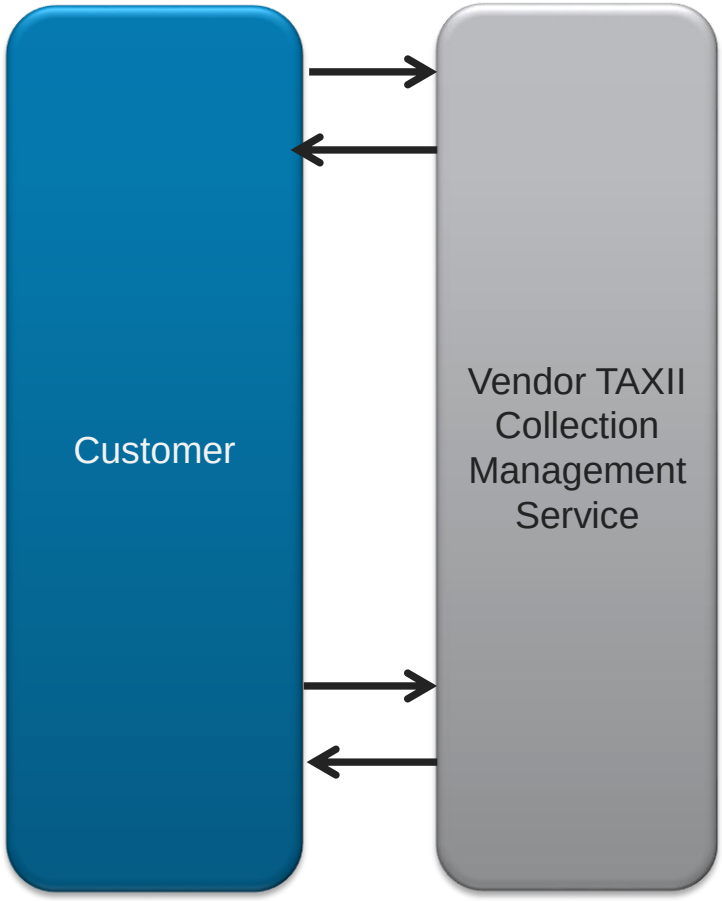
Source / Subscriber Walkthrough

BLUE COAT

- Step 4: Vendor must do at least one of the following:
  - Implement a Poll Service
    - Give customers the option to pull content from a collection
  - Interface with customers' Inbox Services
    - Support pushing content to the customer TAXII Inbox Service
  - Decides NOT to implement a Discovery Service
    - Vendor decides to continue publishing this information using HTML

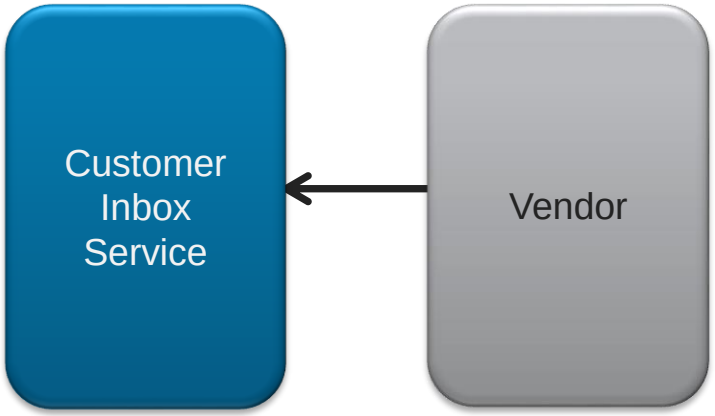
Source / Subscriber Walkthrough

- Step 5: Establish Sharing Relationships
  - Customer contacts vendor's Collection Management Service to get list of collections
  - Customer purchases a contract via Vendor web site
    - Out-of-band
    - Also establishes authentication credentials
  - Customer contacts vendor Collection Management Service to establish a subscription
    - Request verified before acceptance

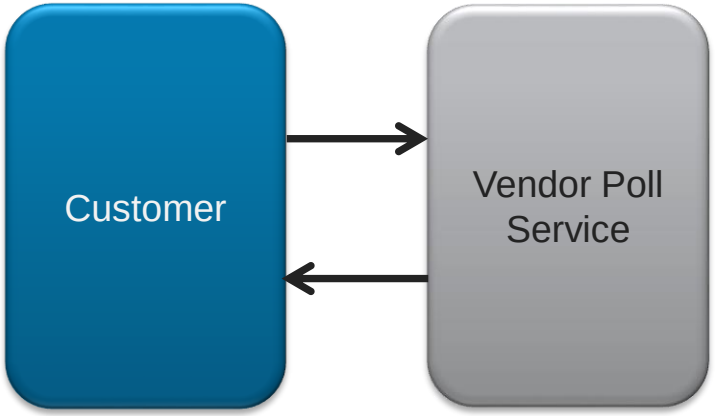


Source / Subscriber Walkthrough

- Step 6: Share Information
- Content can be pushed to Customer's Inbox Service



- Customer can pulls from Vendor's Poll Service
  - Request verified before being fulfilled



Hub & Spoke Walkthrough

Hub & Spoke Walkthrough

- Goals for sharing in hub and spoke model
  - Community exists with a pre-existing intra-group sharing agreement
  - Currently all threat alerts sent via e-mail to the group mailing list, the desire is for automatic re-distributed to all group members

Hub & Spoke Walkthrough

BLUE COAT

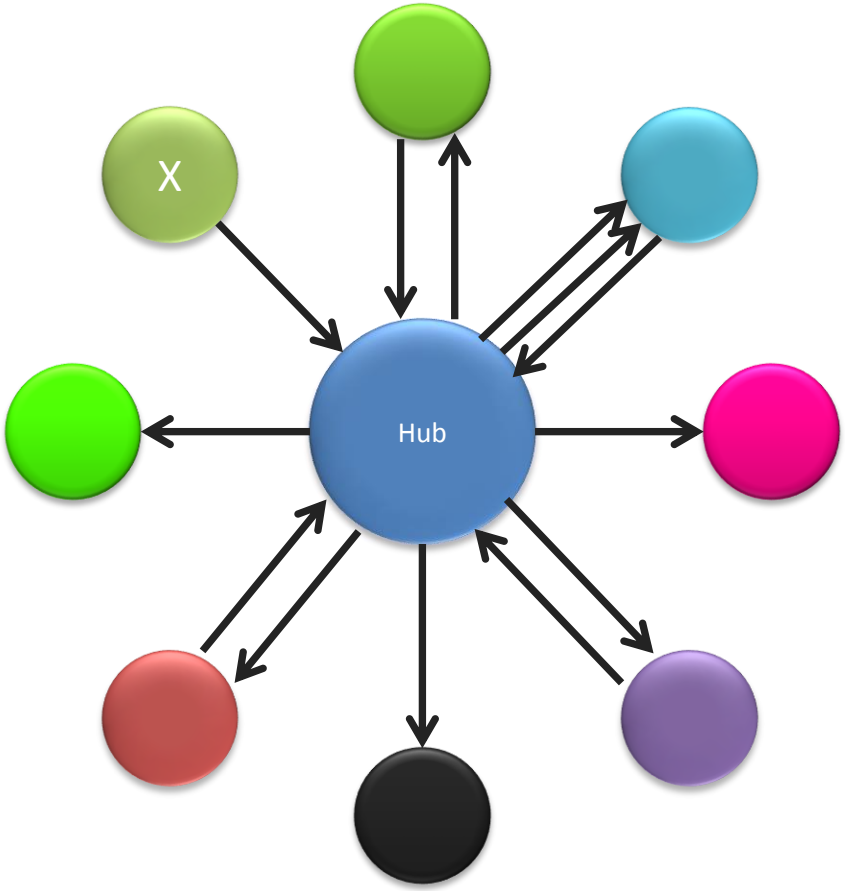
- Step 1: Hub Implements various TAXII services
  - Implements the Inbox Service
    - Used to receive all input from spokes (Hub does not poll)
  - Decide to interface with Spokes' TAXII Inbox Services for message delivery
    - Support pushing of alerts to spokes
  - Decide to implement a Poll Service
    - Support spokes pulling current and/or archived alerts
    - Decide on only one TAXII data feed for all information
    - Decide timestamps = the time the alert arrives in Hub's Inbox
  - Decide NOT to implement a Discovery Service
    - Members informed of the Hub's services via other means
  - Decide NOT to implement a Collection Management Service
    - Spokes automatically enrolled when they join the sharing group

Hub & Spoke Walkthrough

- Step 2: Spokes Implement various TAXII services
  - Spokes that produce data interface with the Hub's TAXII Inbox Service
  - May implement an Inbox Service
    - If spoke wants pushed info, must implement Inbox
    - May avoid implementing if all content to be pulled via Poll Service
  - Some spokes may interface with the Hub's TAXII Poll Service
    - May avoid this use if all content to be pushed to the spoke's Inbox Service

Hub & Spoke Walkthrough

- Step 3: Share
- Spoke X pushes new indicator to Hub's Inbox Service
- Hub re-sends indicator to all spokes that requested push notification
- Hub archives indicator so spokes can poll for the alert at a later time



WHAT

if we do nothing, and just maintain the status quo?

Three Scenarios For The Future

BLUE COAT

- Three options for the future, in regards to cyber threats and their impact on our way of life, society, and the global economy and local GDP.

- Option 1: Muddling
  - Threat Actors continue to erode trust and compromise networks
  - Cyber defenses increase yet continue to play catch-up
  - Confidence in cyber threat innovation wanes or becomes less relevant

Three Scenarios For The Future

BLUE COAT

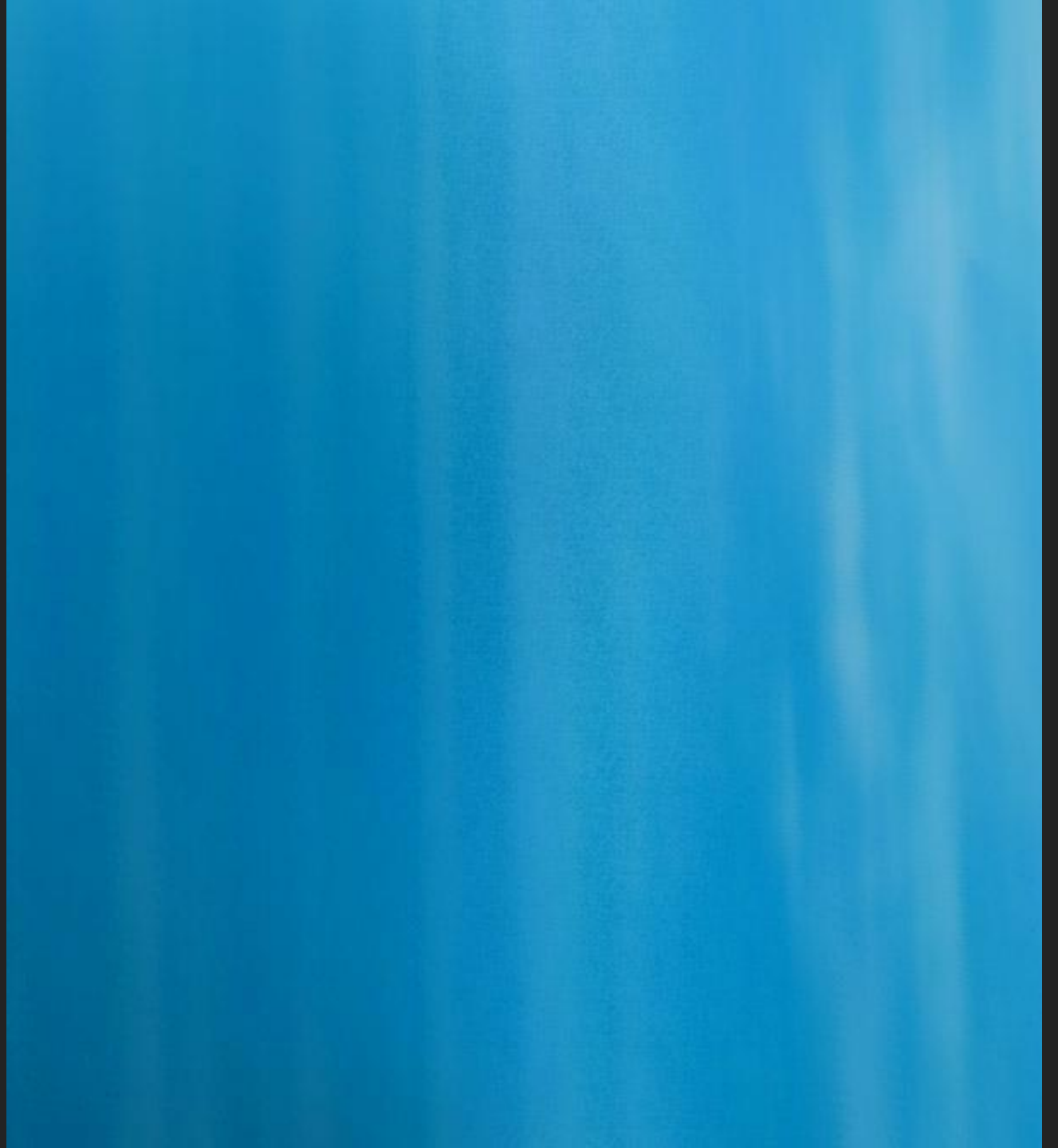
- Option 2: Backlash
  - Threat Actors makes significant progress
  - Rate of compromised networks increases
  - Companies pull back from deploying new technology that is deemed low-value or high risk
  - Technology innovation falters
  - Consumer trust completely erodes
  - Global GDP is effected

Three Scenarios For The Future

- Option 3: Cyber resilience and accelerating digitalization
  - Cyber defenses begin to outpace Threat Actors
  - Network security becomes a reality
  - Costs are transferred to the Threat Actors
  - Advanced zero day toolkits are only useful for days rather than months or years

Final Thoughts

- Join the open community effort
  - Become part of the solution
  - Help build a more secure world
- STIX and TAXII Project Pages
  - http://stixproject.github.io/
  - http://stix.mitre.org/
  - https://taxii.mitre.org/
- Proof of Concept Code
  - STIX APIs and Validators (Python)
    - https://github.com/STIXProject
  - TAXII Client, libtaxii (Python)
  - TAXII Server (Python/Django)
    - https://github.com/TAXIIProject/yeti


BLUE COAT®
Security
Empowers
Business