CTI Automation is harder than it needs to be…

Allan Thomson, LookingGlass Cyber Solutions CTO

Co-Chair OASIS CTI Interoperability

June 2018

FIRST™ Improving Security Together

LOOKINGGLASS

What Cyber Threat Intelligence (CTI) users say about automation

"CTI vendors should figure out how to orchestrate their tools, they are falling behind on protecting because of alert fatigue and are missing legitimate issues"

VP, Security Operations

"If CTI vendors would provide more context to their data, it would be so much easier to know what to do if we see an alert"

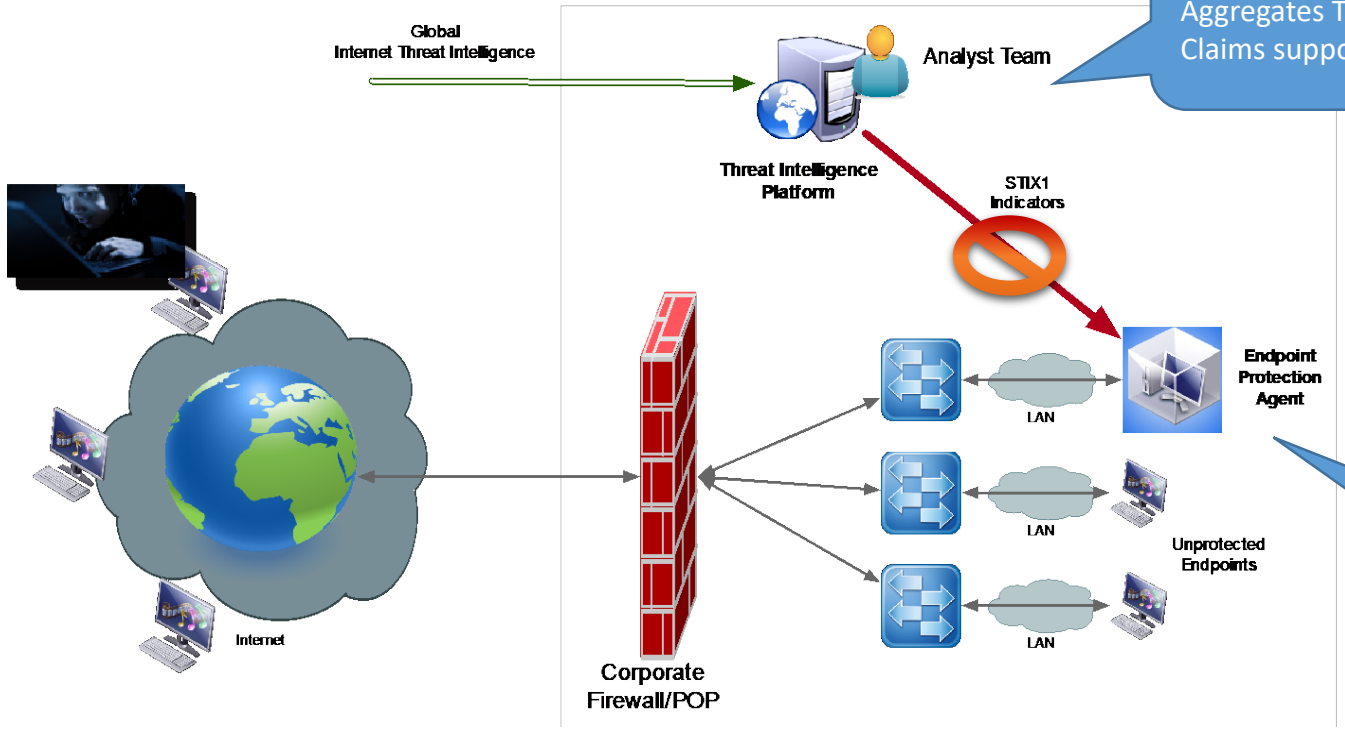
Senior Director, Threat Research

Desired Outcomes for CTI Automation

- Provide Coordinated Actions During Incident Response
- Integrate Multiple Systems
  - Typically different vendors
- Enable Different Functions & Tasks
  - Firewall vs SIEM vs Endpoint protection
  - Threat analysis vs Incident response
- Support Best Practices with Easy Plug & Play

Large Multinational Media Company Challenge

- 10000s of Windows endpoints
- Mature Security Analysis and Operations Team



Vendor A: Threat Intelligence Platform
Aggregates Threat Intelligence feeds
Claims support of STIX Version 1 Indicators

Issue: Indicators not defined in compatible manner despite both vendors verifying against STIX 1 specification

Vendor B: Endpoint Protection Agent
Inspects for malware, correlates against global Indicators
Claims support of STIX Version 1 Indicators

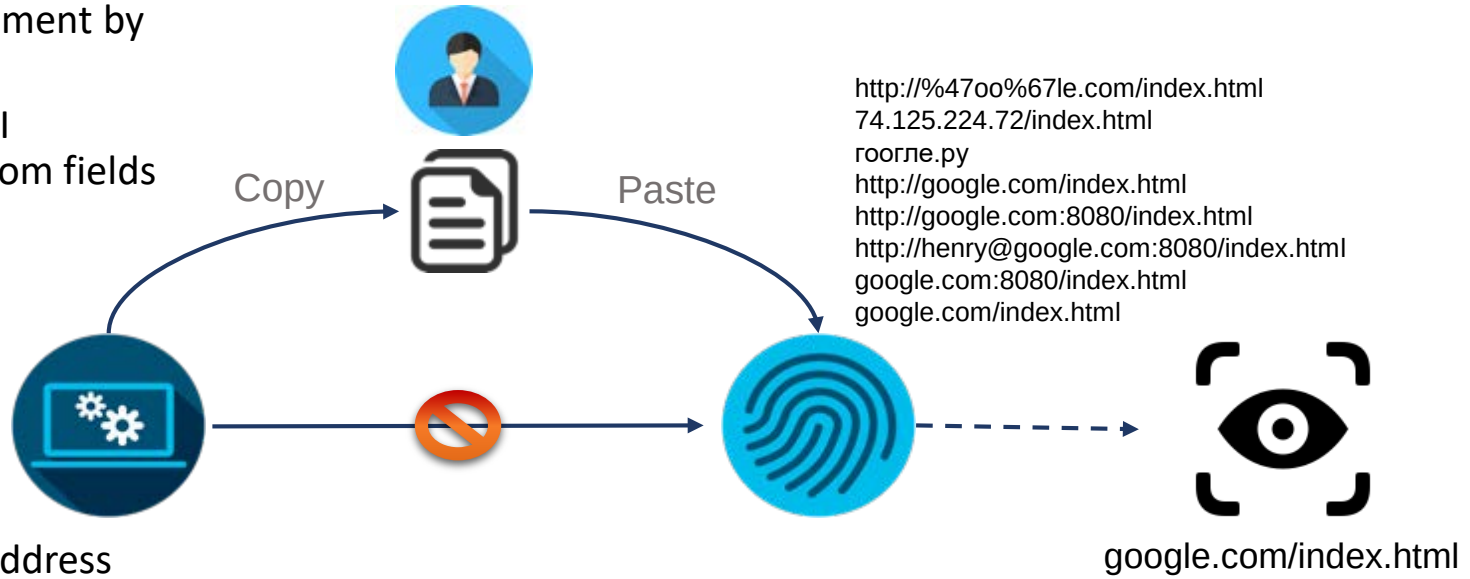
Result: Failed to debug problem, both vendors support & engineering teams involved

Fortune 500 Enterprise Challenges

Issue: Interoperability fails due to authentication or non-standard implementation of STIX 1.x

Heterogenous Integration Points

- Claims support for STIX and TAXII – integration requires development by customer
- Claims support for STIX – API authentication requires custom fields



Data Normalization

- URL-Encoding
- Missing protocol and/or IP address in the URL
- Unicode
- Port, protocol, authentication

Result: Users have to copy-paste indicators from TIP to firewalls' blacklist and manually age them out

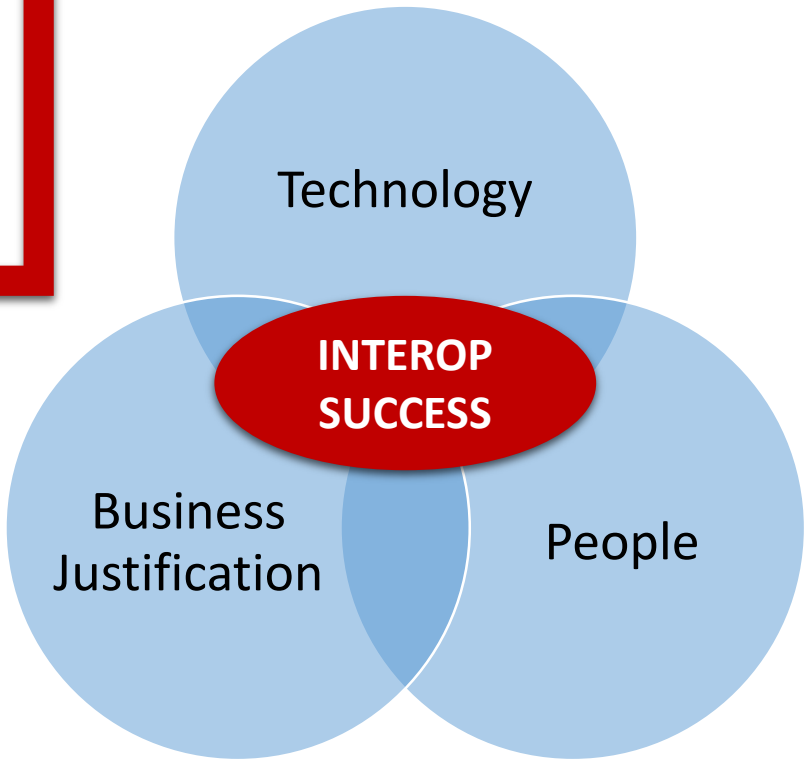
Lack Of Interoperability Impacts Security Response

- Required Expertise & Human Resources
  - To understand technically what is working
- Increased Time & Costs
  - Multiple days/weeks to make it ‘work’
  - Multiple orgs involved
- Reduced Capability
  - Unexpected results
  - Undermines protection

Result is … Adversaries WIN

Where Security Interoperability Challenges Lie…

- Technology
  - Specifically what technology standards supporting automation
- People
  - What are their roles, objectives and motivations
- Business Justification
  - Building a business case for interoperable solutions



OASIS Standards For Security Automation

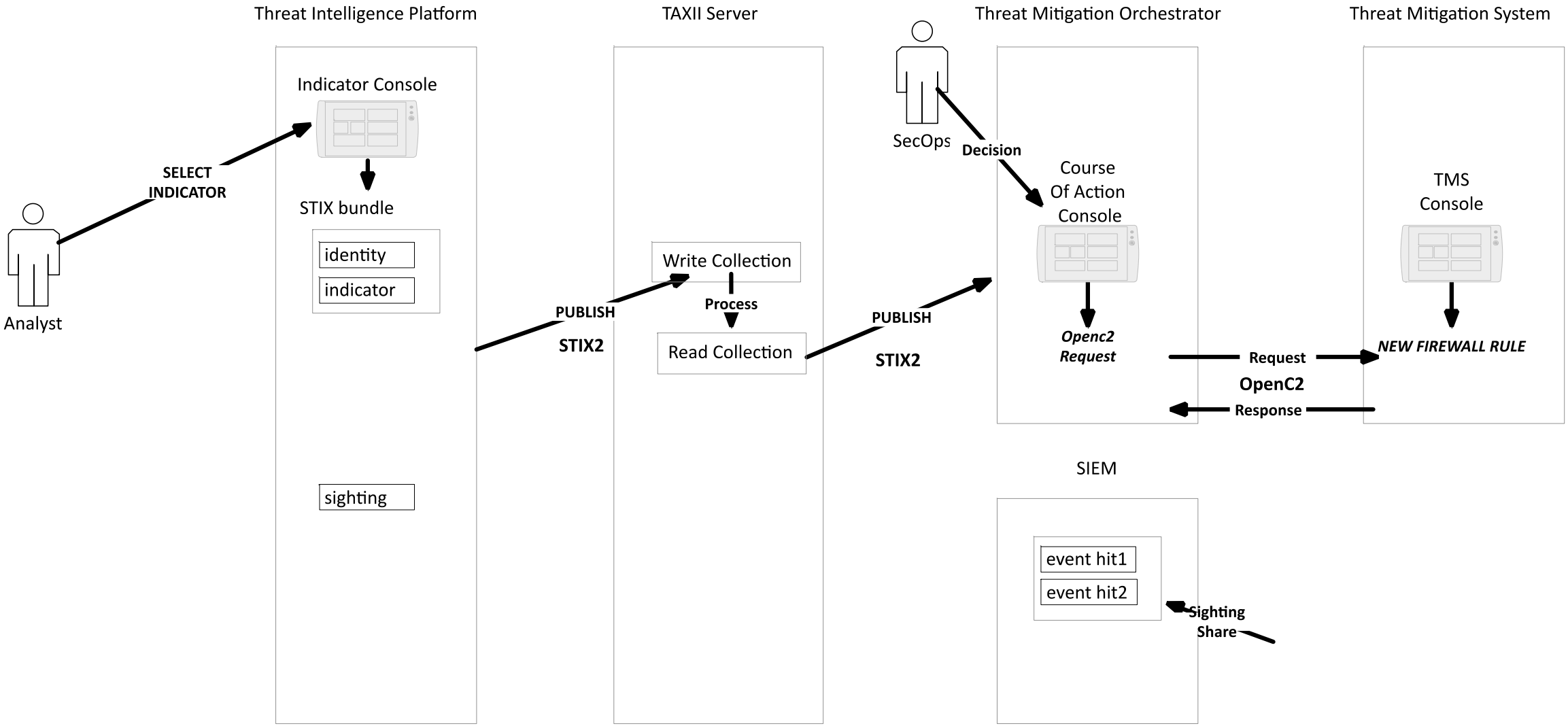
STIX/TAXII Version 2

- Focused on CTI analyst sharing; supports security operations; threat hunting; forensic analysis
- Automation Improvements
  - **JSON, not XML**
    - Scale and performance improvements
  - **Simplicity and Clarity**
    - Reduce variability across implementations
  - **Pragmatism**
    - Fewer, but better-understood objects and properties
  - **Integrated Standard**
    - Integrated observed meta-data with STIX
  - **Relationships as first-class objects**
    - Enabling cross team collaboration
  - **Easy customization & extension**
    - Support organizational specific features

OpenC2

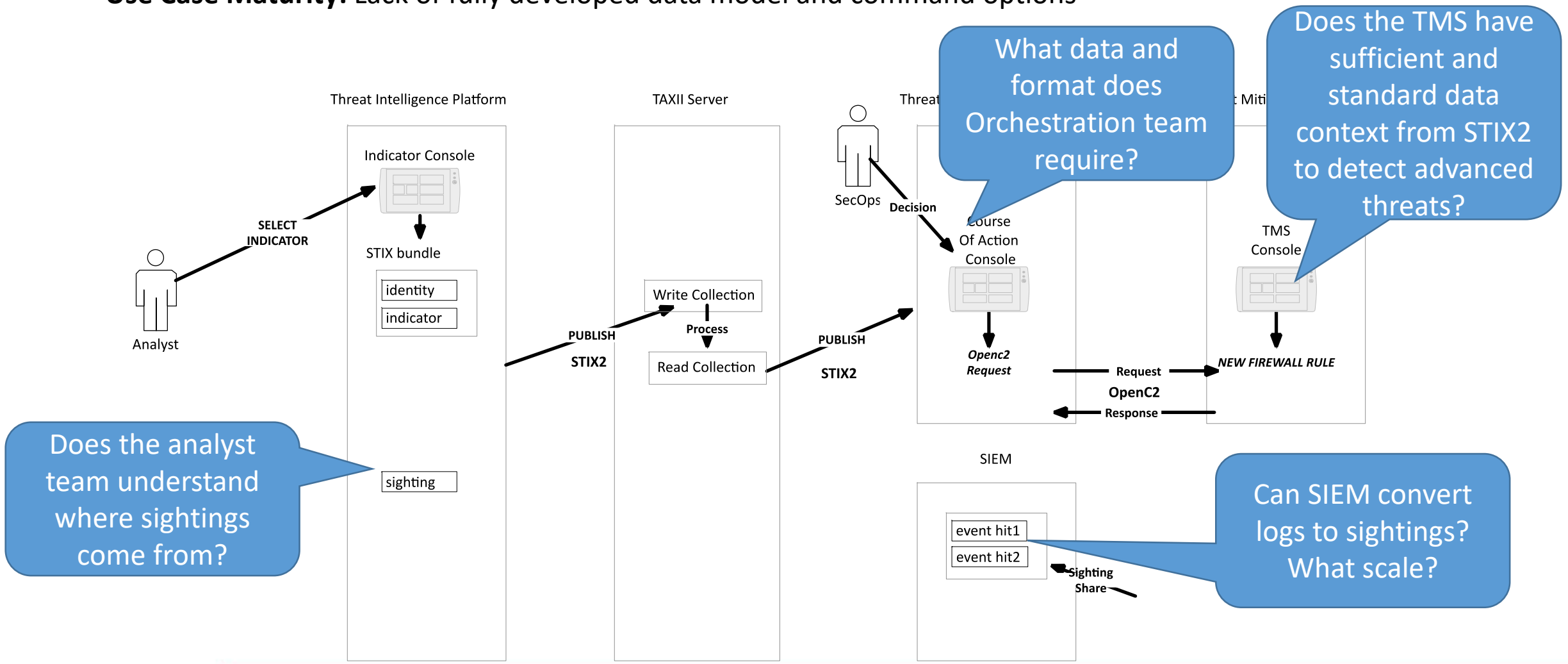
- Focused on command and control orchestration primitives supporting incident response; threat hunting…etc
- Automation language across
  - **JSON-Based**
  - **Mitigation Across All Protected Assets**
    - Endpoint files; registries; memory…etc.
    - Network flows; urls…etc.
    - Users
  - **Mitigation Actions including**
    - Block, Allow
    - Move, Delete
  - **Investigation Actions including**
    - Query
    - Scan
    - Locate

Hypothetical Operational Deployment



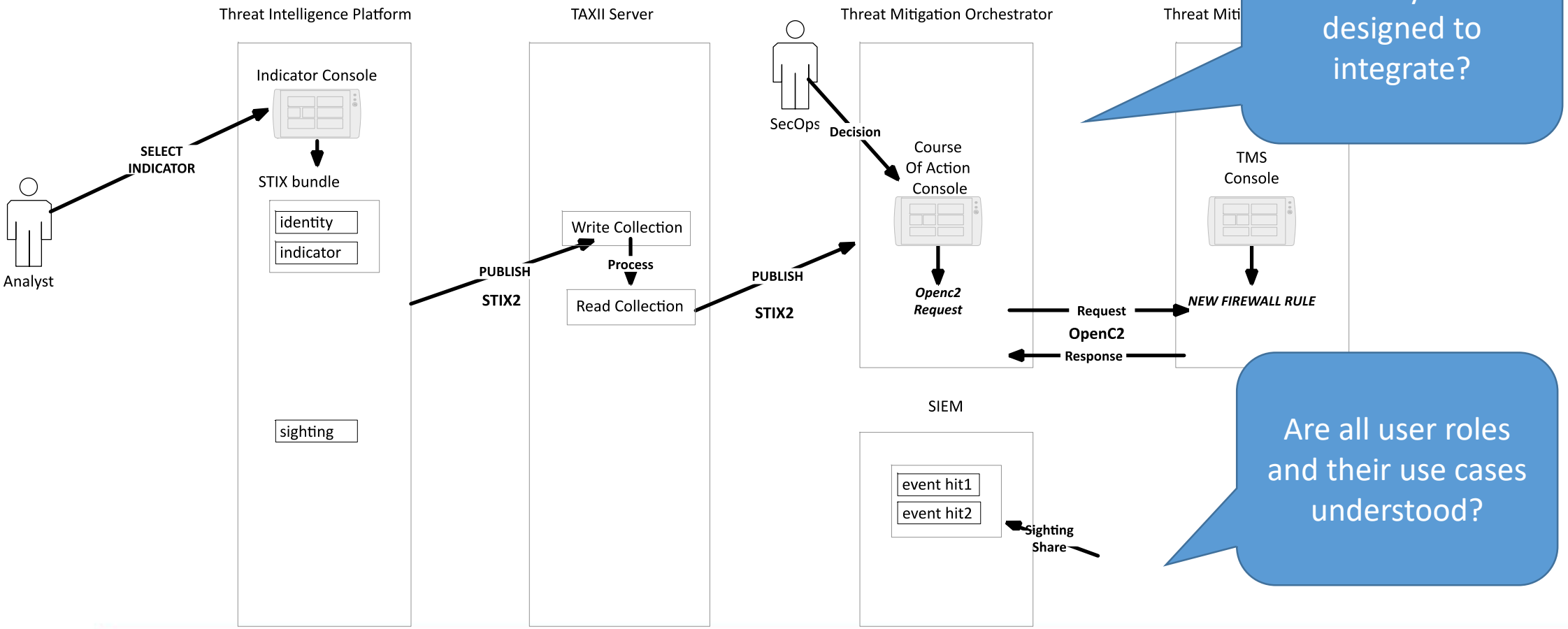
Continuing Challenges with STIX/TAXIIv2 & OpenC2

- **Use Case Maturity:** Lack of fully developed data model and command options



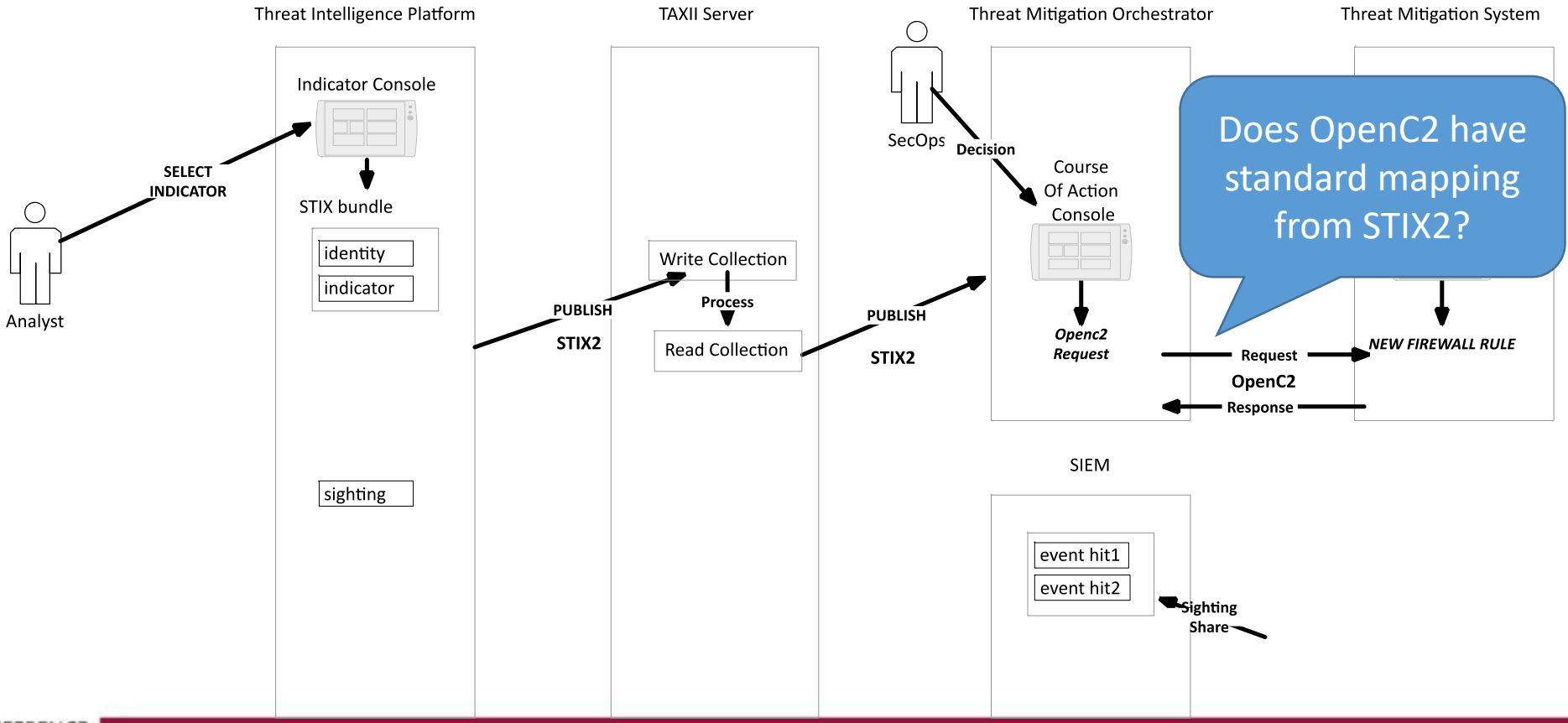
Continuing Challenges with STIX/TAXIIv2 & OpenC2

- **End-to-End Workflows:** Mostly developed independently
  - Lack common vision of how intelligence and C2 are used in coordinated ecosystem



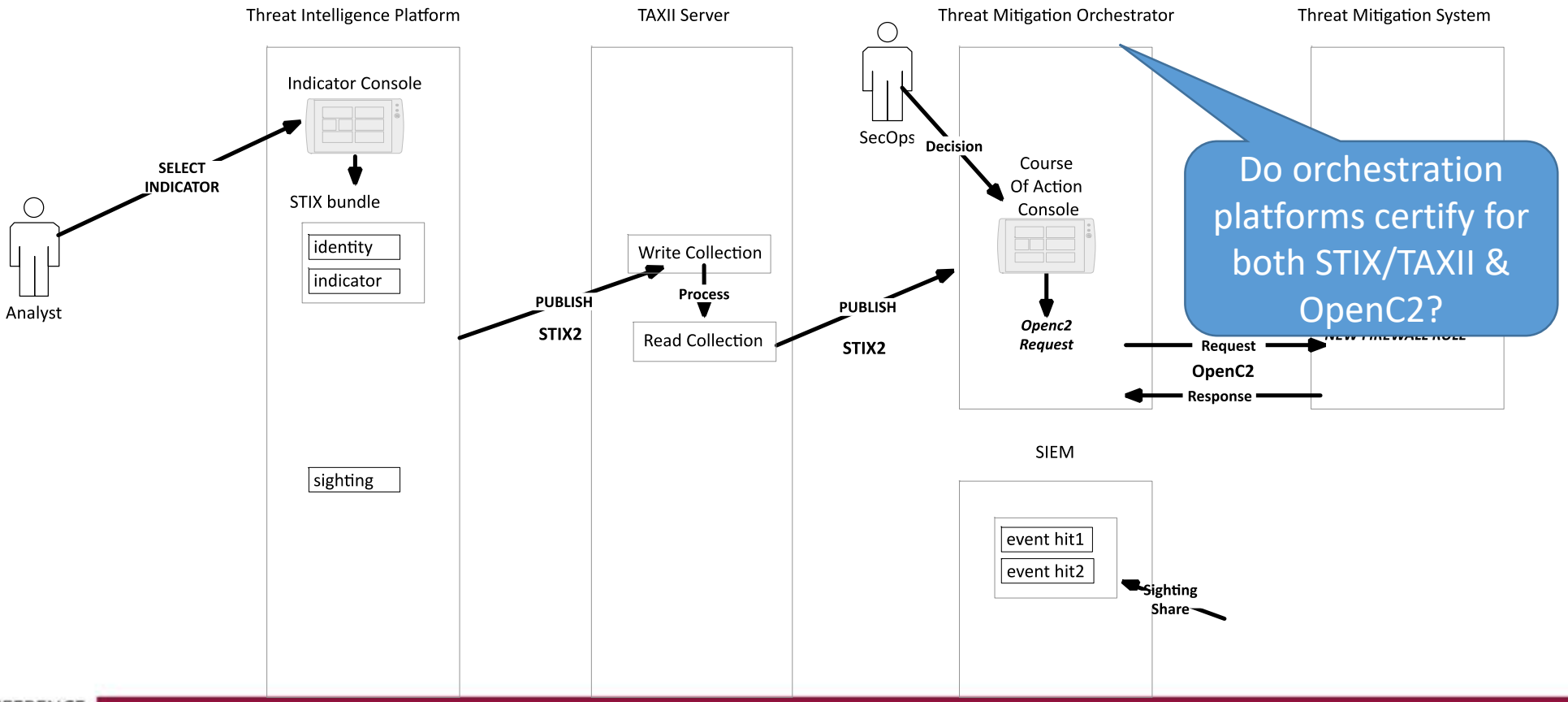
Continuing Challenges with STIX/TAXIIv2 & OpenC2

- **Consistent Operations Model**
  - Lack common mechanisms for identifying sources, versioning and change modifications….etc
  - Operational requirements across technologies supporting both standards



Continuing Challenges with STIX/TAXIIv2 & OpenC2

- **Interoperability Verification**
  - Lack of coordinated interoperability verification
  - A system that does both STIX/TAXII & OpenC2 has no coordinated verification



CTI Interoperability Automation
…a model for future…

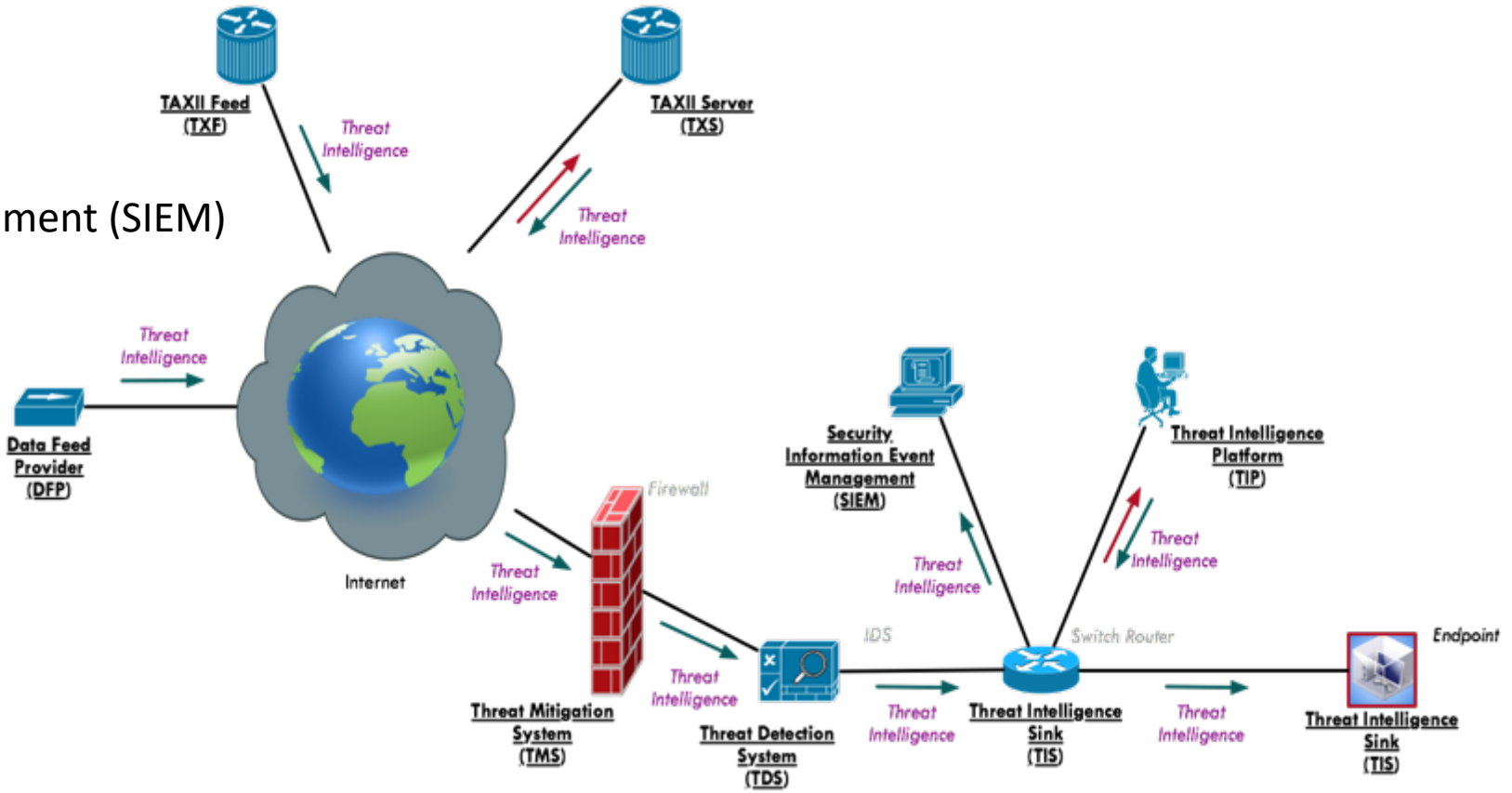
STIXPreferred Certification

- OASIS STIX/TAXII **Version2** Self Certification Program

- Verified capabilities for ***industry selected*** use cases including incident response
- Increase quality and success of CTI ***'Out of the Box'*** Collaboration

STIX TAXII 2 Preferred - Persona

- Data Feed Provider (DFP)
- Threat Intelligence Platform (TIP)
- Security Incident and Event Management (SIEM)
- TAXII Server (TXS)
- TAXII Feed (TXF)
- Threat Mitigation System (TMS)
- Threat Detection System (TDS)
- Threat Intelligence Sink (TIS)



Certification Test Structure

- STIX Sharing (independent of TAXII) Tests – **Part 1 Interoperability**
- STIX over TAXII Sharing - **Part 2 Interoperability**
- Each part defines
  - 1) A set of tests to performed and data
  - 2) A set of expected results & behaviors
  - 3) Checklists define mandatory and optional tests for each persona

Interoperability Certification Part 1 Focus

Description	Producer Personas	Respondent Personas
Indicator Sharing	DFP, TIP	TMS, TIS, TDS, TIP, SIEM
Sightings Sharing	DFP, TIP, TMS, TDS	TIP, SIEM
Versioning	All	All
Data Markings	All	All
Custom Objects & Properties	All	All
Course of Action Sharing	DFP, TIP	TIP, TMS, TIS, TDS

Test Component #1: Data

- A set of tests to performed and data for producer and consumer

To TXS	From TXS

POST /api1/collections/91a7b528-80eb-42ed-a74d-bd5a2116/objects/ HTTP/1.1
Host: 10.1.1.10
Accept: application/vnd.oasis.taxii+json; version=2.0
Authorization: Basic dGVzdDoxMjPCow==
Content-Type: application/vnd.oasis.stix+json; version=2.0
 	
{
"type": "content from test table below...",
}
	HTTP/1.1 202 Accepted
	Content-Type: application/vnd.oasis.taxii+json; version=2.0
	
	{
	"id": "2d086da7-4bdc-4f91-900e-d77486753710",
	"status": "complete",
	"request_timestamp": "2016-11-02T12:34:34.12345Z",
	"total_count": 4,
	"success_count": 4,
	"successes": [
	"List of objects defined in the Part1 bundle test cases"
	],
	"failure_count": 0,
	"pending_count": 0
	}

Test Component #2: Behavior

- A set of expected results & behaviors
  - Goes beyond simple parsing

Setup B Behavior - Read-Write Collection

1. Producer does a get on the Read-Write collection `https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118`
2. Verify at the Producer that the TXS responds with the following information:
   a. **HTTP Response Code** is 200 OK
   b. **id** is `91a7b528-80eb-42ed-a74d-bd5a2118`
   c. **title** is "Read-Write Collection 1"
   d. **description** is "This is Read-Write Collection 1"
   e. **can_read** is true
   f. **can_write** is true
   g. **media_types** is `"application/vnd.oasis.stix+json; version=2.0"`
3. For each section described in Part1: Indicator Sharing Producer Test Cases the Producer will allow an analyst to create an Indicator in the user interface of Producer product and then publish the content to the TXS at `https://10.1.1.10/api1/collections/91a7b528-80eb-42ed-a74d-bd5a2118/objects` where the TXS component will not respond to the post until all objects within the bundle have been processed
4. Verify the TXS accepts the content by verifying the following on the Producer:
   a. **HTTP Response code** is 202 Accepted
   b. **id** represents a unique identifier for each post
   c. **status** is complete
   d. **request_timestamp** represents the time of the post
   e. **total_count** represents the number of objects in the bundle test case
   f. **success_count** is the same as total_count
   g. **successes** is an array of the object identifiers in the submitted bundle and matches the identifiers posted for each indicator
   h. **failure_count** is 0
   i. **pending_count** is 0
5. Verify that the Producer shows that the content shared to the TXS is visually shown to the user that the content was accepted successfully by the TXS.

Test Component #3: Checklists

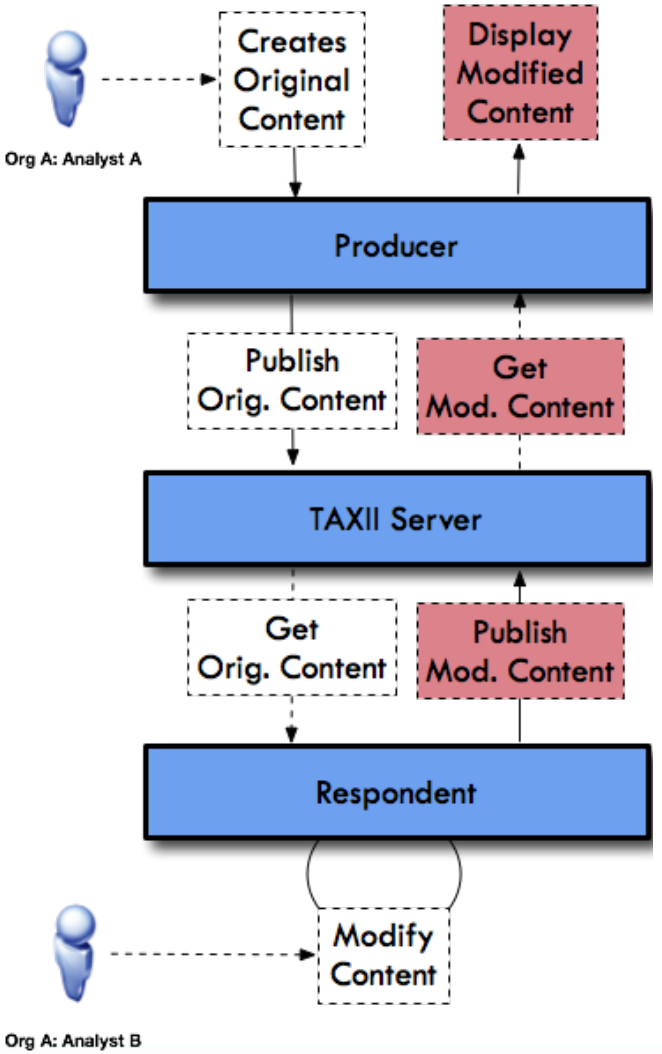
- Checklists define mandatory and optional tests for each persona
  - Ensures consistent capabilities for certified products

Table 3.3.1 - Threat Intelligence Platform (TIP) Part 1 Test Verification List

Use Case	Test	Verification	Results
Indicator Sharing	Indicator IPv4 Address	Mandatory	<fill in>
Indicator Sharing	Indicator IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Two Indicators with IPv4 Address CIDR	Mandatory	<fill in>
Indicator Sharing	Indicator with IPv6 Address	Optional	<if supported, fill in>
Indicator Sharing	Indicator with IPv6 Address CIDR	Optional	<if supported, fill in>
Indicator Sharing	Indicator FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator URL	Mandatory	<fill in>
Indicator Sharing	Indicator URL or FQDN	Mandatory	<fill in>
Indicator Sharing	Indicator File hash with SHA256 or MD5 values	Mandatory	<fill in>
Sighting Sharing	Producer Test Case Data	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv4 Address	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv4 Address Matching CIDR	Mandatory	<fill in>
Sighting Sharing	Sighting + Indicator with IPv6 Address Matching CIDR	Optional	<if supported, fill in>
Sighting Sharing	Sighting + Indicator with NO observed data	Mandatory	<fill in>

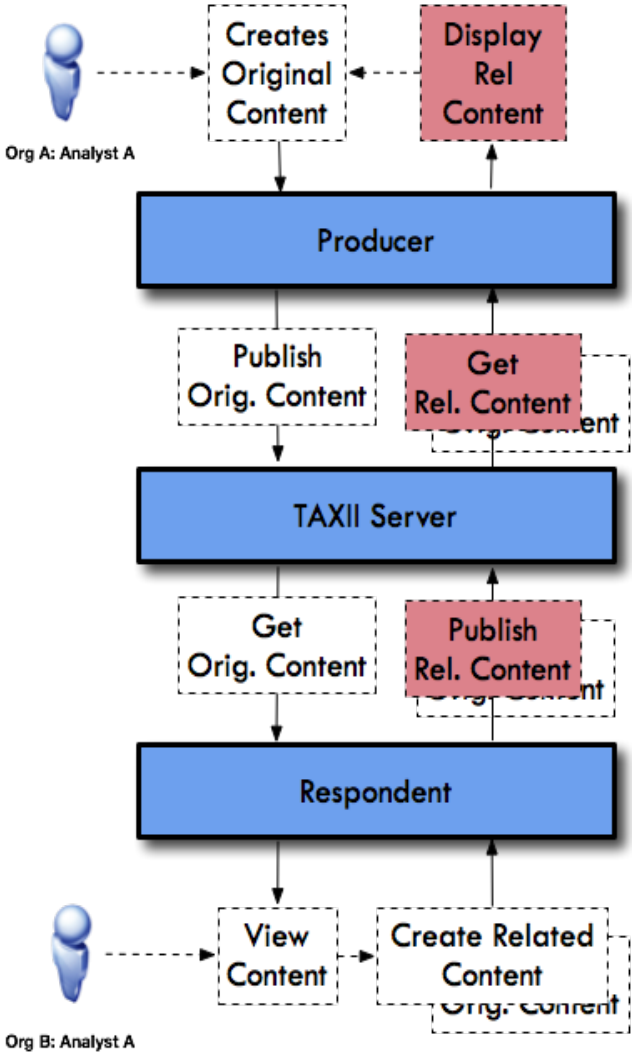
User Focused Verification Example #1

- **Same organization** sharing and modifying **common** intelligence between two analysts using two systems
  - First analyst creates an intelligence element that they wish to share with other analysts within the same organization
  - Second analyst receives the intelligence from the first analyst and then proceeds to modify the existing intelligence and reshares back to the first analyst



User Focused Verification Example #2

- **Different organizations** sharing and modifying **related** intelligence between two analysts using two systems
  - First analyst creates an intelligence element that they wish to share with another set of analysts in a sharing community
    - The other analysts in this sharing community belong to different organizations
  - Second analyst receives the intelligence from the first analyst and then proceeds to find some new content that they believe is related to the original intelligence
    - They proceed to then share the new intelligence back to the sharing community, including the relationship that connects the intelligence together



Interoperability: 4 *Select* Lessons Learned

**** January 2018 STIX/TAXII v2 Plugfest in Utah***

Summary	Issue
Absolute URLs impact cloud deployments	Absolute Taxii URL problem can't be used in certain deployments. Requires specification work to allow either discovery of URL or relative URLs for taxii
Media Types cause implementation ambiguity	Different Media types on different endpoints is confusing and causes problems in implementations Client could put both STIX and TAXII media types in requests accept header
Message limits ambiguity	Messages and how large they could be caused confusion resulting in poor implementation choices
Common practice of tagging not mandatory	Specification ambiguous. Vendor was expecting a mandatory field but it's not included resulting in their product rejecting missing content

3 Lessons To Making Automation Easier…

- Automation projects succeed when sharing a **common objective** across all aspects

- **Leverage standards-based** security technologies whenever possible:
  - STIXPreferred Persona Certification
  - OpenC2 Actuator Profiles

- **Verify and fail-fast**

Learn More...

- ...on standards: **OASIS**
  - Membership https://www.oasis-open.org/
  - Events https://www.oasis-open.org/events/calendar

- ...on CTI Interoperability: **STIX/TAXIIv2 Interoperability Subcommittee**
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-interoperability

- ...on CTI: **STIX/TAXII Technical Committee**
  - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

- …on OpenC2: **Technical Committee**
  - https://www.oasis-open.org/apps/org/workgroup/openc2/

Questions?

@LG_Cyber

www.LookingGlassCyber.com

FIRST
Improving Security Together

LOOKINGGLASS