CTI Automation is harder than it needs to be...

Allan Thomson, LookingGlass Cyber Solutions CTO
Co-Chair OASIS CTI Interoperability
June 2018
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

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

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

Result: Failed to debug problem, both vendors support & engineering teams involved
Fortune 500 Enterprise Challenges

Heterogenous Integration Points

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

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

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
Continuing Challenges with STIX/TAXIIv2 & OpenC2

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

Does the TMS have sufficient and standard data context from STIX2 to detect advanced threats?

What data and format does Orchestration team require?

Can SIEM convert logs to sightings? What scale?

Does the analyst team understand where sightings come from?
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

Are all systems designed to integrate?

Are all user roles and their use cases understood?
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

Does OpenC2 have standard mapping from STIX2?
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

Do orchestration platforms certify for both STIX/TAXII & OpenC2?
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

<table>
<thead>
<tr>
<th>Description</th>
<th>Producer Personas</th>
<th>Respondent Personas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator Sharing</td>
<td>DFP, TIP</td>
<td>TMS, TIS, TDS, TIP, SIEM</td>
</tr>
<tr>
<td>Sightings Sharing</td>
<td>DFP, TIP, TMS, TDS</td>
<td>TIP, SIEM</td>
</tr>
<tr>
<td>Versioning</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Data Markings</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Custom Objects &amp; Properties</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Course of Action Sharing</td>
<td>DFP, TIP</td>
<td>TIP, TMS, TIS, TDS</td>
</tr>
</tbody>
</table>
Test Component #1: Data

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

<table>
<thead>
<tr>
<th>To TXS</th>
<th>From TXS</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST /api1/collections/91a7b528-80eb-42ed-a74d-bd5a2116/objects/ HTTP/1.1</td>
<td>HTTP/1.1 202 Accepted</td>
</tr>
<tr>
<td>Host: 10.1.1.10</td>
<td>Content-Type: application/vnd.oasis.taxii+json; version=2.0</td>
</tr>
<tr>
<td>Accept: application/vnd.oasis.taxii+json; version=2.0</td>
<td>&quot;id&quot;: &quot;2d086da7-4bdc-4f91-900e-d77486753710&quot;,</td>
</tr>
<tr>
<td>Authorization: Basic dGVzdDoxMjIC==</td>
<td>&quot;status&quot;: &quot;complete&quot;,</td>
</tr>
<tr>
<td>Content-Type: application/vnd.oasis.stix+json; version=2.0</td>
<td>&quot;request_timestamp&quot;: &quot;2016-11-02T12:34:34.12345Z&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;total_count&quot;: 4,</td>
</tr>
<tr>
<td></td>
<td>&quot;success_count&quot;: 4,</td>
</tr>
<tr>
<td></td>
<td>&quot;successes&quot;: [</td>
</tr>
<tr>
<td></td>
<td>&quot;List of objects defined in the Part1 bundle test cases&quot;</td>
</tr>
<tr>
<td></td>
<td>}, &quot;Failure_count&quot;: 0,</td>
</tr>
<tr>
<td></td>
<td>&quot;pending_count&quot;: 0</td>
</tr>
</tbody>
</table>
Test Component #2: Behavior

• A set of expected results & behaviors

• Goes beyond simple parsing
Test Component #3: Checklists

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

<table>
<thead>
<tr>
<th>Summary</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute URLs impact cloud deployments</td>
<td>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</td>
</tr>
</tbody>
</table>
| 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

• ...on CTI: STIX/TAXII Technical Committee

• ...on OpenC2: Technical Committee
Questions?

@LG_Cyber
www.LookingGlassCyber.com