CTI Interoperability

Tampa Onsite 2015

What Should We Do?

- Verify CTI Standard Implementations? (act as a certification body)
- Create a Process for Validation?
- Drive Mature Use of Standards?
- How Far (Deep) Do We Go?

A Basic Model

STIX

5 – Report

4 – Actor, Campaign

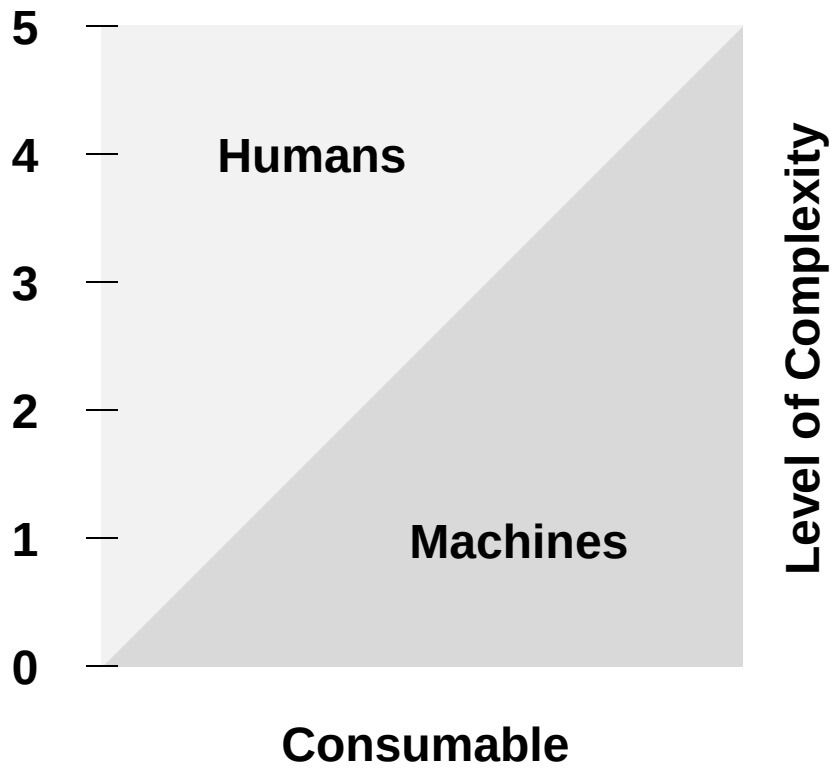
3 – TTP, Incident

2 – CoA, Exploit Target

1 – Observables, Indicators

0 – Connection

TAXII



Process Levels/ Definitions

- TAXII – Connection & Transport
- STIX – Data Validation
- STIX – Data Understanding

Implementation Review Results

- OASIS CTI Members Review
- Will Replace the Mitre Support Page

STIX & TAXII Security Standards Integration						
Company Name	Company Interoperability Contact	Service / Product Name(s)	Product Version Tested	Date Tested	CTI Testing Organization #1	CTI Testing Organization #2

STIX & TAXII Security Standards Integration							
Service / Product Name(s)	TAXII				STIX		
	TAXII Version(s)	Feed Pull "Ingests"	Feed Publish "Shares Out"	Inbox "Shares Back"	STIX Version(s)	STIX Validation	High Level Objects Supported Observable, Indicator, Exploit Target, Incident, Courses of Action, Campaign, TTP, Threat Actor
Communities							
Intelligence Providers							
Secuity Tools							

Moving Forward

- TAXII – Connection & Transport
  - Discovery
  - Query
  - Channels
- STIX – Data Understanding
  - Full STIX Profiles
  - Additional Controlled Vocabularies
- Define Product Genres
  - TIPs, SIEMs, Network, End Point, etc.
  - Drives Implementation Maturity