RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking

SESSION ID: PST-W08

Cyber Threat Intelligence Sharing Standards

Jerome Athias

Cybersecurity Specialist
Saudi Aramco
@JA25000

Agenda

- Cyber Threat Intelligence (CTI)
- CTI Sharing Standards
- Summary & Apply
- Q&A

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Cyber Threat Intelligence (CTI)

#RSAC

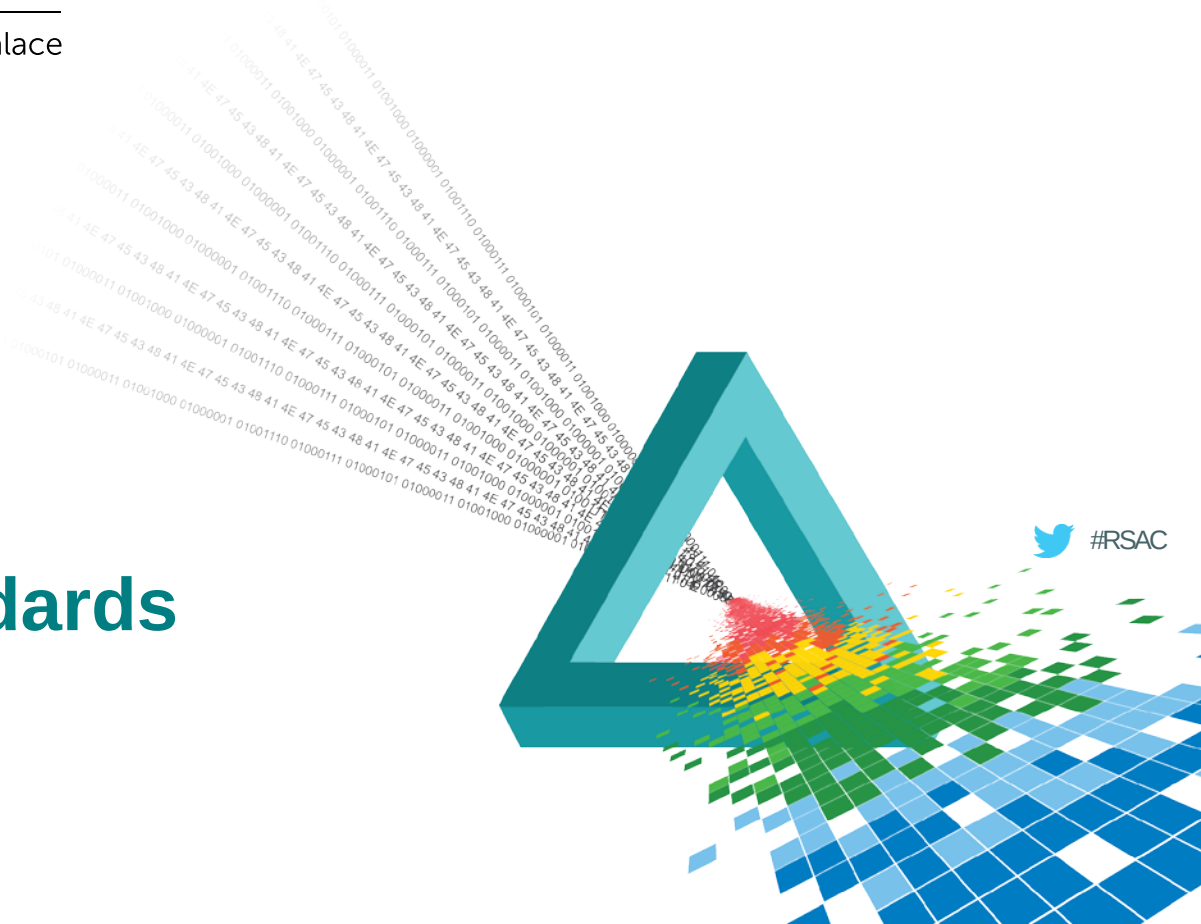
Cyber Threat Intelligence (CTI)

- What is CTI?
  - Definition(s) of this Capability
- Why is it useful?
  - Identify, Protect, Detect, Respond, Recover. *More and faster*
  - Situational Awareness, Know your enemy, be proactive (Observe, Learn, Prioritize, Adapt, Adjust, Defend, *React*, Prevent, Track, Disrupt, Deter…)
  - Interoperability (Common Language)
  - Automation (M2M)
  - Actionable (data-driven decisions, visualization, COAs)

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CTI Sharing Standards



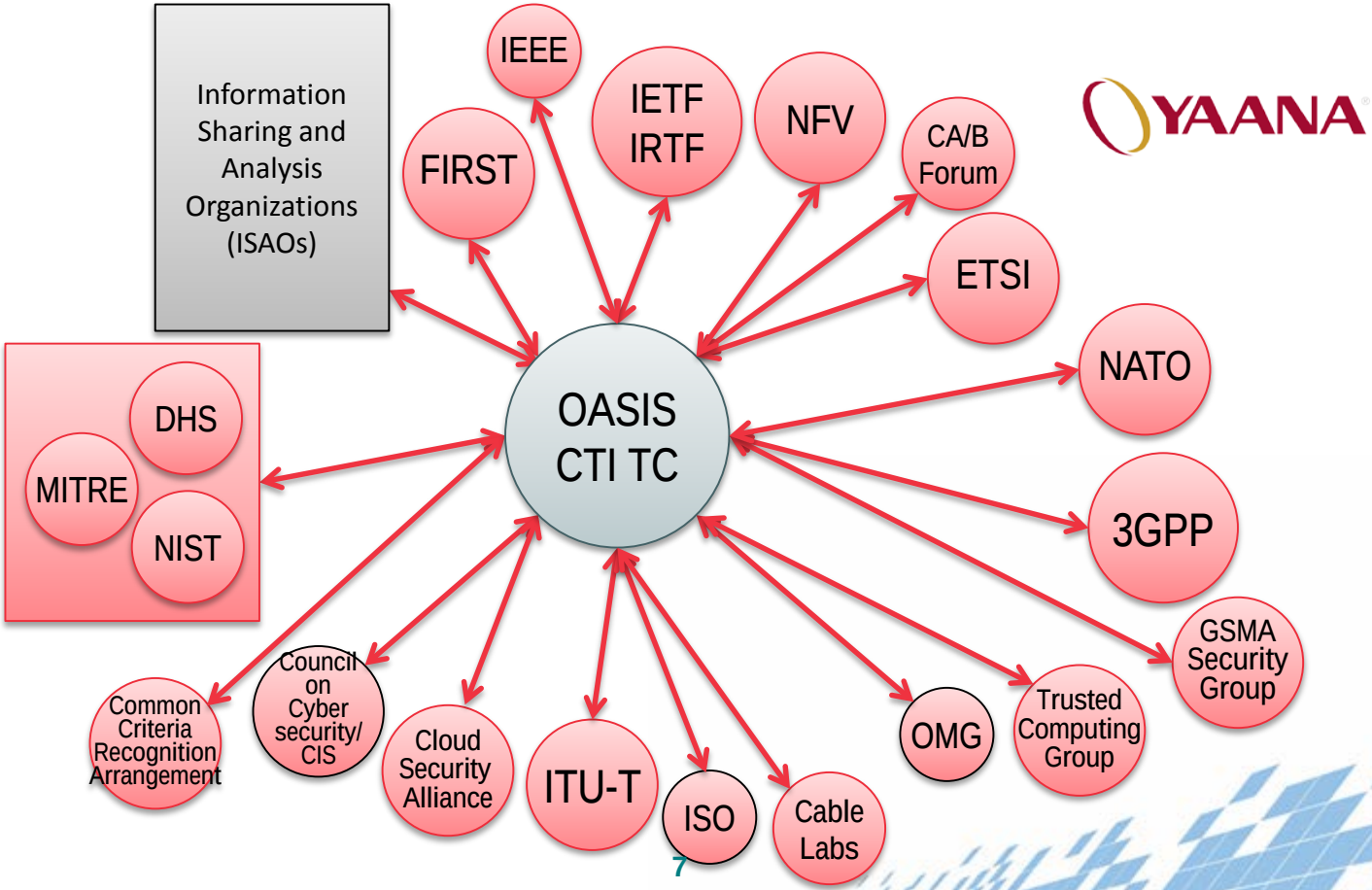
CTI Sharing Standards

- Why?

“Information is a source of learning. But unless it is organized, processed, and available to the right people in a format for decision making, it is a burden, not a benefit.” William Pollard

- Where? Who?
  - Internal/External
  - Continuous Monitoring, Fast Incident Prevention and Response
  - CERTs, CSIRTs, SOCs, Threat Forensic Malware Analysts, etc.
- What?
  - Information Model, Data Model from community-driven initiatives
- How?
  - Commonly XML schemas, language, protocols, tools

CTI ecosystem

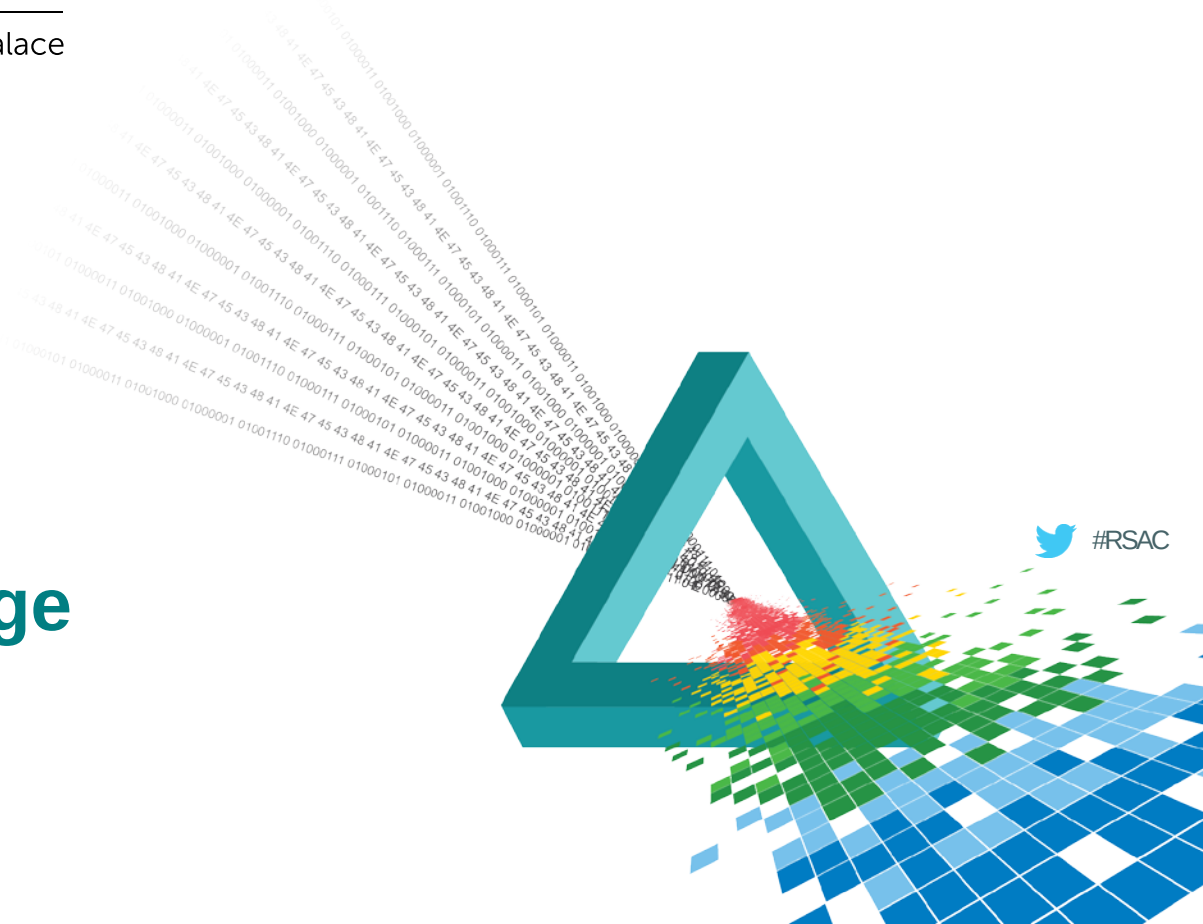


CTI Sharing Standards

- To name a few
  - OpenIOC, Mandiant
  - VERIS, Verizon
  - IODEF, IETF
  - DFXML WG, NIST - DFAX
  - OASIS-CTI (DHS) (CybOX, STIX, TAXII, MAEC, …)
- Support and leverage well-known frameworks and standards (and tools)
  - LM Kill Chain, Diamond Model, OODA loop
  - TLP
  - CVE, CAPEC, CPE, OVAL, CIQ…
  - SNORT, YARA

RSAConference2015

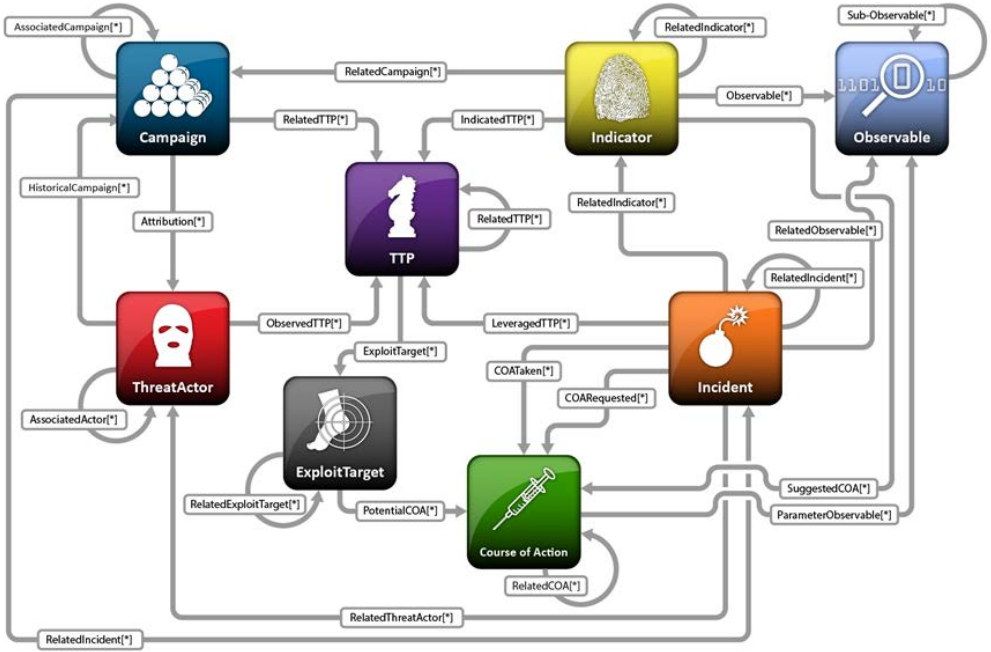
Abu Dhabi | 4–5 November | Emirates Palace



Common Language

Common Concepts

https://stixproject.github.io/documentation/



STIX™ Architecture

Contextual relationships

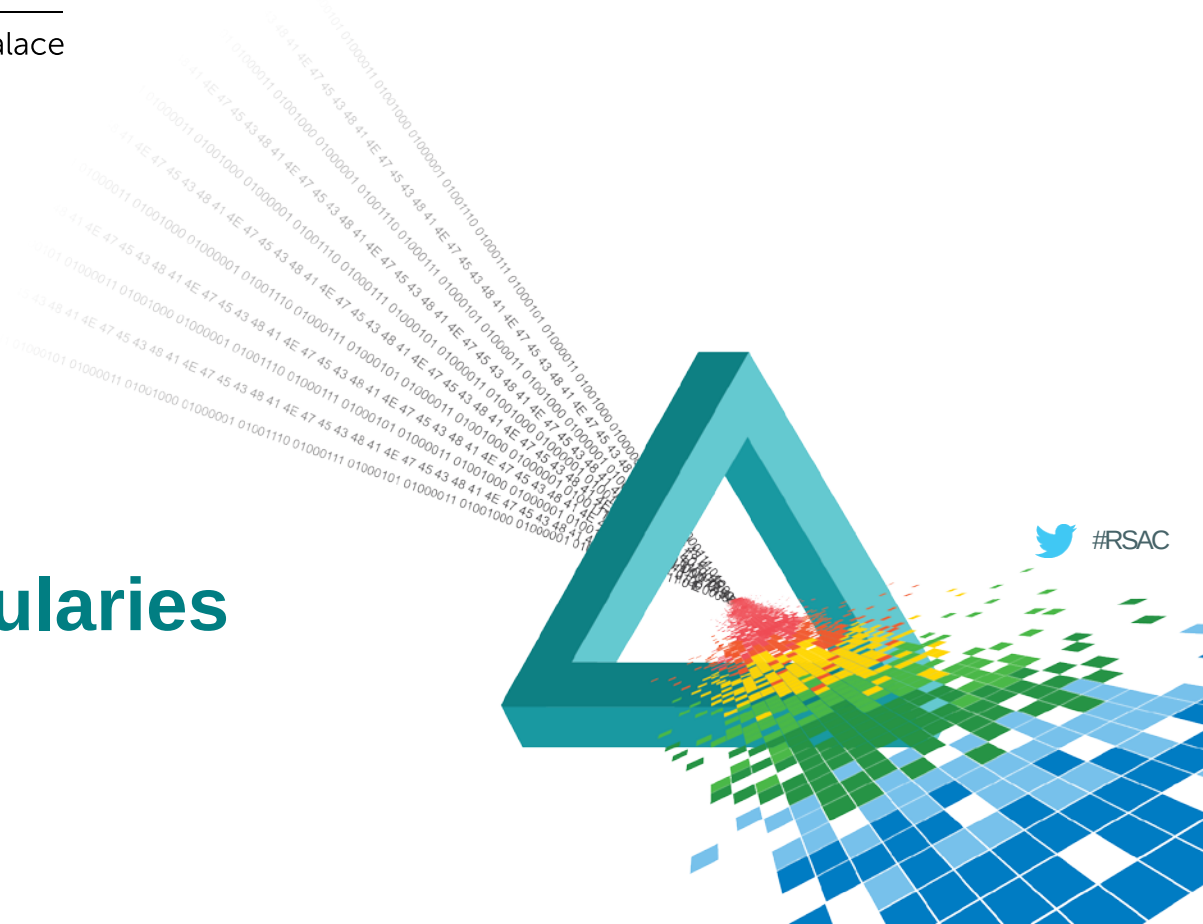
Fictitious Example

- **Incident**: Rogue AP at RSA Conference 2015 Abu Dhabi
- **ExploitTarget**: RSA Conference's attendees
- **TTP**: Rogue Wi-Fi Access Point, MITM tools, answers to any ESSID
- **Threat Actor**: The French Fries Gang
- **Threat Campaign**: Wi-Fi hijacking over the world
- **Indicator**: Too nice to be true Wi-Fi AP name
- **Observables**: ssid="FreeWifiRSA", spoofed DNS queries
- **COAs**: Training, Monitoring, Eradication, Public Disclosure

Other Examples

- Victim Targeting by Sector, for a Campaign
- Assets Affected in an Incident
- Incident Essentials - Who, What, When
- Vulnerability (CVE) in an Exploit Target
- Malicious E-mail Indicator With Attachment
- Malware: File Hash Reputation, Characterization using MAEC
- Command and Control IP List
- Course of Action to Block Network Traffic

Controlled Vocabularies



Controlled Vocabularies

STIX™ IncidentEffect

- Brand or Image Degradation
- Data Breach or Compromise
- Degradation of Service
- Destruction
- Financial Loss
- …

IODEFv2 business impact

- Degraded-reputation
- Breach-*
- Loss-of-service
- Asset-damage
- Theft-financial
- …

STIX™ Default Vocabularies (overview)

Threat Information

Management

Controlled Vocabulary

STIX™ Threat Actor Type

- Cyber Espionage Operations
- Hacker
- Hacktivist
- State Actor / Agency
- Insider Threat
- Disgruntled Customer / User
- eCrime Actor - Credential Theft
- eCrime Actor - Malware Developer
- eCrime Actor - Organized Crime Actor
- eCrime Actor - Spam Service
- eCrime Actor - Traffic Service

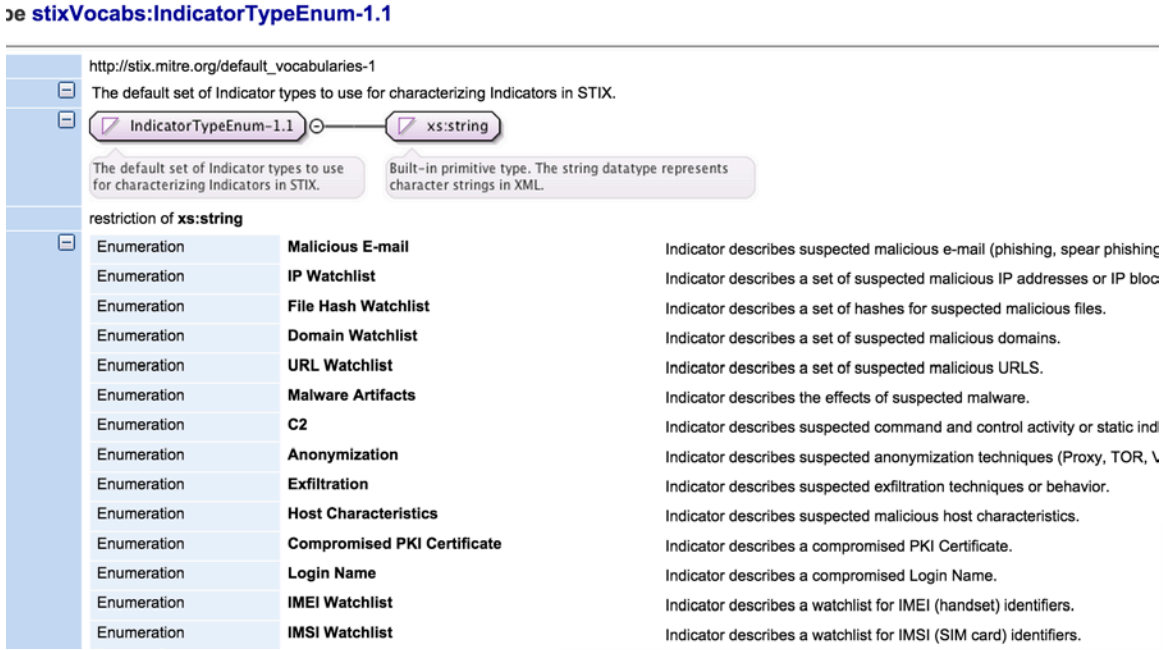
Controlled Vocabulary

STIX™ Motivation

- Ego
- Financial or Economic
- Military
- Opportunistic
- Political
- Ideological…

IncidentCategory

- Unauthorized Access
- Improper Usage
- Denial of Service
- Malicious Code
- Scans/Probes/Attempted Access
- Exercise/Network Defense Testing



pe **stixVocabs:IndicatorTypeEnum-1.1**

http://stix.mitre.org/default_vocabularies-1

The default set of Indicator types to use for characterizing Indicators in STIX.

IndicatorTypeEnum-1.1 — xs:string

The default set of Indicator types to use for characterizing Indicators in STIX.

Built-in primitive type. The string datatype represents character strings in XML.

restriction of **xs:string**

Enumeration	**Malicious E-mail**	Indicator describes suspected malicious e-mail (phishing, spear phishing
Enumeration	**IP Watchlist**	Indicator describes a set of suspected malicious IP addresses or IP bloc
Enumeration	**File Hash Watchlist**	Indicator describes a set of hashes for suspected malicious files.
Enumeration	**Domain Watchlist**	Indicator describes a set of suspected malicious domains.
Enumeration	**URL Watchlist**	Indicator describes a set of suspected malicious URLS.
Enumeration	**Malware Artifacts**	Indicator describes the effects of suspected malware.
Enumeration	**C2**	Indicator describes suspected command and control activity or static ind
Enumeration	**Anonymization**	Indicator describes suspected anonymization techniques (Proxy, TOR, V
Enumeration	**Exfiltration**	Indicator describes suspected exfiltration techniques or behavior.
Enumeration	**Host Characteristics**	Indicator describes suspected malicious host characteristics.
Enumeration	**Compromised PKI Certificate**	Indicator describes a compromised PKI Certificate.
Enumeration	**Login Name**	Indicator describes a compromised Login Name.
Enumeration	**IMEI Watchlist**	Indicator describes a watchlist for IMEI (handset) identifiers.
Enumeration	**IMSI Watchlist**	Indicator describes a watchlist for IMSI (SIM card) identifiers.

Controlled Vocabularies

Ex: types of indicators (IOCs) in STIX™

Observables

CybOX Objects

Network

- Address
- Domain Name
- Hostname
- URI
- Email Message, SMS
- Network Connection, Packet…

System

- Account
- File Unix/Win (PDF, Exe, X509…)
- Process
- Win Service
- Win Registry Key
- Device, Disk, Memory…

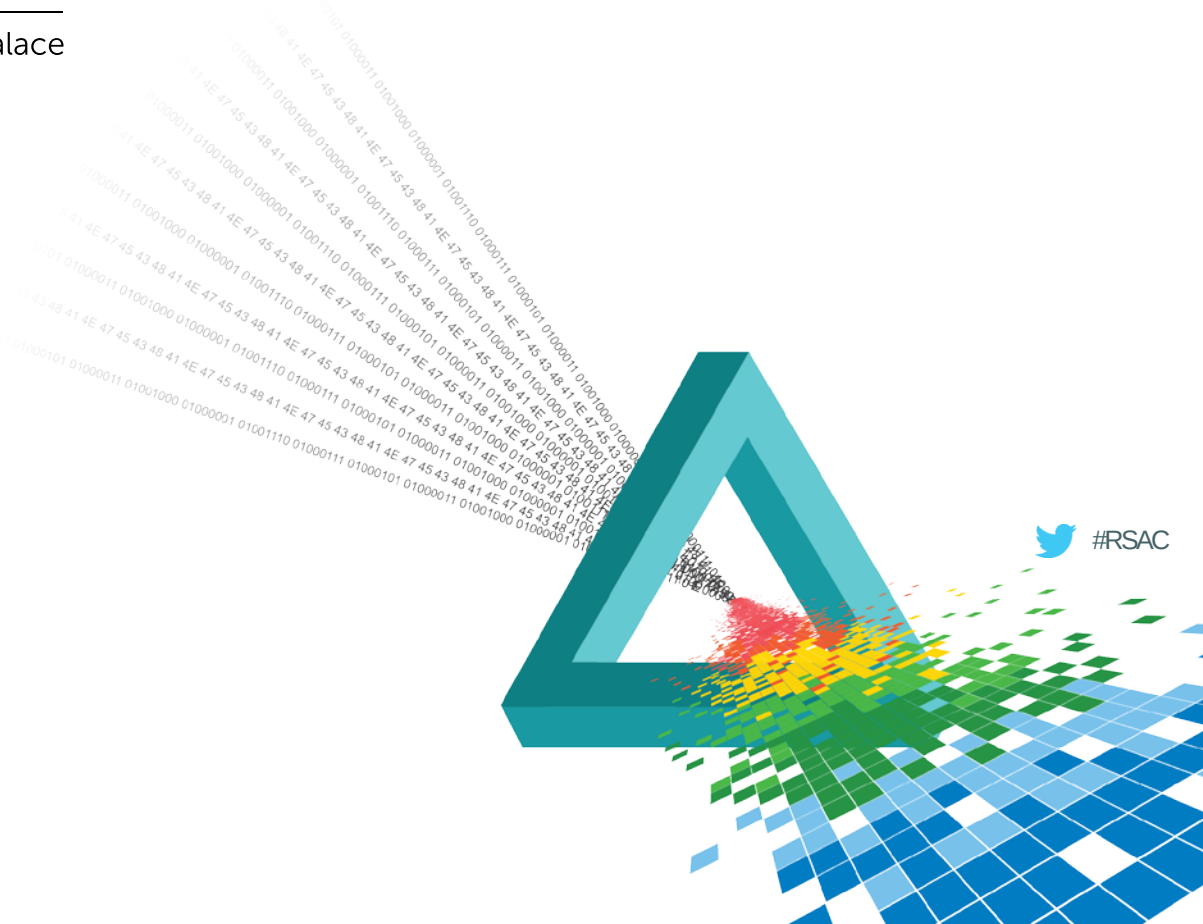
Name	Inverse	Applicable Objects (Source)	Applicable Objects (Related)
Created	Deleted, Killed	Archive File, Process	File, Process, Mutex, Win Registry Key, Win Service, Win Thread
Created_By	Deleted_By, Killed_By	File, Process, Mutex, Win Registry Key, Win Service, Win Thread	Archive File, Process
Deleted	Created	Process	File, Mutex, Win Registry Key, Win Service
Deleted_By	Created_By	File, Mutex, Win Registry Key, Win Service	Process
Modified_Properties_Of	n/a	Process	File, Win Registry Key, Win Service
Properties_Modified_By	n/a	File, Win Registry Key, Win Service	Process
Downloaded_From	n/a	File	URI, Domain Name, Address, Hostname
Downloaded_To	Uploaded_To	URI, File	File
Downloaded	Uploaded	Process	File
Downloaded_By	Uploaded_By	File	Process
Uploaded	Downloaded	Process	File
Uploaded_By	Downloaded_By	File	Process
Uploaded_To	Downloaded_To	File	URI, Domain Name, Address, Hostname

CybOX™ Objects Relationships

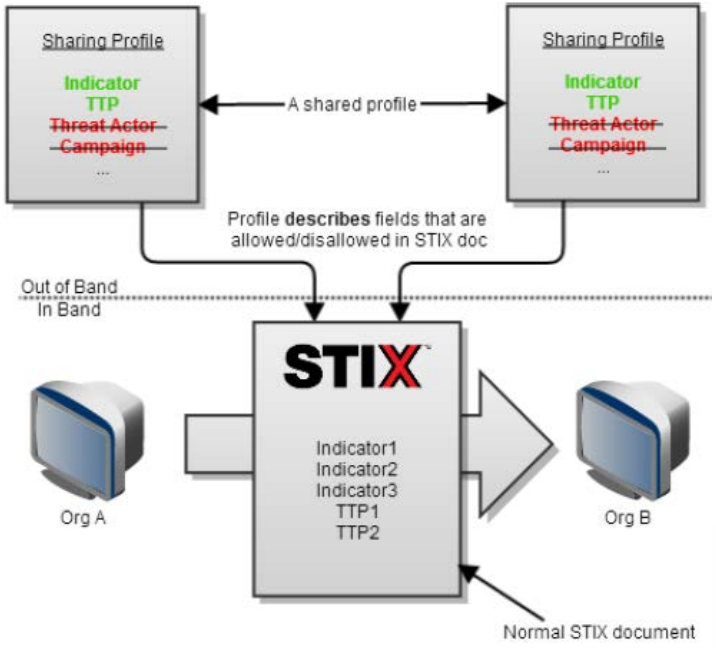
https://cyboxproject.github.io/documentation/object-relationships/

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace



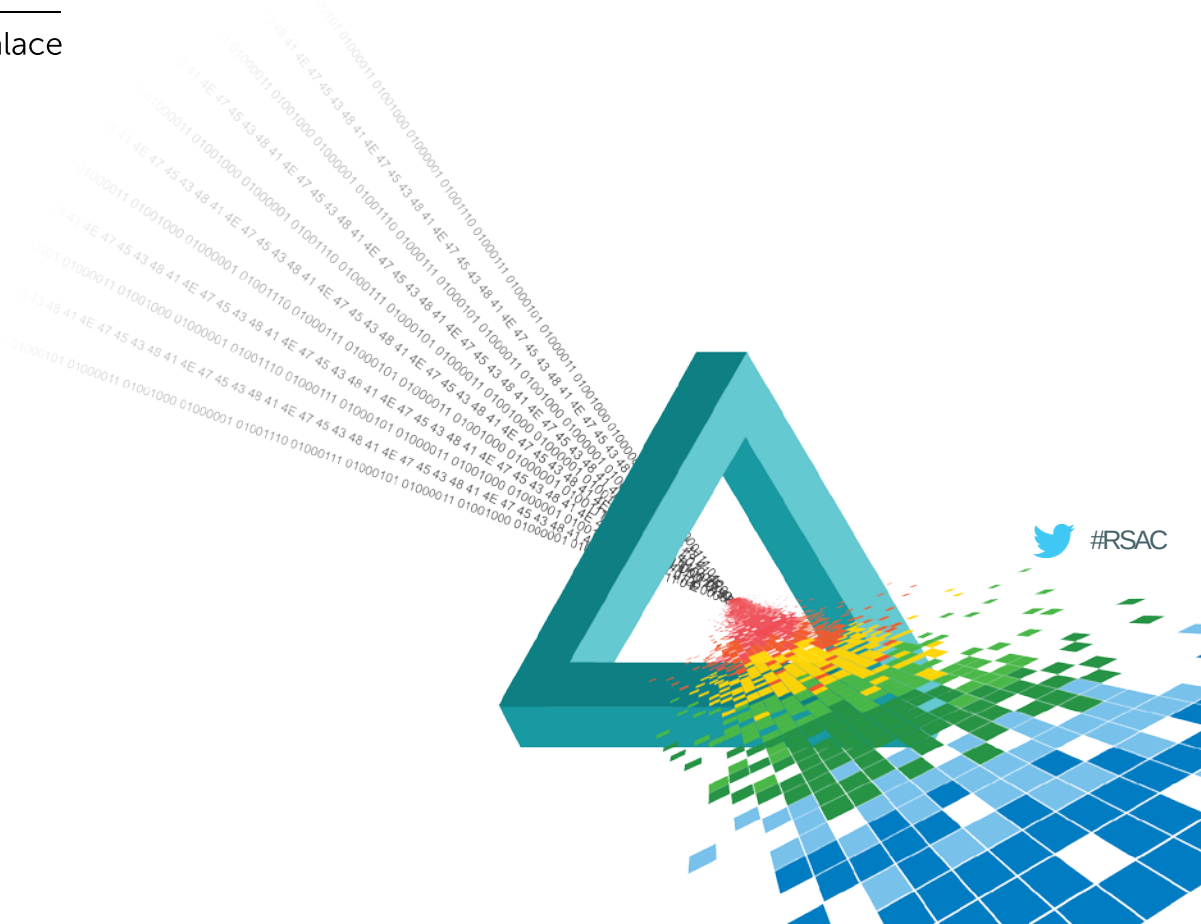
Profiles



STIX™ Profiles, Workflow

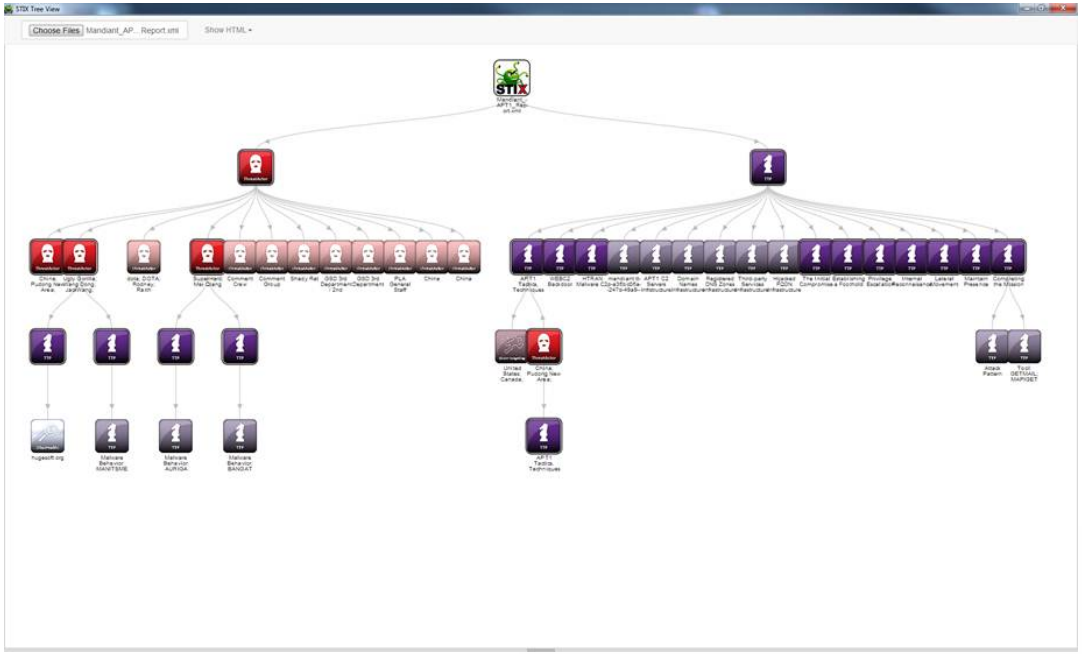
https://stixproject.github.io/documentation/profiles/

Tools



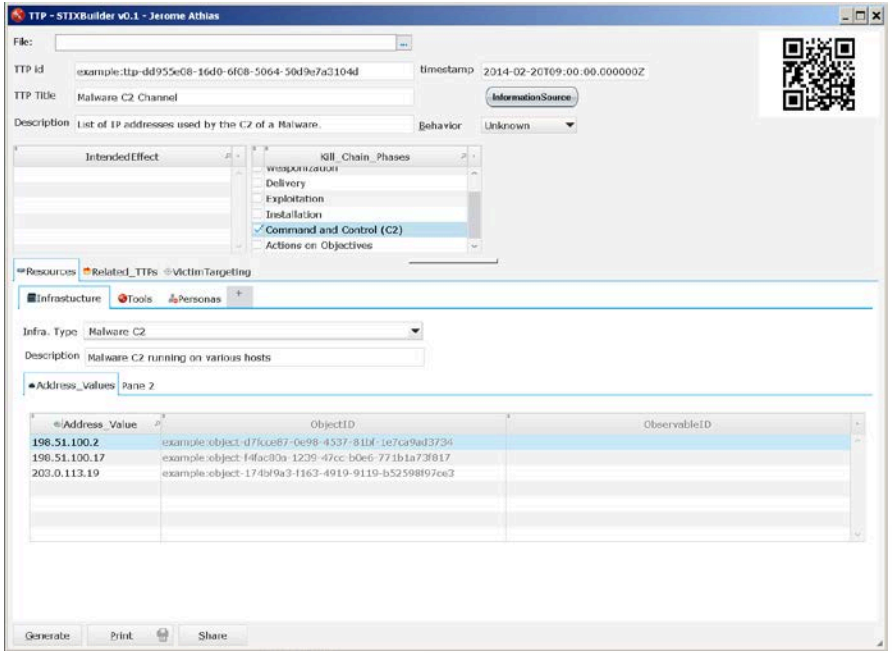
Tools

- APIs, Bindings: Python-stix, Java-stix
- Stix-validator
- Openioc2stix
- Stix2html
- STIX Generator
- STIXViz
- TAXII™: lib-taxii, java-taxii, YETI…



MITRE STIXViz

https://github.com/STIXProject/stix-viz



STIX Builder

http://xorcism.org

Apply CTI

- Foundation (month 1-6)
  - Identify needs, knowledge gaps. Threat Intelligence Lifecycle
  - Identify resources
  - Collect and analyze data. (asset-, adversary-, technology- centric approaches)
- Training and Framework (month 6-12)
  - Strategy (e.g. internal/external sharing, human/machine)
  - Consult experts
- Mature and Automate
  - Collaborate
  - CTI Platform and Processes

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Thank you
Q&A