STIX™

Structured Threat Information eXpression

Sean Barnum

October 2012

MITRE

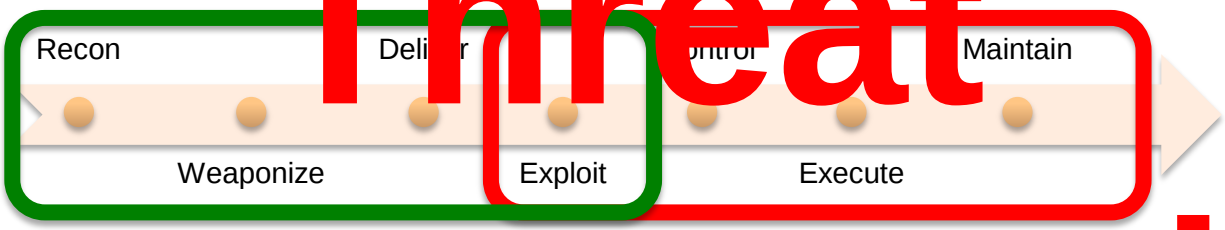
© 2012 The MITRE Corporation. All rights reserved.

Diverse and evolving threats

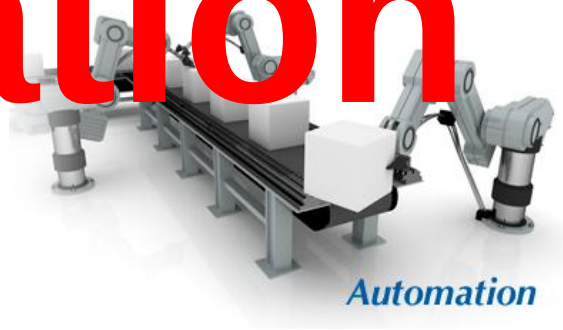
Balance inward & outward focus

Standardized Threat Representation

Proactive & reactive actions



Information sharing



Need for holistic threat intelligence

MITRE

© 2012 The MITRE Corporation. All rights reserved.

Information Sharing

Cyber threat information (particularly indicators) sharing is not new

Typically very atomic and very limited in sophistication.

IP lists, File hashes, URLs, email addresses, etc.

Most indicator sharing is human-to-human exchanges of unstructured descriptions of potential indicators

Often conducted via web-based portals or encrypted email.

A more recent trend is the machine-to-machine transfer of relatively simple sets of indicator data

STIX aims to extend indicator sharing to enable management and exchange of significantly more expressive sets of indicators as well as other full-spectrum cyber threat information.

MITRE

© 2012 The MITRE Corporation. All rights reserved.

Evolution of Standardized Representations for Threat

Vulnerabilities

Weaknesses

Attack Patterns

Malware Behavior

Cyber Observables

Based on ←

? **Threat Indicators** →

IDXWG community of Threat Intel and Incident Response experts begins working on defining a standard representation for cyber threat indicators

What is an Indicator?

Community iterated on scope

Defined Indicator scope as a part of broader cyber threat information architecture

Structured threat information architecture evolved into STIX

MITRE

© 2012 The MITRE Corporation. All rights reserved.

What is STIX?

Language

Specify **Capture** **Characterize** **Communicate**

Cyber Threat Information

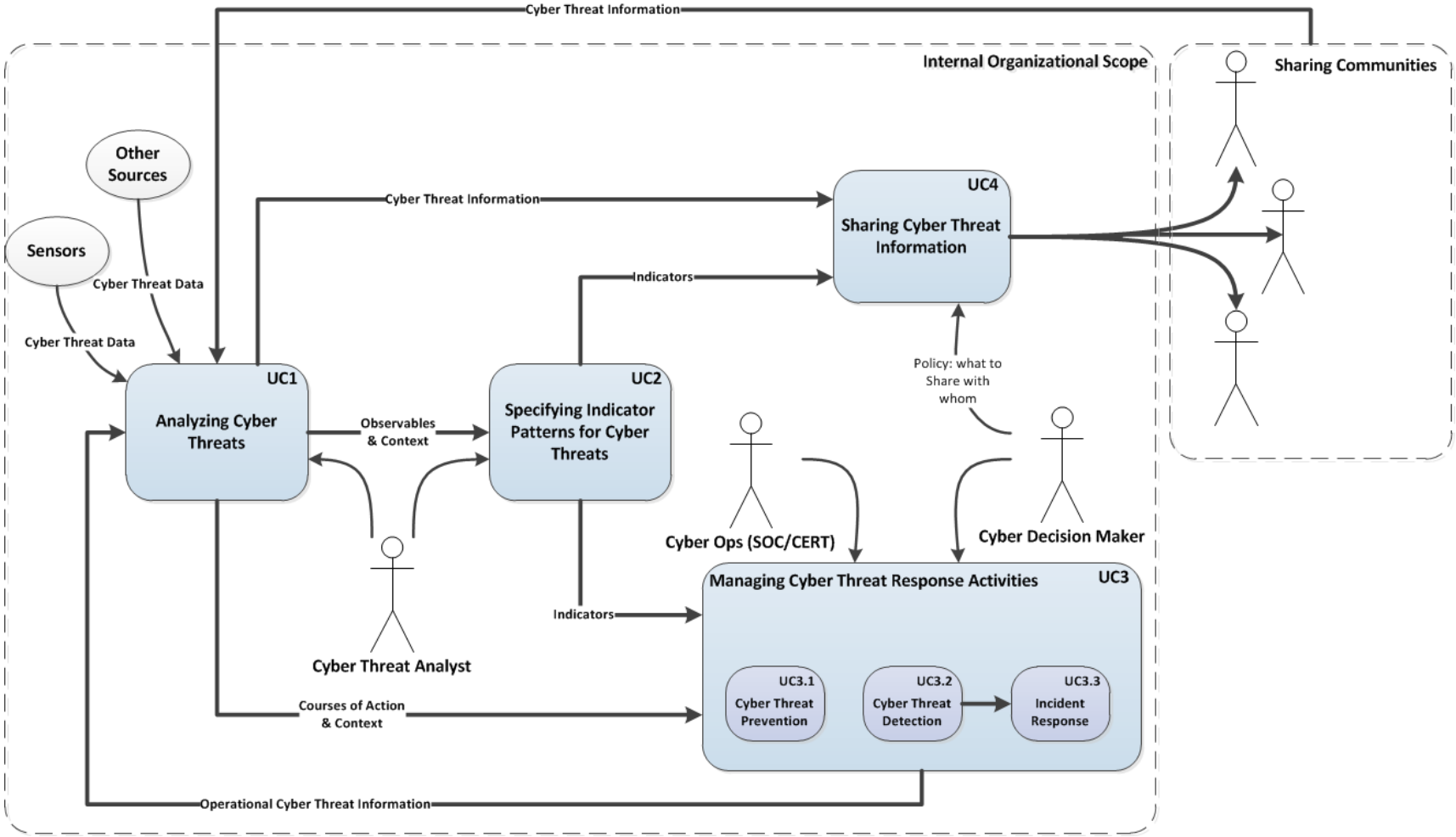
Community-driven

Consistency **Clarity** **Support automation**

MITRE

© 2012 The MITRE Corporation. All rights reserved.

STIX Use Cases



- **STIX provides a common mechanism for addressing structured cyber threat information across and among this full range of use cases improving consistency, efficiency, interoperability, and overall situational awareness.**

MITRE

© 2012 The MITRE Corporation. All rights reserved.

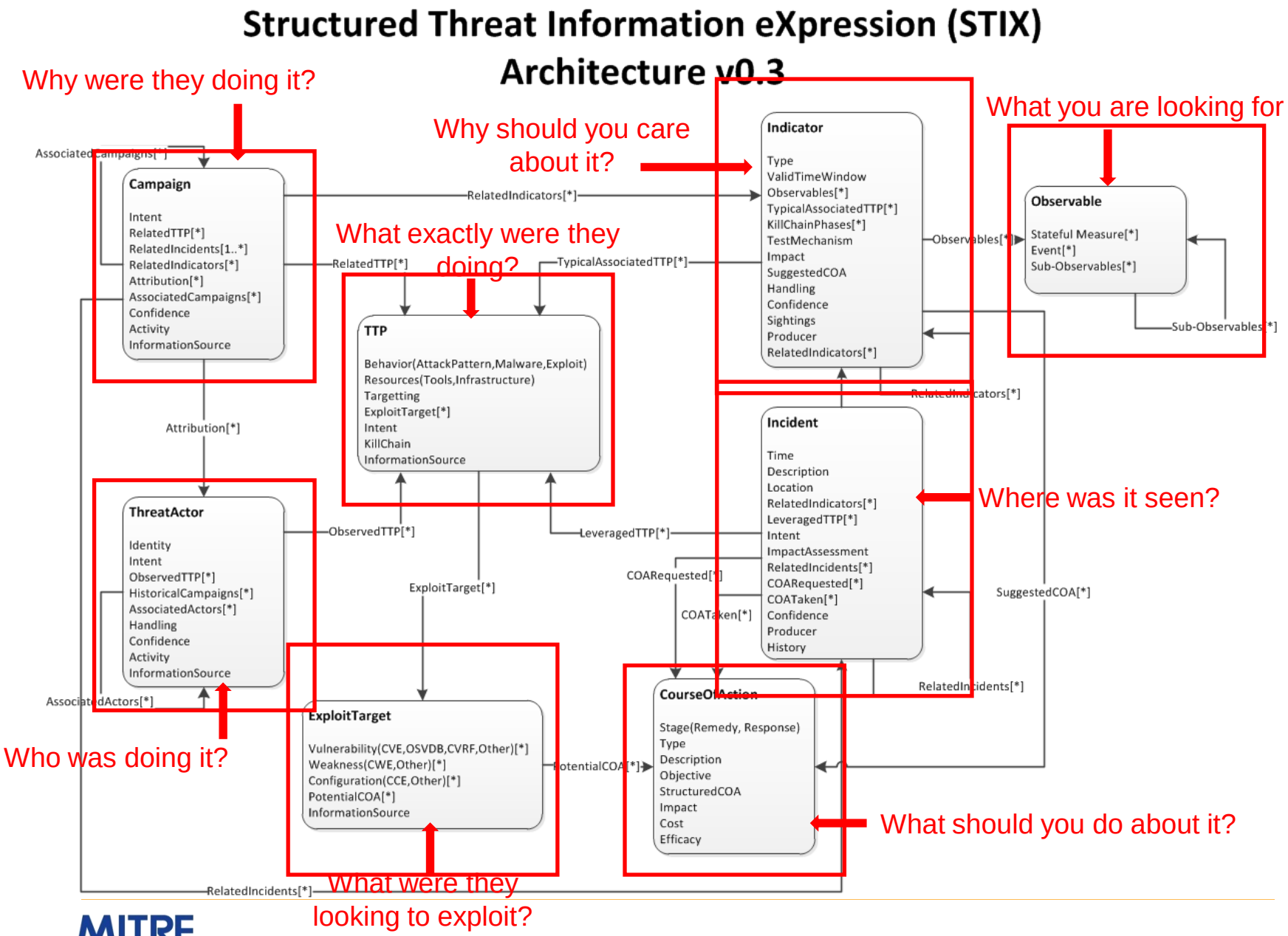
STIX Guiding Principles

- Expressivity
- Integrate rather than Duplicate
- Flexibility
- Extensibility
- Automatability
- Readability

MITRE

© 2012 The MITRE Corporation. All rights reserved.

STIX Architecture



MITRE

© 2012 The MITRE Corporation. All rights reserved.

Implementations

- Initial implementation has been done in XML Schema
  - ubiquitous, portable and structured
- Concrete strawman for community of experts
- Practical structure for early real-world prototyping and POC implementations
- Plan to iterate and refine with real-world use
- Once stable it will be abstracted into an implementation-independent specification.
  - Support other implementations such as semantic web (RDF/OWL), JSON-centric, protobuf, etc.

© 2012 The MITRE Corporation. All rights reserved.

Utilities

- CybOX Resources (released under New BSD license): GitHub site
  - Snort -> CybOX
  - OpenIOC -> CybOX and CybOX -> OpenIOC
  - CybOX -> OVAL
  - Full set of Python bindings for CybOX
  - Email -> CybOX parsing tool
  - CybOX Comparator Script (Python)
- MAEC Resources (released under New BSD license): GitHub site
  - Full set of Python bindings for MAEC
  - Anubis → MAEC Translator (Python)
  - ThreatExpert → MAEC Translator (Python)
  - MAEC → OVAL Translator (Python)
  - MAEC → HTML Transform (XSL)
  - MAEC Comparator Script (Python)
- STIX Resources (Coming Soon)
  - Full set of Python bindings for STIX
  - Suspicious email -> STIX tooling extensions
  - Etc.

© 2012 The MITRE Corporation. All rights reserved.

Adoption & Usage

Still early and immature but already generating extensive interest and initial operational use

- Being investigated/considered by several public/public, public/private and private/private information sharing communities
- Active interest from several large “user” organizations
- Active interest from some service/product vendors

© 2012 The MITRE Corporation. All rights reserved.

A sampling of some of the organizations contributing to the STIX conversation includes:

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

NCI Security LLC

Booz | Allen | Hamilton

© 2012 The MITRE Corporation. All rights reserved.

STIX Community Discussion and Collaboration

- **Currently IDXWG email list**
- **New STIX Community: Discussion List**
  - **Request to join: http://stix.mitre.org/community/registration.html**
  - **Archives will be available**
- **MITRE hosts a social networking collaboration environment: https://handshake.mitre.org**
- **Supplement to mailing list to facilitate collaborative development**

© 2012 The MITRE Corporation. All rights reserved.

Orient on the Adversary!

We want you to be part of the conversation.

stix@mitre.org

https://stix.mitre.org

STIX™
Structured Threat Information eXpression

MITRE

© 2012 The MITRE Corporation. All rights reserved.