Cyber Threat Intelligence with the Structured Threat Information eXpression (STIX)

Sean Barnum

July 2012

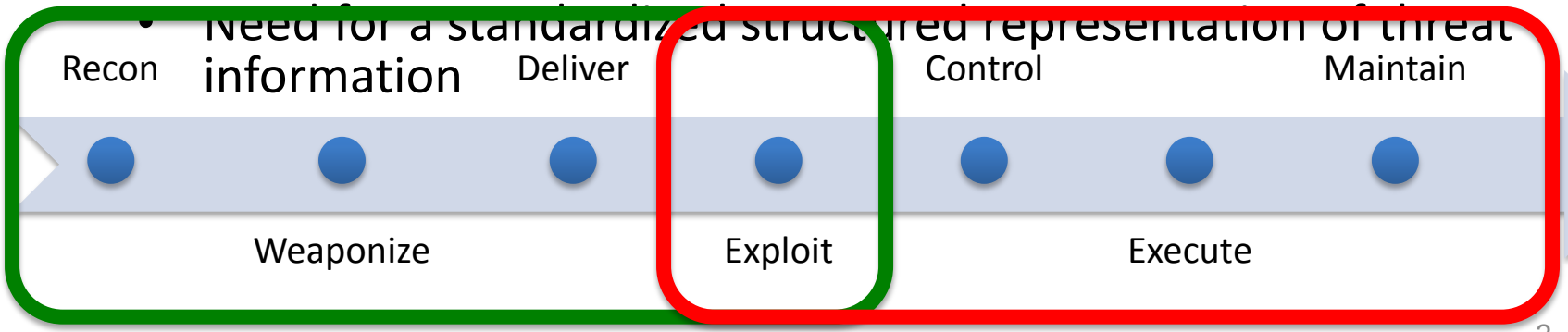
Background

Obvious

- Cyber security is a very complex and multifaceted domain
- The threat environment is very diverse and evolving
- Traditional approaches focusing inward only on vulnerability are necessary but insufficient
- There is a need to also focus outward to understand the adversary's behavior, capability and intent
- Need for more proactive, not just reactive, actions (move left of the hack)
- Need for holistic threat intelligence
- Need for information sharing and coordination
- Need for automation
- Need for a standardized structured representation of threat information

Less Obvious

- **Proactive detection "left of exploit"**
- **Incident detection and response "right of exploit"**



Current Approaches

- Cyber threat information (particularly indicators) sharing is not new
- Typically very atomic, inconsistent, and very limited in sophistication and expressivity.
- Where standardized structures are used, they are typically focused on only an individual portion of the overall problem, do not integrate well with each other, or lack coherent flexibility.
- Many existing indicator sharing activities are human-to-human exchanges of unstructured or semi-structured descriptions of potential indicators, 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 fitting already well-known attack models.
- 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.

Structured Threat History

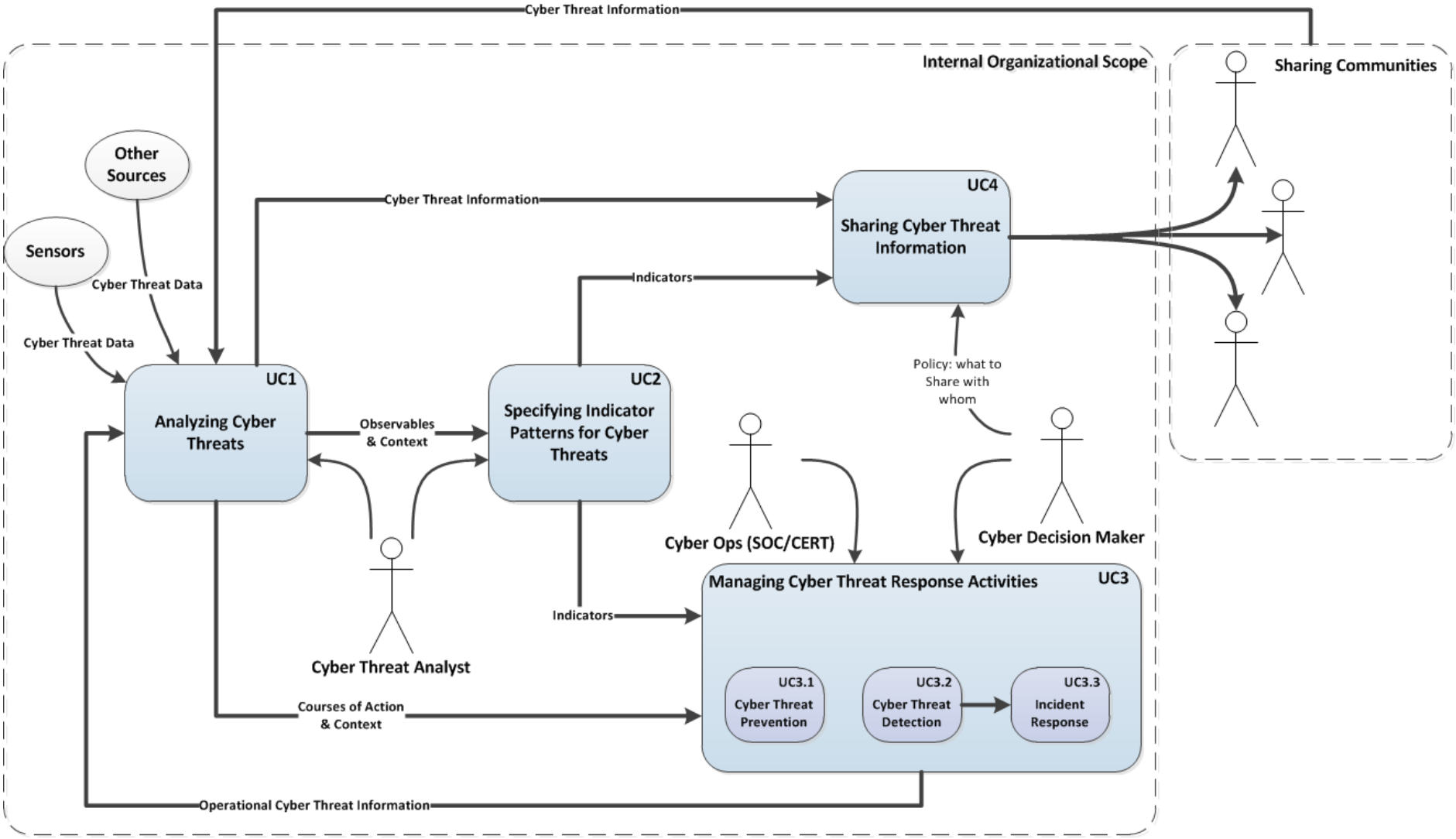
- Common Vulnerabilities and Exposures (CVE)
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration and Classification (CAPEC)
- Malware Attribute Enumeration and Characterization (MAEC)
- Cyber Observable eXpression (CybOX)
- Idxwg community of Threat Intel and Incident Response experts begins working on defining a standard representation for cyber threat indicators
  - Very urgent need
  - Based on CybOX
- Diverse opinions on what did or did not belong as part of indicators
- Community held workshop and established a clear scope for indicators
  - Threat-related information defined out of indicator scope was worked into a rough structured threat information architecture diagram
- Structured threat architecture was refined and implemented for further maturation and use

Structured Threat Information eXpression (STIX)

- What is STIX?
  - The Structured Threat Information eXpression (STIX) is a ***language***, being developed in collaboration with any and all interested parties, for the specification, capture, characterization and communication of ***cyber threat information***. It does so in a ***structured*** fashion to support more effective cyber threat management processes and application of automation.

- A variety of high-level cyber security use cases rely on such information including:
  - Analyzing cyber threats
  - Specifying indicator patterns for cyber threat
  - Managing cyber threat response activities
  - Sharing cyber threat information
- 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.

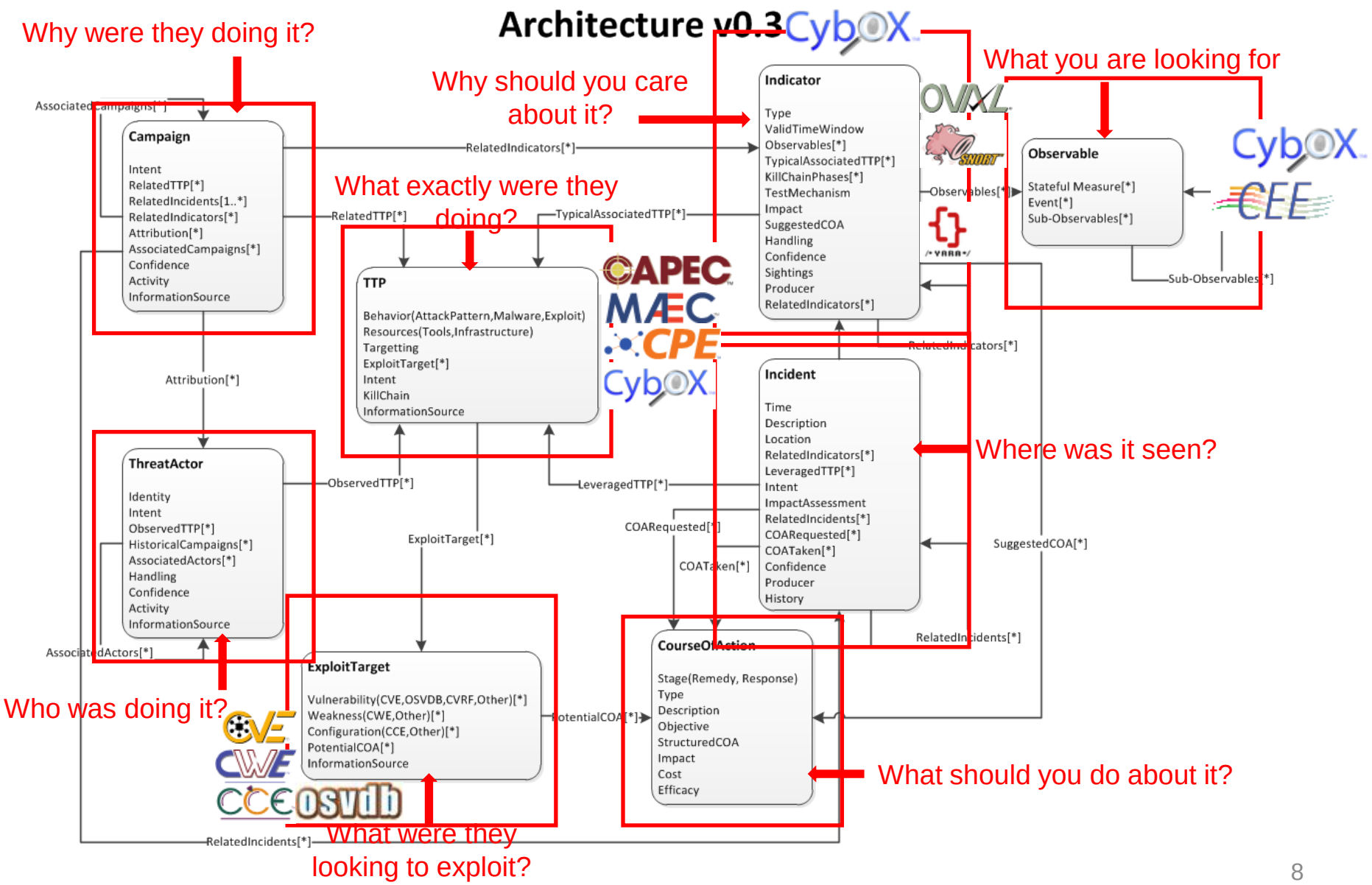
STIX Use Cases



STIX Guiding Principles

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

STIX Architecture



Implementations

- Initial implementation has been done in XML Schema
  - ubiquitous, portable and structured
- Intended as a concrete strawman for ongoing collaborative development among the community of experts
- Also targeted to provide an initial practical structure for early real-world prototyping and proof of concept implementations
- Only through appropriate levels of collaborative iteration among a relevant community of experts and vetted through real-world data and use cases can a practical and effective solution evolve
- Once an initial stable structure for the language evolves it is planned to be abstracted into an implementation-independent specification.
  - This will then enable other potential implementations to be derived including possibilities such as semantic web (RDF/OWL), JSON-centric, protobuf, etc.

Adoption & Usage

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

- Basis of US-CERT strategic approach
  - TAXII
- Announced as the basis for FS-ISAC threat information sharing
- Being integrated into MITRE's CRITs tool and processes
- Being investigated/considered by several public/public, public/private and private/private information sharing communities
- Active interest from some service/product vendors
- Basis for a new public/private threat information sharing community in Japan

- A small sampling of some of the organizations contributing to STIX includes:
  - MITRE Corporation
  - United States Computer Emergency Readiness Team (US-CERT)
  - National Institute of Standards and Technology (NIST)
  - Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - CERT Coordination Center (CERT/CC)
  - Research and Engineering Networking Information Sharing and Analysis Center (REN-ISAC)
  - Depository Trust & Clearing Corporation (DTCC)
  - Department of Defense Cyber Crime Center (DC3)
  - CrowdStrike, Inc.
  - NCI Security

Questions / Comments?

Sean Barnum

sbarnum@mitre.org