

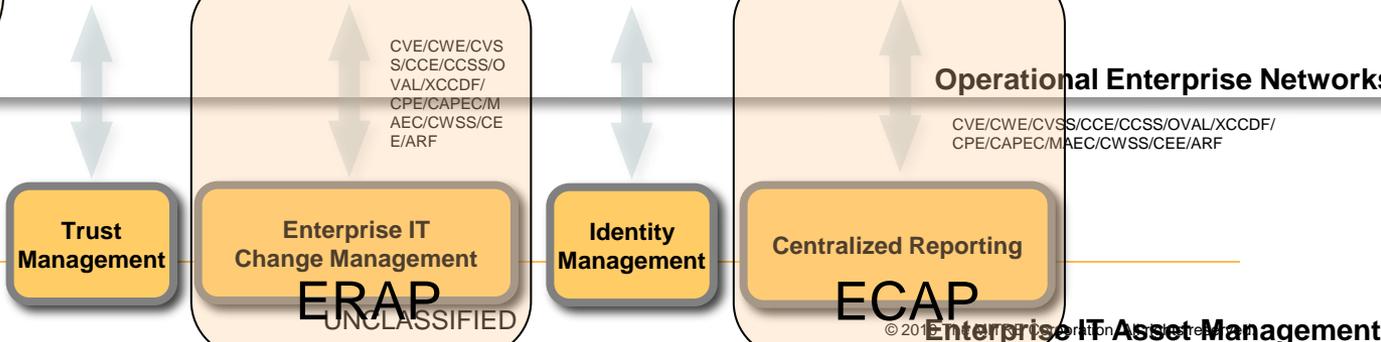
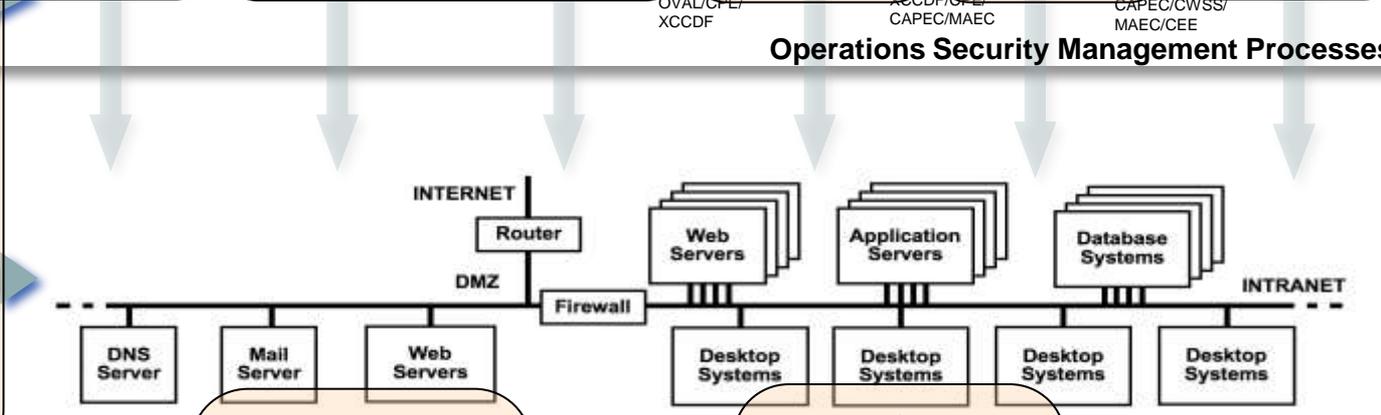
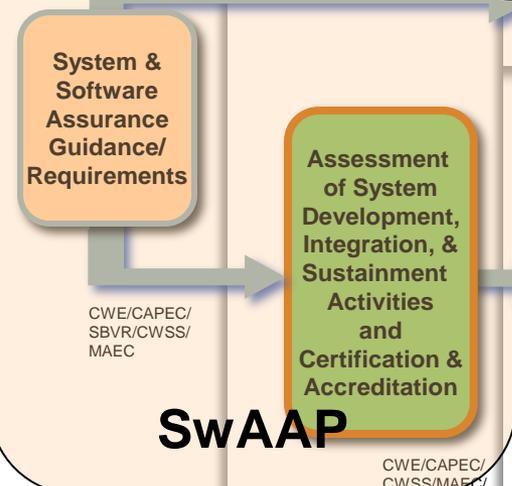
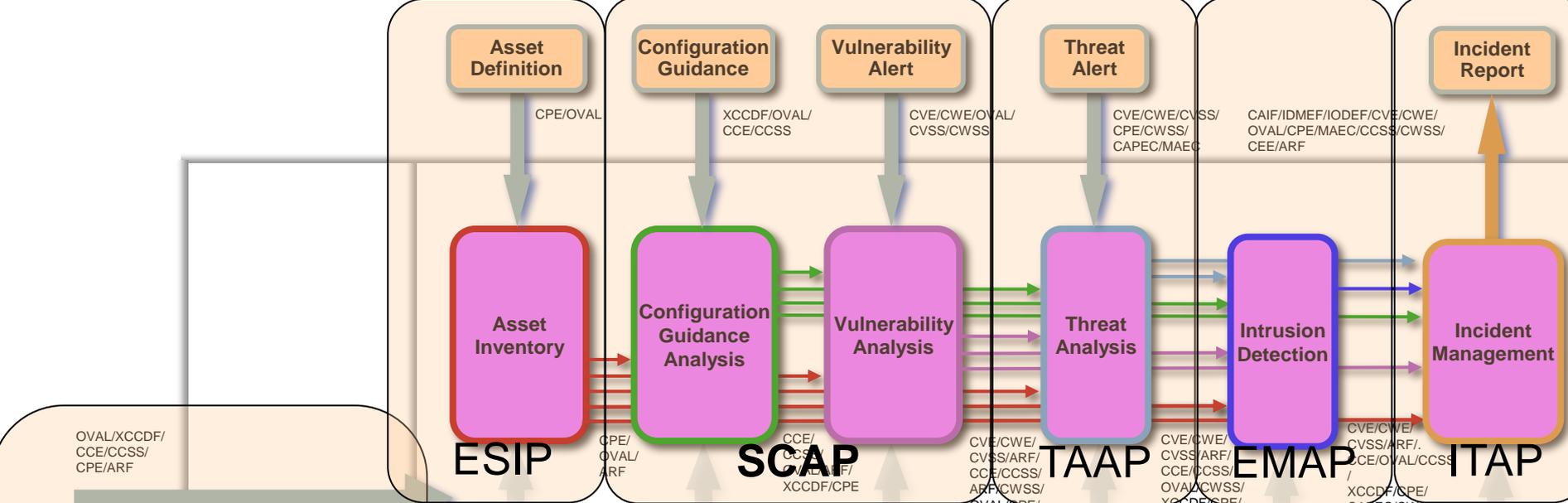
Cyber Observables and Integration with EMAP

EMAP 2011 Developer Days

Sean Barnum

Aug 2011

Knowledge Repositories



Cyber Observables Overview

- **The Cyber Observables construct is intended to capture and characterize events or properties that are observable in the operational domain.**
- **These observable events or properties can be captured and shared, defined in rules or used to adorn the appropriate portions of attack patterns and malware profiles in order to tie the logical pattern constructs to real-world evidence of their occurrence or presence for attack detection and characterization.**
- **By capturing them in a structured fashion, the intent is to enable future potential for detailed automatable sharing, mapping and analysis heuristics.**

Cyber Observables Apply to Numerous Domains

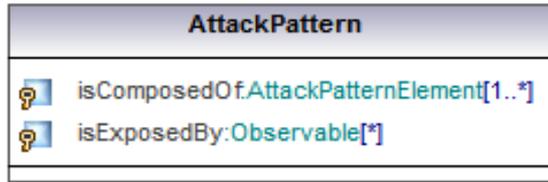
- Detailed attack patterns
- Malware characterization
- Operational Events
- Logging
- Cyber situational awareness
- Incident response
- Forensics
- Etc.

The Role of Cyber Observables in Interoperability

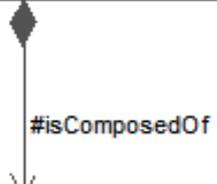
- **Characterizing event records or streams as standardized observables**
[observable isComposedOf event]
- **Mapping observables to detection rules**
[observable isModeledBy detectionRule]
- **Mapping attack patterns to observables**
[attackPatternElement isExposedBy observable]
- **Mapping malware characteristics to observables**
[malwareCharacteristic isExposedBy observable]
- **Incident Management automation through information exchange of standardized observables-based content**

IR/IM

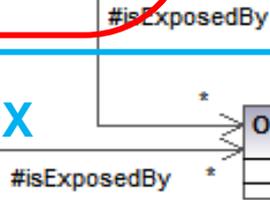
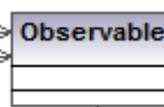
CAPEC



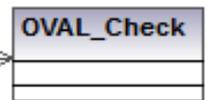
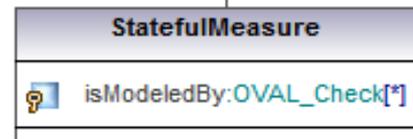
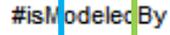
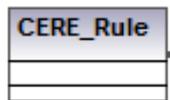
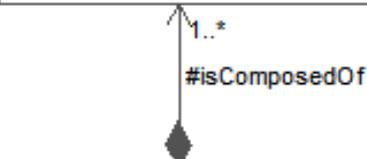
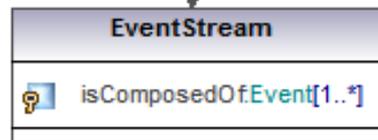
MAEC



CybOX



CEE



A Brief History of Cyber Observables

- **September 2009: Concept introduced to CAPEC in Version 1.4 as future envisioned adornment to the structured Attack Execution Flow**
- **June 2010: Broader relevance to MSM recognized leading to CAPEC, MAEC & CEE teams collaborating to define one common structure to serve the common needs**
- **August 2010: Discussed with US-CERT at GFIRST 2010**
- **December 2010: Cyber Observables schema draft v0.4 completed**
- **December 2010: Discussions with Mandiant for collaboration and alignment between Cyber Observables and Mandiant OpenIOC**
- **January 2011: Discussed & briefed with MITRE CSOC**
- **February 2011: Discussed & briefed with NIST – EMAP and US-CERT who also have a need for this construct and had begun to work on parallel solutions**
- **May 2011: Schematic alignment and integration with CEE**
- **May 2011: Spun off as independent effort called the Cyber Observable eXpression (CybOX)**

So how does CybOX integrate with EMAP?

Notional EMAP Components

■ Common Event Expression (CEE)

- A suite of specifications to define taxonomy, syntax, transport, logging recommendations, and parsing information about event records

■ Open Event Expression Language (OEEL)

- A language to express parsing and normalization logic using CEE Profiles to convert event records into CEE

■ Common Event Rule Expression (CERE)

- A common format to express rules for pattern matching, filtering, and correlation

■ Common Event Scoring System (CESS)

- A specification that provides metrics of event severity and impact based on multiple factors

■ Cyber Observable eXpression (CybOX)

- A language to express cyber observable events or stateful measures that provides a common foundation for many of the other standards

The Role of CybOX within EMAP

■ Role of CybOX with CEE

- Comprehensive structure of CybOX enables CEE to support full spectrum of event capture and sharing use cases that enterprise cyber security would require of an EMAP.
- Common underlying structure would allow CEE events to be an integral and automatable part of holistic IR/IM.
- CEE controlled vocabulary, taxonomy and object model benefits from a much broader and richer stakeholder community

■ Role of CybOX with OEEL

- CybOX offers architected structure for defining CEE Profiles and a strategically consistent basis for normalization and mapping from independent formats

■ Role of CybOX with CERE

- CybOX offers architected structure for defining automatable patterns and rules that are universally consistent and useful within EMAP and interchangeably with other automation protocols

CybOX Open Questions

- **Level of abstraction**
 - **Notional object relations and abstractions**
 - **Process *belongsTo* Application**
 - **PEInfoFile *typeOf* File**
 - **How to represent and encode into XML Schema in a understandable and manageable way**
- **Modeling similar but not identical objects**
- **Modeling Networks**
- **Use: Reporting vs. Querying**
- **Unifying terminology and project goals**

CEE-CybOX Compatibility

- **Map CEE Fields to CybOX Object-Fields**
 - Can be included in the CEE Profile Field definitions
 - Are these one-to-one mappings?
 - Who does these mappings?
 - Is mapping required or do CybOX Object-Fields become the CEE Fields?
 - CEE Profiles can be created by external entities; what about CybOX?
- **CybOX may support object-nesting**
 - How does this translate into CEE?
 - Difficult to map to deeply nested observables

CEE vs. CybOX

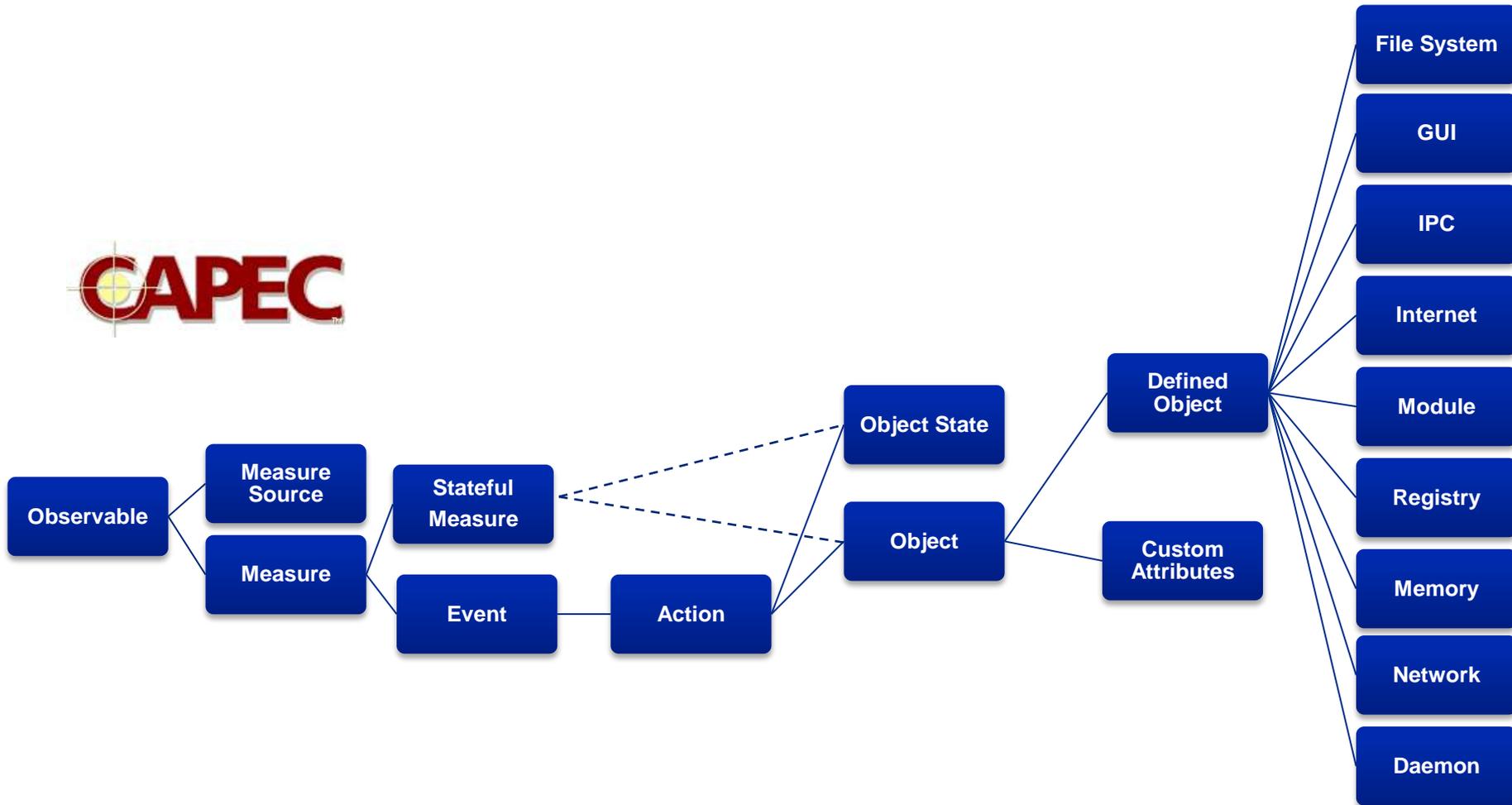
CEE

- Focus: Event Transmission
- Efficiency
- Terse
- Low-level details
- Multiple Encoding
- Inclusion by Reference

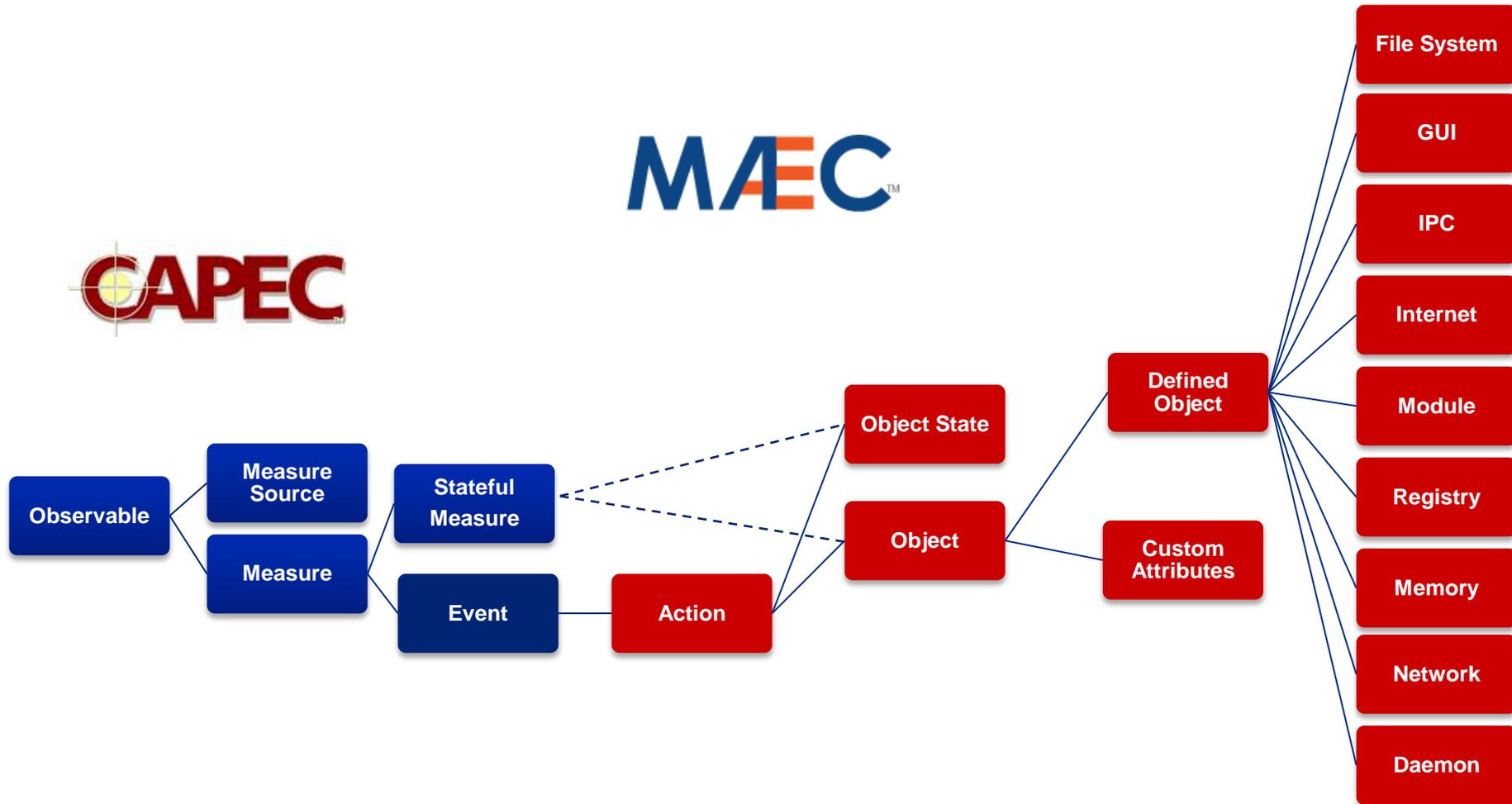
CybOX

- Focus: Reporting
- Expressive
- Complete
- High-level reports
- XML Encoding
- Inclusion by Reference or Object

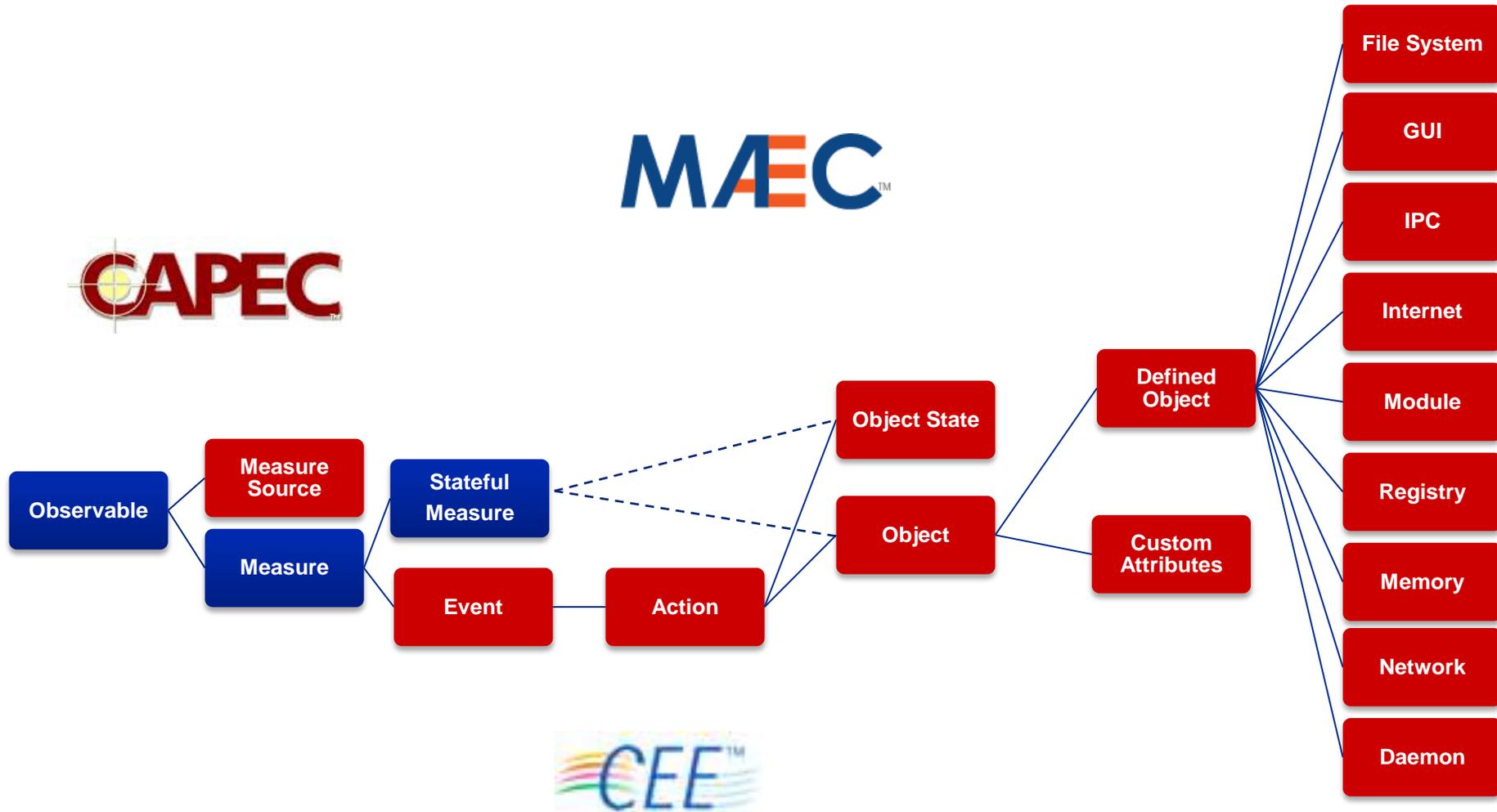
Common Cyber Observables (CybOX) Schema



Common Cyber Observables (CybOX) Schema

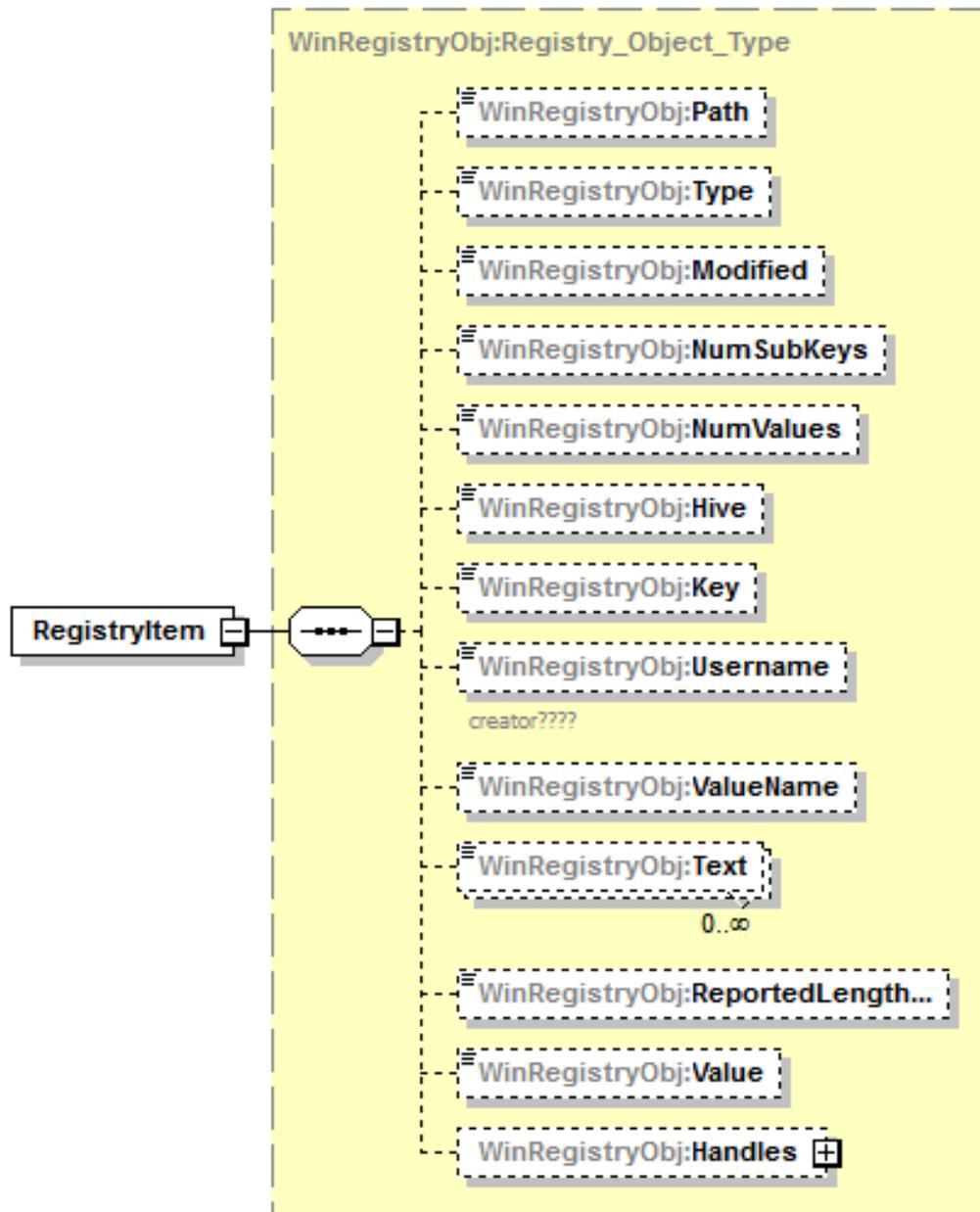


Common Cyber Observables (CybOX) Schema



Various Defined Object Schemas

- Account
 - Disk
 - Disk Partition
 - DNS Cache
 - Email Message
 - File
 - GUI
 - Library
 - Package
 - Memory
 - Network Connection
 - Network Route
 - Linux Package
 - Product
 - Service
 - Socket
 - System
 - User Session
 - Volume
 - Win Critical Section
 - Win Driver
 - Win Event
 - Win Event Log
 - Win Kernel
 - Win Kernel Hook
 - Win Handle
 - Win Mailslot
 - Win Mutex
 - Win Named Pipe
 - Win Network Route
 - Win Prefetch
 - Win Registry
 - Win Semaphore
 - Win System Restore
 - Win Task
 - Win Thread
 - Win Waitable Timer
 - X509 Certificate
 - ...
- (more on the way)



Wide Range of Cyber Observable Use Cases

- Potential ability to analyze data from all types of tools and all vendors
- Improved sharing among all cyber observable stakeholders
- Detect malicious activity from attack patterns
- Empower & guide incident management
- Identify new attack patterns
- Prioritize existing attack patterns based on tactical reality
- Ability to metatag cyber observables for implicit sharing controls
- Enable automated signature rule generation
- Enable new levels of meta-analysis on operational cyber observables
- Potential ability to automatically apply mitigations specified in attack patterns
- Etc....

Use Case: Detect Malicious Activity

■ Current:

- Manual effort to pull together data across many sensors
 - Results in limited situational awareness
- Attack patterns and rules are typically too detailed (physical signatures) or ambiguous prose
- High level of effort
- High false negatives & positives

■ CybOX-enabled:

- Diverse set of sensors output data in common format
- Attack patterns and rules can be defined in a uniform fashion
- Pattern matching and analysis heuristics can be easily automated

Use Case: Incident Response Data Capture

■ Current:

- Very manual
- Inconsistent between analysts & organizations
- Prose-based and imprecise
- Difficult to automate capture and actionable alerts

■ CybOX-enabled:

- Improved consistency
- Ability to tie everything together
- Simplified and automated data capture
- Alerts become actionable for automation

Use Case: Malware Analysis

■ Current:

- Difficult to combine different analysis perspectives or tools
- Difficult to share info
- Difficult to recognize if malware has been seen before
- Does not scale well

■ CybOX(MAEC)-enabled:

- Easier to integrate different forms of analysis, different tools and even information from different sources
- Easier to share information
- Easier to recognize malware (including variants and perturbations)
- Enables automated interaction among the various dimensions of malware analysis

Use Case: Malware Artifact Hunting

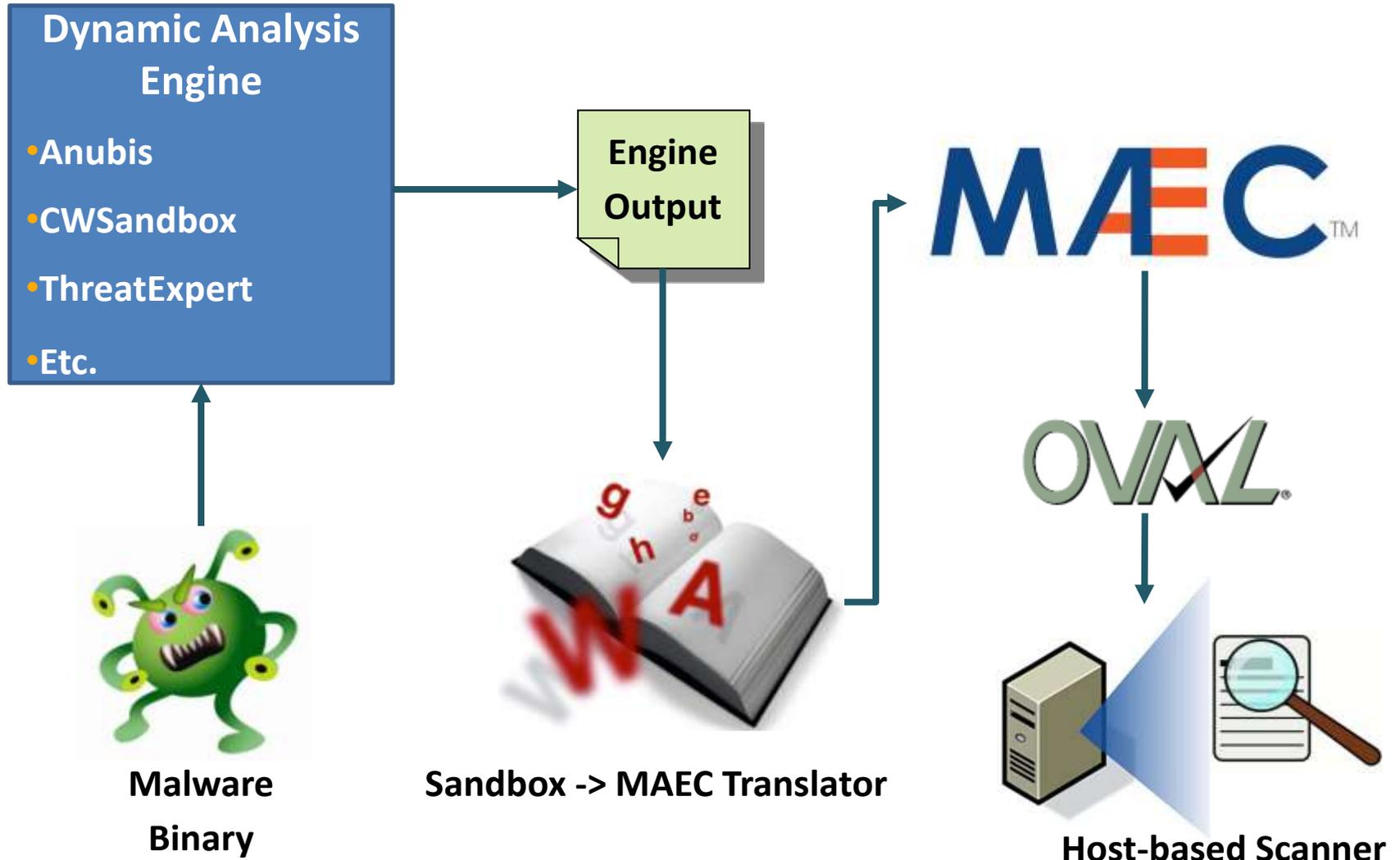
■ Current:

- Very manual
- Often imprecise and inconsistent
- Localized

■ CybOX(MAEC)-enabled:

- Very automated
- Consistent
- Enables broad, non-localized sharing and hunting

Use Case: Host Based Detection



Use Case: IR/IM Alerts

■ Current:

- Typically unstructured prose
- Labor intensive and slow
- Limited actionable (in an automated fashion) data

■ CybOX-enabled:

- Structured and consistent
- Alert generation can be much faster and less labor intensive
- Potentially actionable in an automated context

Notional Flow of a Modern Security Incident

- 1. An attack on an information system occurs involving social engineering, vulnerability exploit, malware + command and control (C2).**
- 2. CybOX-enabled operational sensors (IDS, host-based, etc.) pick up anomalous activity and report it in CEE/CybOX formats.**
- 3. Automated analysis tools & rules attempt to match anomalous activity against CybOX-adorned CAPEC attack patterns but discover no matching patterns.**
- 4. Incident is reported – Incident Response/Management process is initiated.**
- 5. IR personnel capture discovered detail of incident in CybOX-compliant formats, including CEE.**
- 6. IR personnel detect malware as part of the ongoing attack.**

Notional Flow of a Modern Security Incident (cont.)

- 7. Malware undergoes automated analysis (dynamic and/or static) and results are captured in MAEC (CybOX-integrated) language.**
- 8. Malware analysts are able to correlate the current malware instance with a broad range of pre-existing malware samples and analysis data from MAEC-enabled repositories and zoos.**
- 9. Malware analysts capture new discovered detail of the malware in MAEC format, including the CWE or CVE exploited .**
- 10. Sample and analysis data from current malware instance are entered into appropriate malware repositories and zoos.**
- 11. CybOX observables of malware effects on hosts are extracted from MAEC content to generate OVAL checks to determine if any given host has been infected/affected by the current malware instance.**
- 12. OVAL checks are distributed and run against other areas of the domain or enterprise to determine breadth of compromise.**

Notional Flow of a Modern Security Incident (cont.)

- 13.** IR/IM personnel apply appropriate mitigations/remediations to negate the effects of the attack.
- 14.** A new CAPEC attack pattern is authored to describe this new observed attack behavior, and is adorned as appropriate with CybOX content observed for this pattern in the operational space.
- 15.** IR/IM personnel issue relevant alerts for the observed incident including the new CAPEC pattern, MAEC bundle and related CEE/CybOX content.
- 16.** Secure development takes advantage of this new CAPEC pattern to: define/refine appropriate security policy, training & requirements; guide security engineering (control selection), architectural risk analysis, secure code review and security testing; identify relevant CWE weaknesses, CVE vulnerabilities & CCE configuration issues; prioritize relevant CAPEC patterns based on real-world observed prevalence/frequency profiled through automated observation of CybOX patterns in the operational space .

Where is CybOX today?

- **Currently integrated into CAPEC**
- **Currently integrated into MAEC**
- **In process of being integrated into CEE**
- **Part of the strategic approach for EMAP**
- **Part of the strategic vision for IR/IM with US-CERT**
- **Continued integration discussions planned for Mandiant OpenIOC once initial drafts of Object schemas are complete**
- **Currently being evaluated for integration into multiple research projects**
- **Website should be up soon**

Timeline

- **Initial CybOX Schemas released with CAPEC v1.6**
- **CEE v0.6 Released**
 - Have some internal mappings to CybOX
 - Formalized, released in next update
- **MAEC 2.0 update leveraging CybOX coming out within a few weeks**
- **Revised CybOX to be released EOFY11**
 - Support limited OS & host-based objects
 - Limited or no network observables

Questions / Comments?



Sean Barnum
sbarnum@mitre.org

ITSAC (Oct 31 - Nov 2) – Crystal City