Enabling Distributed Event Management: Interoperability for Automated Response and Prevention

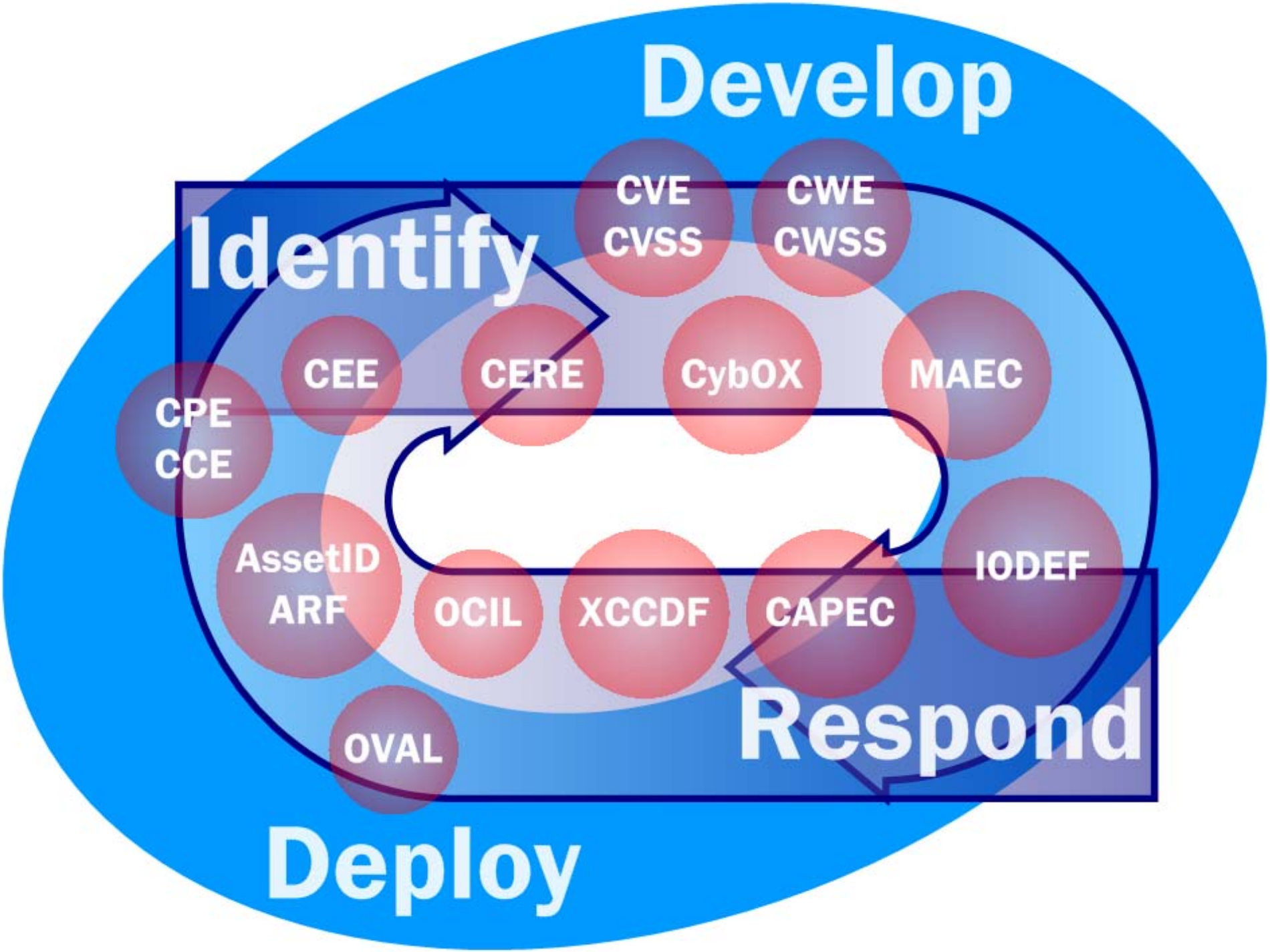
Sean Barnum
George Saylor

Aug 2011

Homeland Security

MITRE

NIST


Develop
Identify
Respond
Deploy
CVE
CVSS
CWE
CWSS
CEE
CERE
CybOX
MAEC
CPE
CCE
AssetID
ARF
OCIL
XCCDF
CAPEC
IODEF
OVAL

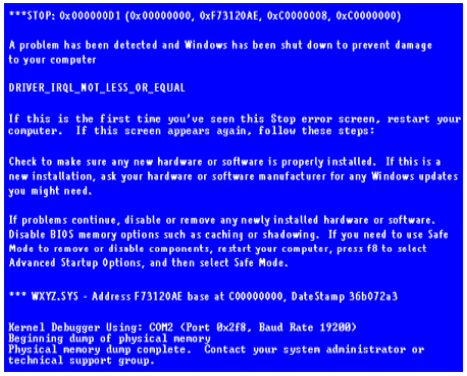
Premise

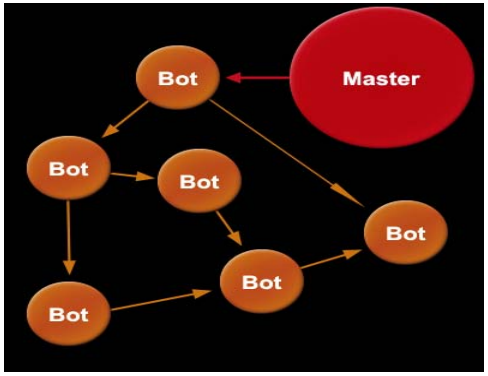
- **Supporting attack detection and automated courses of action in today's advanced threat environment requires integration and correlation of diverse sets of event producers as well as standardized structured event representations to support interoperability**

- **Solution Resources**
  - Event Management Automation Protocol (EMAP)
  - Cyber Observable eXpression (CybOX)

The Problem

- Lots of events, all in different formats





The Problem (Continued)

```
# tail -f /var/log/iptables.log | colorize
DAYMON TIME     ACTION CHAIN   IN   OUT  SRCIP           SPORT DSTIP
-- --- -------- ------ ------- ---- ---- --------------- ----- ---------------
29 Jul 15:52:35 DROP   net2fw  eth0      68.67.25.226    1143  68.67.111.66
29 Jul 15:52:41 DROP   net2fw  eth0      68.67.25.226    1143  68.67.111.66
29 Jul 15:52:41 DROP   ne
29 Jul 15:52:41 DROP   ne
29 Jul 15:52:41 DROP   ne
29 Jul 15:52:42 DROP   ne
29 Jul 15:53:01 ACCEPT fw
29 Jul 15:53:01 ACCEPT fw
29 Jul 15:53:06 ACCEPT lo
29 Jul 15:53:13 ACCEPT lo
29 Jul 15:53:19 ACCEPT lo
29 Jul 15:53:25 ACCEPT lo
29 Jul 15:54:33 ACCEPT lo
```

```
root@ubuntu access.log (Thu Aug  6 08:2
File  Edit  View  Terminal  Tabs  Help
illa/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0
(intrepid) Firefox/3.0.12"
192.168.0.191 - - [06/Aug/2009:08:21:26 -0400]
illa/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0
(intrepid) Firefox/3.0.12"
192.168.0.191 - - [06/Aug/2009:08:21:26 -0400]
illa/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0
(intrepid) Firefox/3.0.12"
192.168.0.191 - - [06/Aug/2009:08:21:26 -0400]
illa/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0
(intrepid) Firefox/3.0.12"
00] access.log                                  2KB -
[Wed Aug 05 11:37:21 2009] [error] [client 192.168.0.191] Fil
var/www/favicon.ico
[Wed Aug 05 11:37:21 2009] [error] [client 192.168.0.191] Fil
var/www/favicon.ico
[Wed Aug 05 11:37:24 2009] [error] [client 192.168.0.191] Fil
var/www/favicon.ico
[Thu Aug 06 08:00:28 2009] [
apache2: Could not reliably
using 127.0.1.1 for ServerNa
[Thu Aug 06 08:00:30 2009] [
 normal operations
01] error.log *Press F1/<CTR
```

```
Oct 19 04:38:06 Thu Oct 02 01:
217:6000 to 67.158.78.125:7212
Oct 19 04:38:06 Thu Oct 02 01:
217:6000 to 67.158.78.125:8000
Oct 19 04:38:06 Thu Oct 02 01:
217:6000 to 67.158.78.125:3128
Oct 19 04:39:43 Thu Oct 02 01:
34.205 to 67.158.78.125
Oct 19 04:40:05 Thu Oct 02 01:
186:30396 to 67.158.78.125:135
Oct 19 04:40:13 Thu Oct 02 01:
 67.158.78.125:1026
Oct 19 04:40:13 Thu Oct 02 01:
 67.158.78.125:1027
Oct 19 04:40:58 Thu Oct 02 01:
57:12200 to 67.158.78.125:8800
Oct 19 04:46:59 Thu Oct 02 01:
 67.158.78.125:1026
Oct 19 04:47:41 Thu Oct 02 01:33:11 2008 D-Link Syste
 67.158.78.125:1026
Oct 19 04:48:47 Thu Oct 02 01:34:16 2008 D-Link Syste
0:1258 to 67.158.78.125:25099
Oct 19 04:49:18 Thu Oct 02 01:34:47 2008 D-Link Syste
```

```
UbuntuServerHTG
geek@ubuntuServ:/var/log/mysql$ tail -f mysql.log
                    54 Query       SELECT user_id, usernam
e, user_colour, user_birthday
                FROM phpbb_users
                WHERE user_birthday LIKE '17- 5-%'
                        AND user_type IN (0, 3)
                    54 Query       SELECT u.username, u.us
ernamе_clean, u.user_id, u.user_type, u.user_allow_viewonli
ne, u.user_colour, s.session_ip, s.session_viewonline
                        FROM phpbb_users u, phpbb_sessions
s
                        WHERE s.session_time >= 1179379785
                                AND u.user_id = s.session_u
ser_id
                        ORDER BY u.username_clean ASC, s.se
ssion_ip ASC
```

```
[**] [116:151:1] (snort decoder) Bad Traffic Same Src/Dst IP [**]
11/20-10:34:09.497033 127.0.0.1 -> 127.0.0.1
ICMP TTL:64 TOS:0x0 ID:6392 IpLen:20 DgmLen:84
Type:0  Code:0  ID:57927  Seq:0  ECHO REPLY

[**] [116:150:1] (snort decoder) Bad Traffic Loopback IP [**]
11/20-10:34:09.497033 127.0.0.1 -> 127.0.0.1
                                    DgmLen:84
                                    REPLY
```

From	To	Start	Duration	Status
Sip Send <sip:sipsend	*1100*421	12/3/06 12:19 AM	1 minute, 6 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 1:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 2:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 3:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 4:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 5:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 6:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 7:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 8:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 9:19 AM	1 minute, 7 seconds	Completed
Sip Send <sip:sipsend	*1100*421	12/3/06 10:19 AM	1 minute, 7 seconds	Completed

What is EMAP?

- A program to establish a protocol to enable standardized content, representation, exchange, correlation, searching, storing, prioritization, and auditing of event records within an organizational IT environment
- A specification to meet these goals and define how relevant technical specifications will interact to achieve the desired outcomes.
- Develop and implement validation of products that conform to the standard

What is EMAP? (Continued)

Languages

Express logs and policies

- Common Log formats
- Log correlation rules
- Logging configuration
- Audit Settings
- Normalization
- Incident Description
- Observable Description

Metrics

Event scoring framework

- Severity of logged events
- Criticality
- Impact

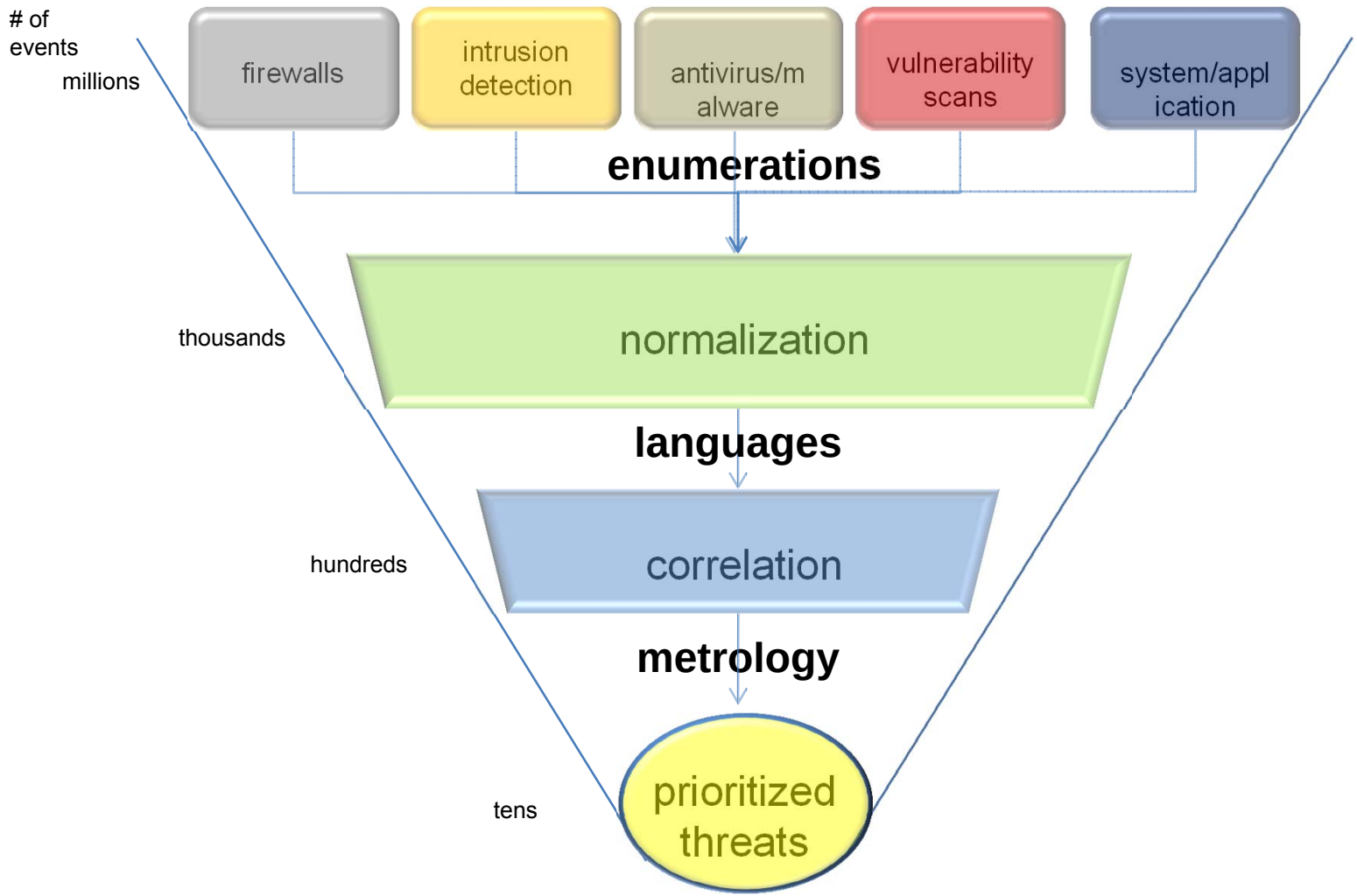
Enumerations

Convention for identifying and naming

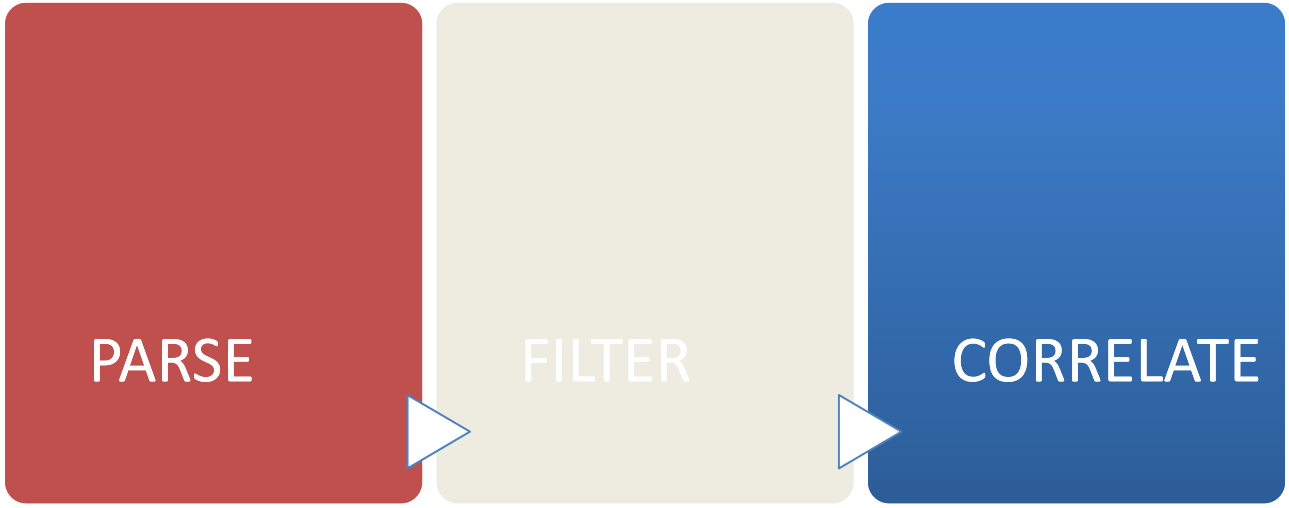
- Log taxonomy
- Enrichment information
- Observables

(U)

Event Funnel



How it all works



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

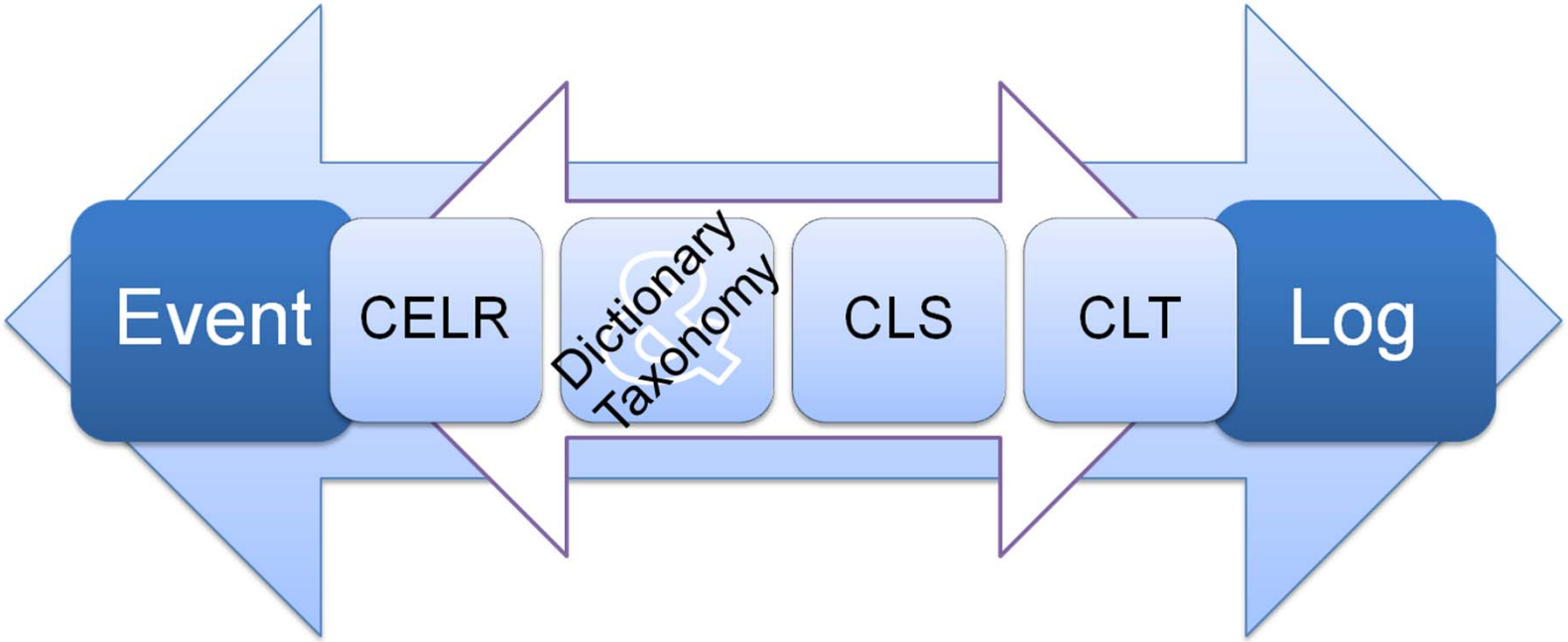
Notional EMAP Components

- 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

CEE Components

- CEE Dictionary
- CEE Taxonomy (CEET)
- Common Event Log Recommendations (CELR)
- Common Log Syntax (CLS)
- Common Log Transport (CLT)

CEE Architecture



OEEL

- Provide a standardized ability to represent parsing logic external to the parsing application
  - Provide vendors and consumers to express and share parsing logic in a standard format
  - Simplify product development
  - A way to change a native log into a standard format (example Apache to CEE)
  - Combine multiple log and data sources together into common output

CERE

- Provide vendors and consumers a way to express and share rules for pattern matching, correlation, and filtering of logs
  - Support distributed multi-vendor enterprises
  - Aid in acquisition
  - Simplify sharing detection rules to public
  - Achieve this with minimal impact to vendors and consumers

CESS

- Provide a metric for scoring the severity, criticality, and impact of a given event, set of events, or incident
  - Leverage EMAP components to derive reasonably accurate scoring
  - Use CESS to assist in filtering and correlation
  - Provide vendors, responders, analysts a reliable and repeatable means of calculating and sharing this information

Enabling Automated Response and Prevention

- Interoperability
  - Mapping observables and indicators to detection rules
  - Mapping attack patterns to observables and detection rules
  - Mapping malware characteristics to observables and rules
  - Incident Management automation through information exchange of standardized content

Cyber Observables Overview

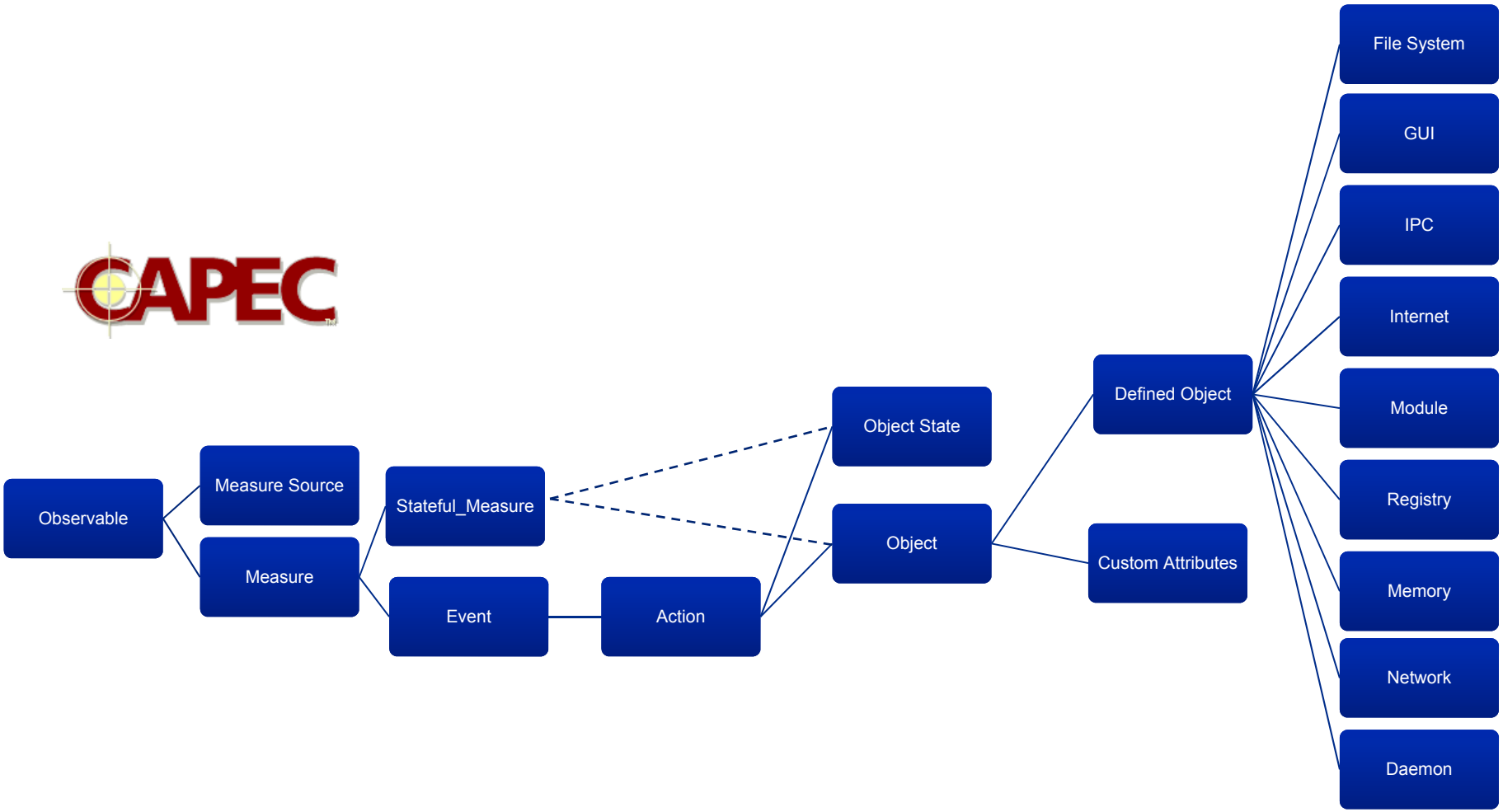
- The Cyber Observables construct is intended to capture and characterize events or properties that are observable in the operational domain.
- These observable events or properties can be defined in rules or used to adorn the appropriate portions of the attack patterns in order to tie the logical pattern 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 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.

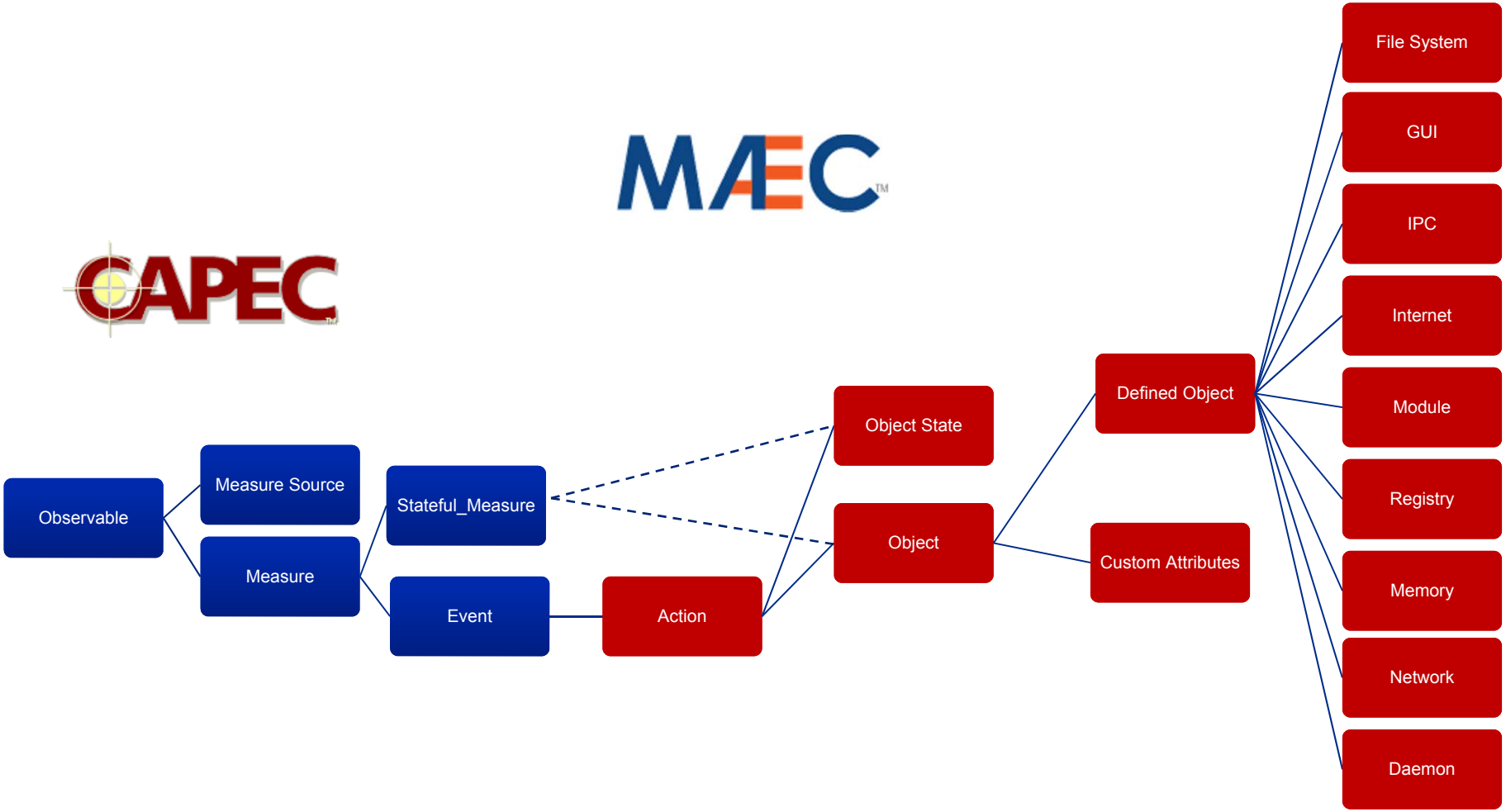
A Brief History of Cyber Observables

- 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

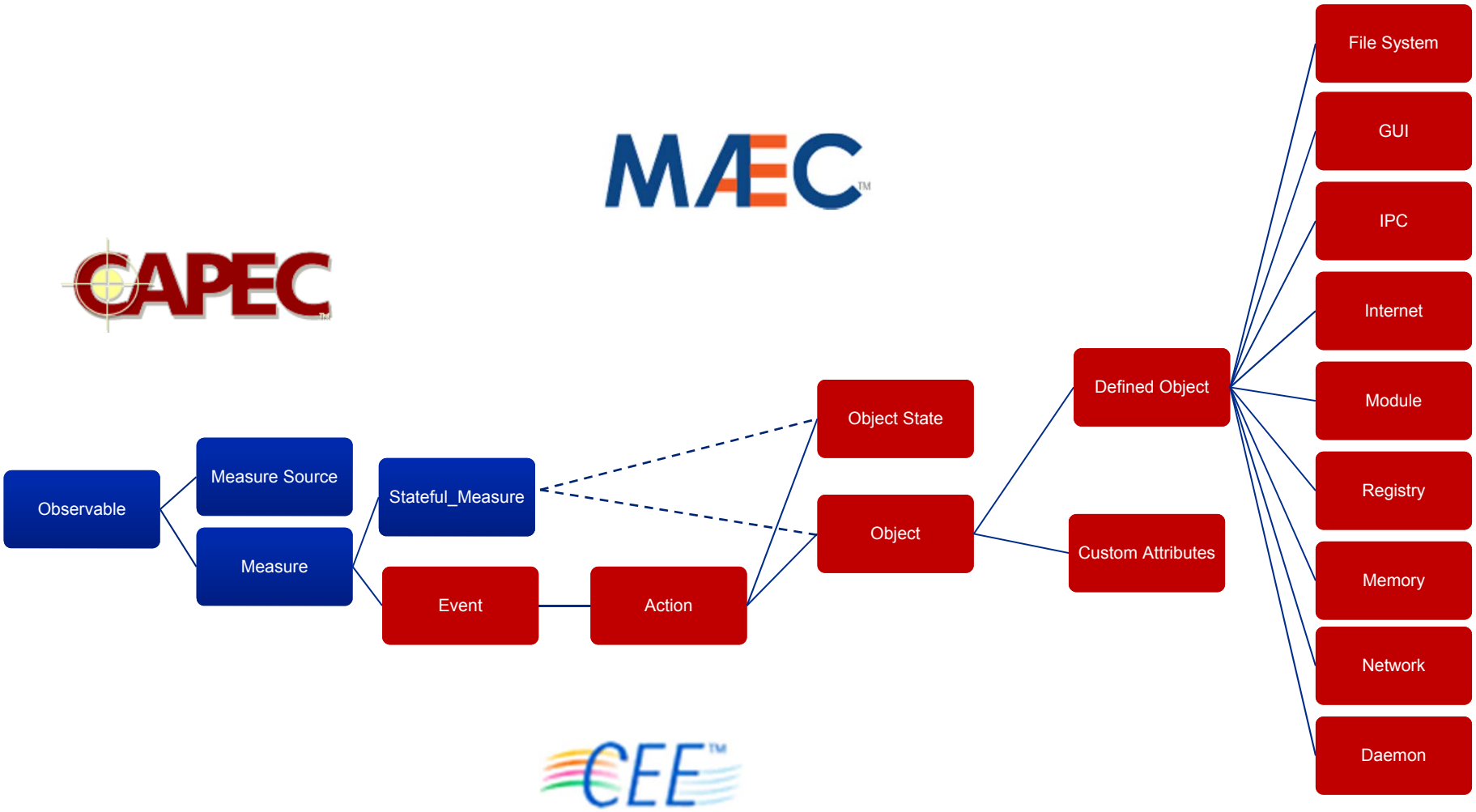
Common Cyber Observables (CybOX) Schema



Common Cyber Observables (CybOX) Schema



Common Cyber Observables (CybOX) Schema

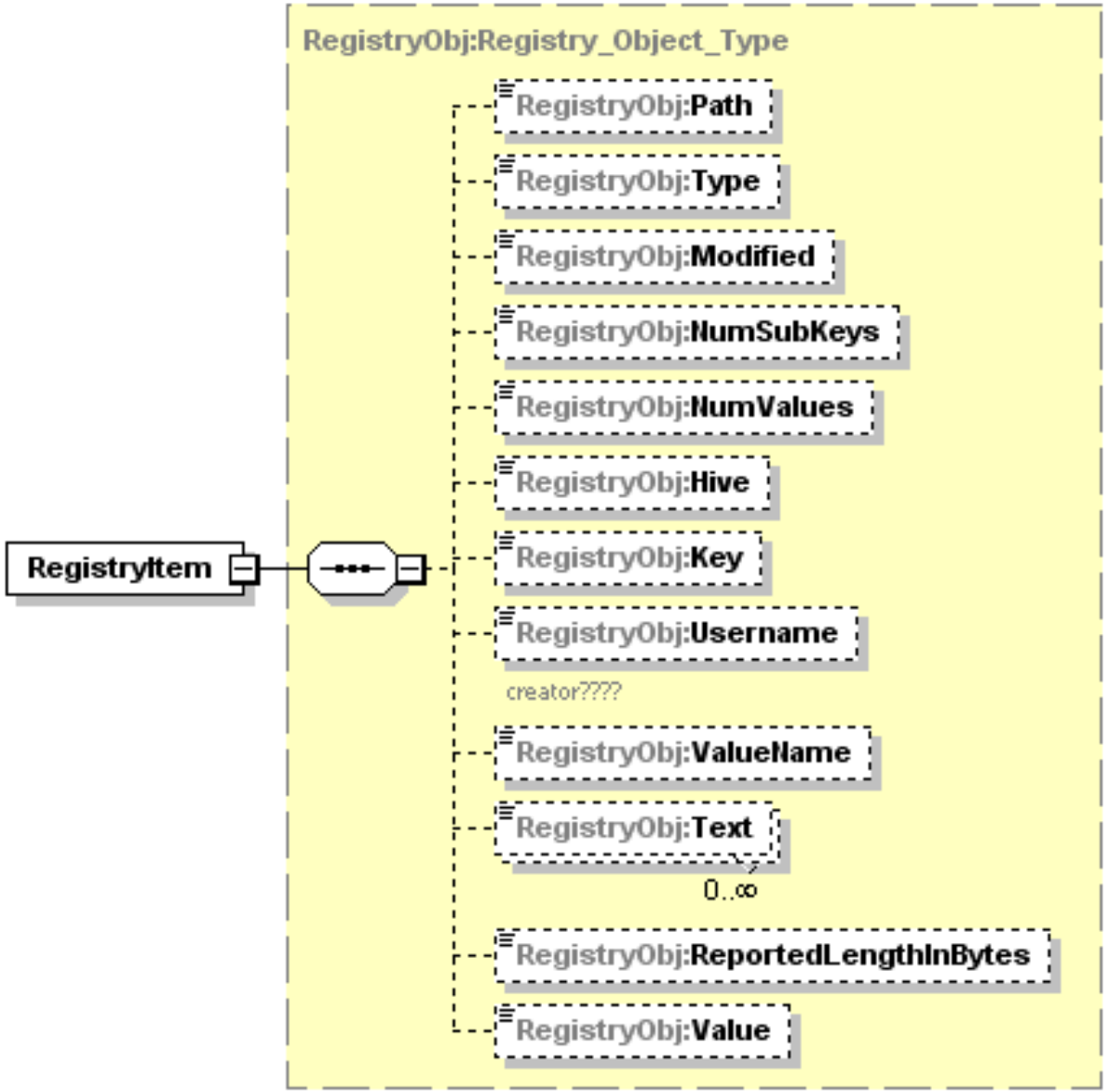


Various Defined Object Schemas

- 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)



Generated by XMLSpy www.altova.com

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**

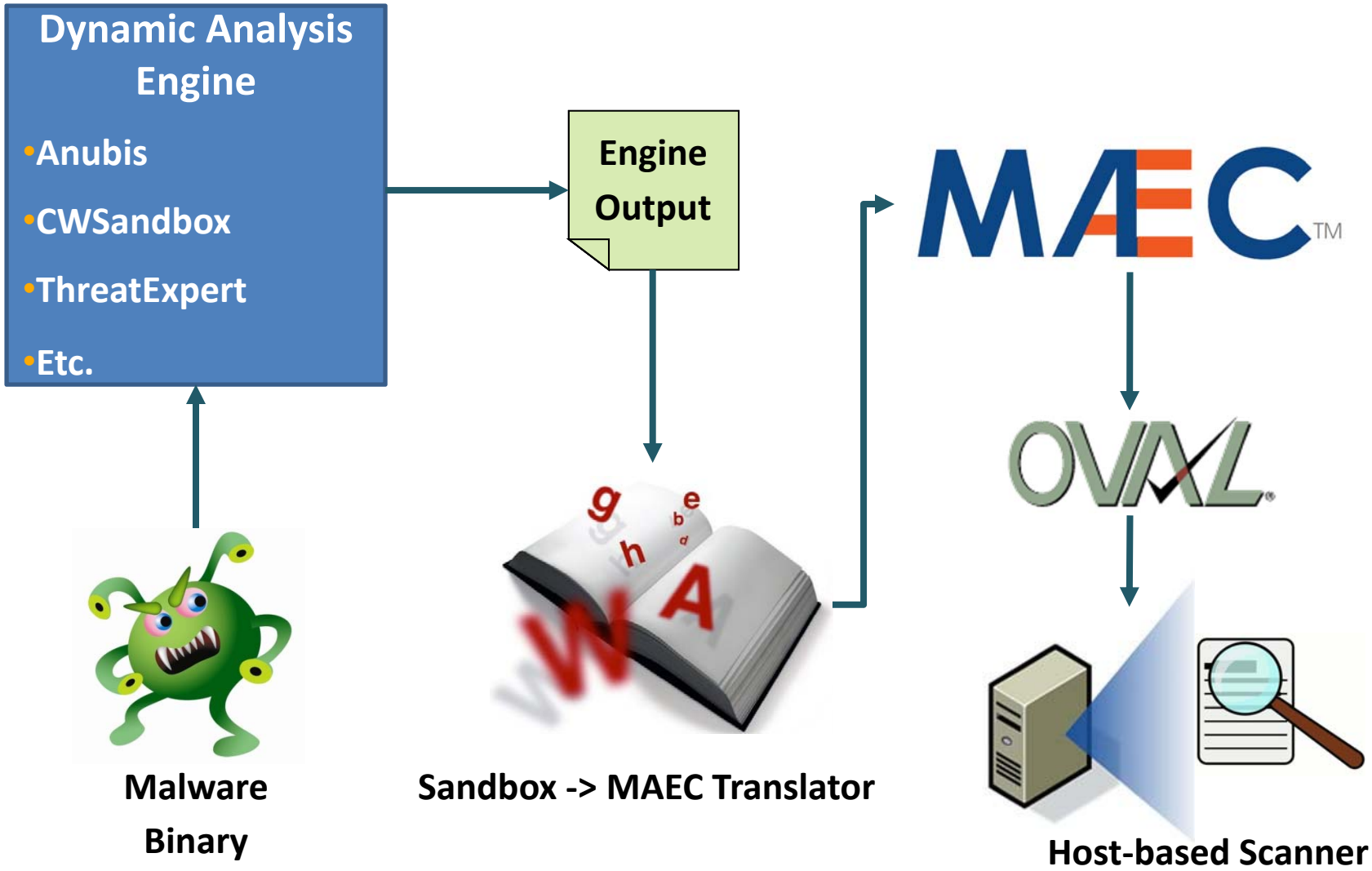
- **CybOX(MAEC)-enabled:**
  - **Easier to integrate different forms of analysis, different tools and even information from different sources**
  - **Easier to share information**
  - **Easier to recognize malware (including variants and pertubations)**
  - **Enables automated interaction among the various 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

Questions / Comments?

Sean Barnum
sbarnum@mitre.org

George Saylor
george.saylor@nist.gov

EMAP Developer Days (Aug 29-30) – NIST

http://scap.nist.gov/events

ITSAC (Oct 31 - Nov 2) – Crystal City