Penny Chase **Ivan Kirillov**

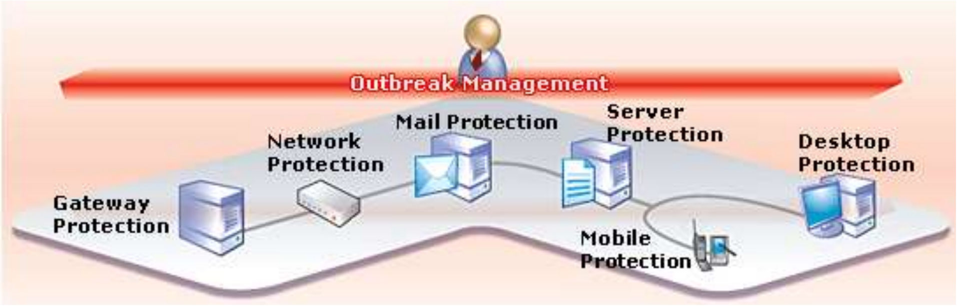
31 October 2011 //ITSAC 2011

Agenda

- Introduction
- MAEC & Security Automation
- Future MAEC Directions
- Community Outreach

Why Do We Need to Develop Standards for Malware?

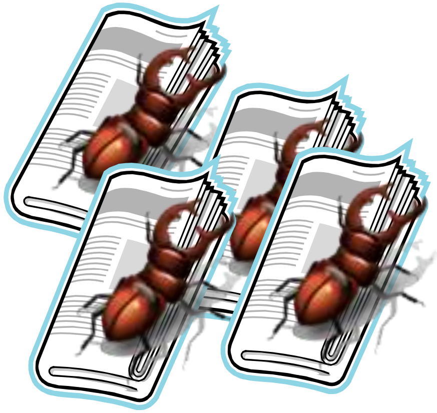
Multiple layers of protection

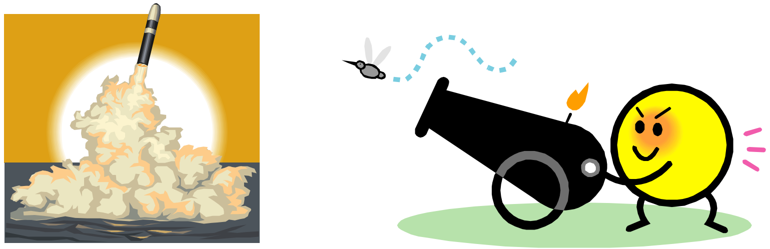


Lots of products

debian
qualys
WHITEHAT
SPI DYNAMICS
NETWITNESS
ArcSight
redhat
netIQ
SofCheck
Sun
Nessus
PARASOFT
CENZIC
Klockwork
Lancope
nCircle
Internet Security Systems
Novell
BARRACUDA
ORACLE
BOTERIA
VERACODE
eset
CORE
IBM
F-SECURE
authentium
FORTINET
symantec
ca
FORTIFY
RADAR
McAfee
GRISOFT
SOPHOS
tripwire
BIGFIX
OUNCE LABS
watchfire
Microsoft
Configuresoft
STAT
SOURCEfire
ThreatGuard
Secure Software

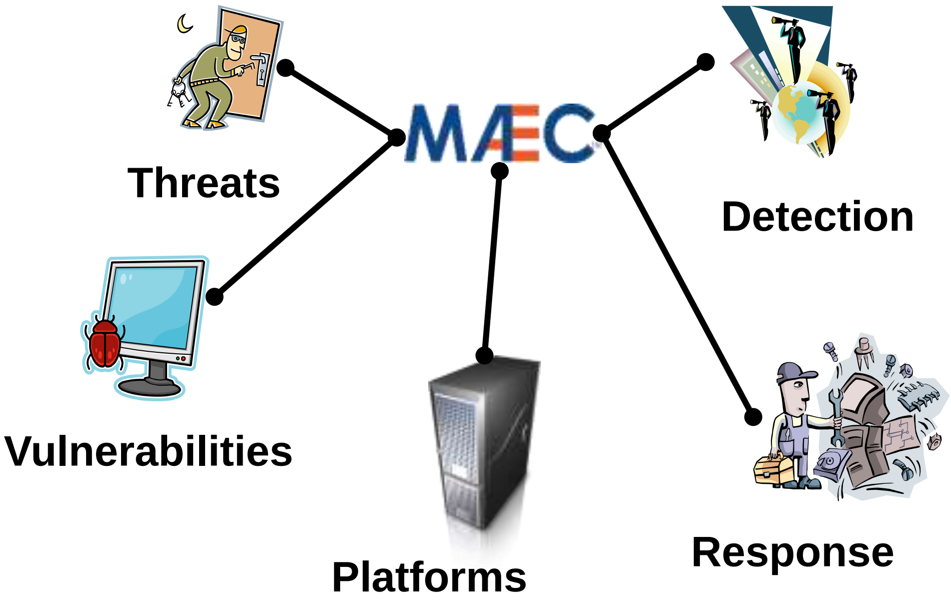
Inconsistent reports





There’s an arms race

Malware Attribute Enumeration and Characterization (MAEC)



MÆC

Threats

Vulnerabilities

Platforms

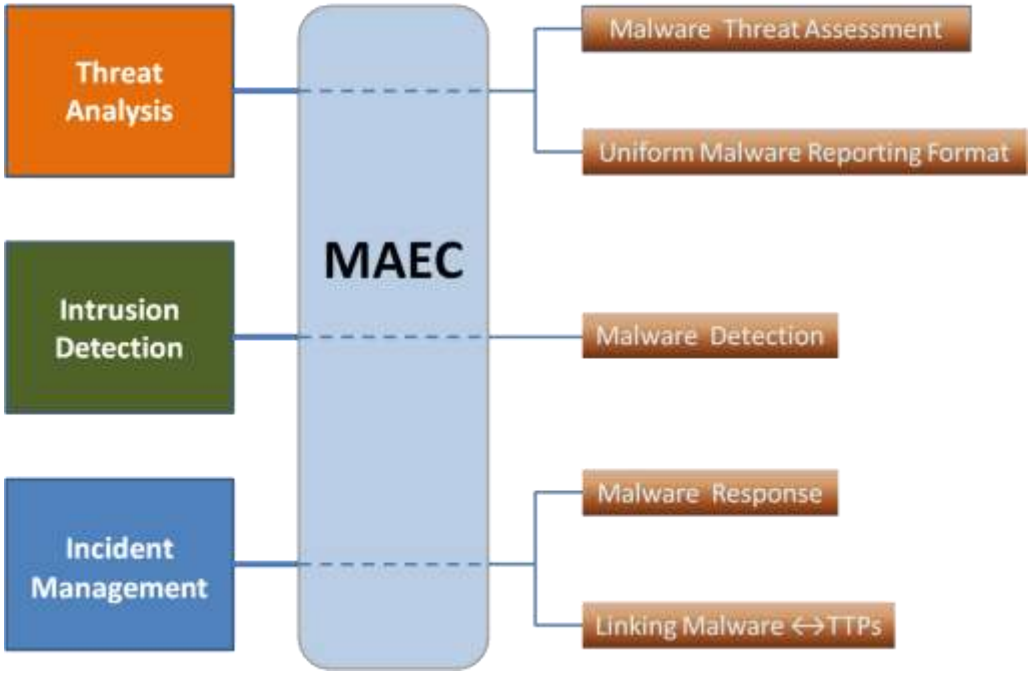
Detection

Response

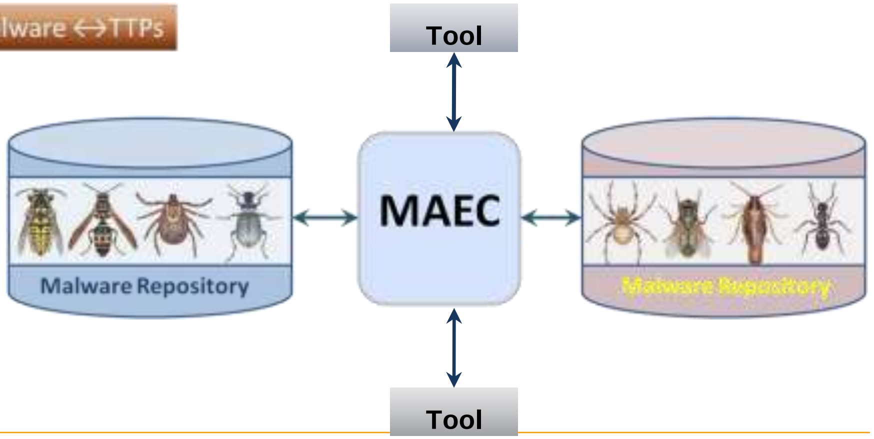
- Language for sharing structured information about malware
  - Grammar (Schema)
  - Vocabulary (Enumerations)
  - Collection Format (Bundle)
- Focus on attributes and behaviors
- Enable correlation, integration, and automation

MAEC Use Cases

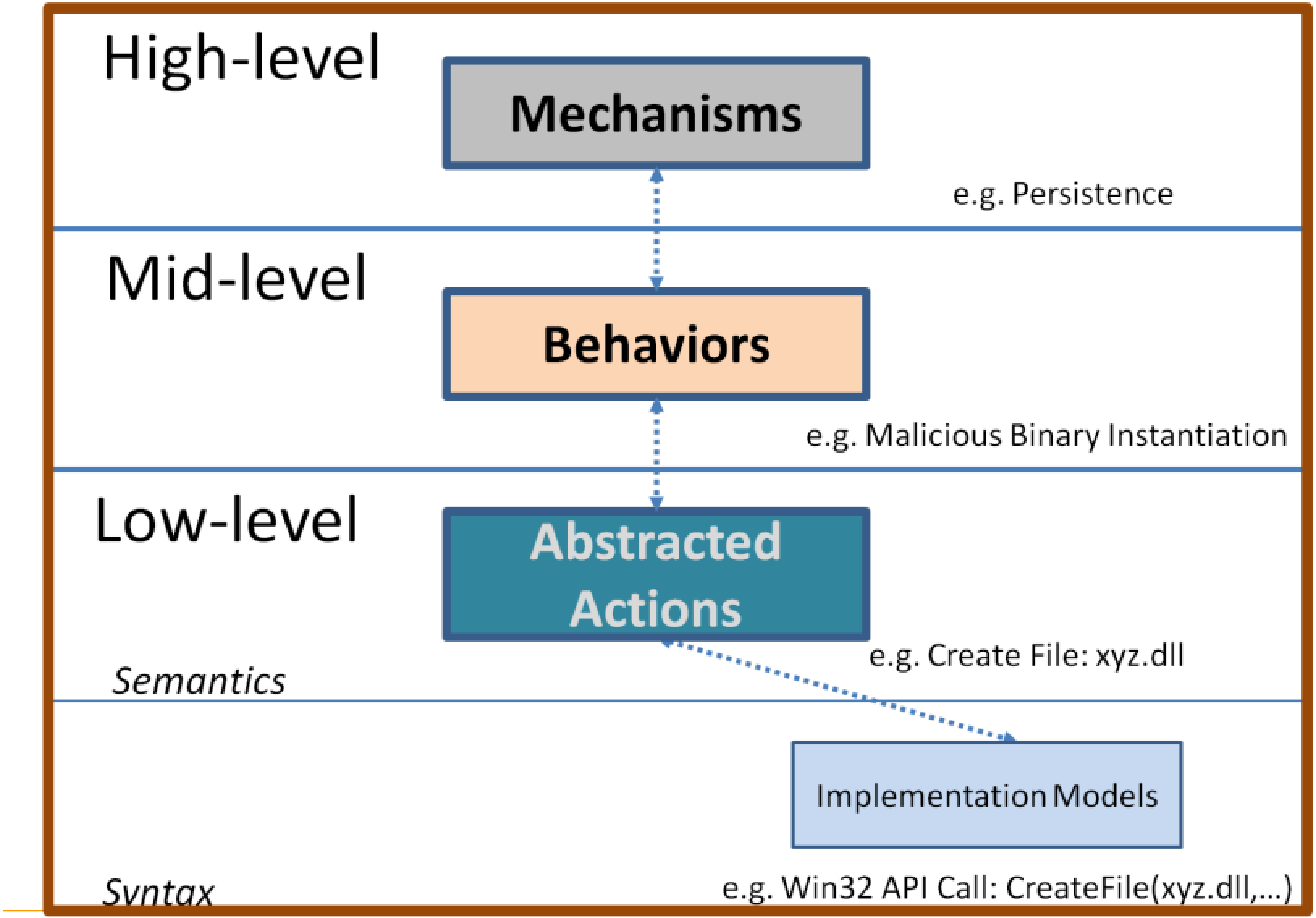
- Operational



- Analysis
  - Help Guide Analysis Process
  - Standardized Tool Output
  - Malware Repositories



MAEC Structure Overview



High-level

Mechanisms

e.g. Persistence

Mid-level

Behaviors

e.g. Malicious Binary Instantiation

Low-level

Abstracted Actions

e.g. Create File: xyz.dll

Semantics

Implementation Models

Syntax

e.g. Win32 API Call: CreateFile(xyz.dll,...)

MAEC’s Current Format

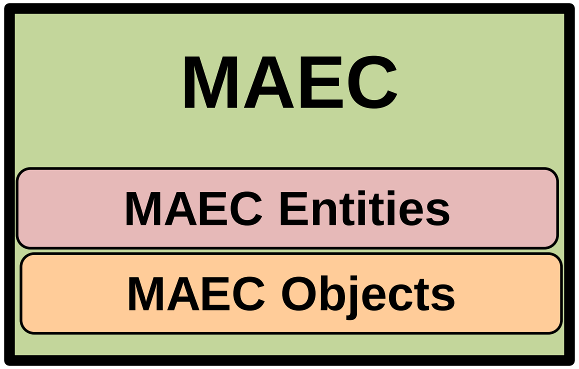
- XSD Schema
  - v1.0 – June 2010
    - Initial release
    - Focused on dynamic analysis output
  - v1.1 – January 2011
    - Added static analysis capability (PE attributes)
    - Schema changes, proper versioning implemented
  - v2.0 – Fall/Winter 2011
    - MAEC object model replaced with CybOX
    - ActionType simplified
    - EffectType refined
    - Lots of ‘under the hood’ tweaks and minor additions

MAEC v2.0 Additions

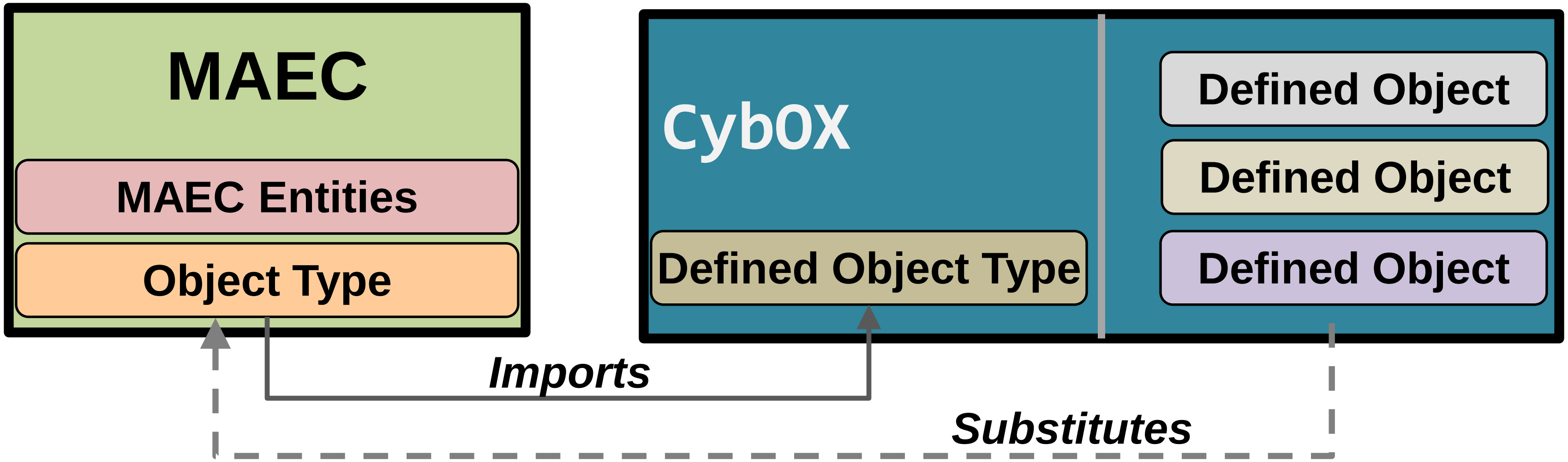
- Indicator Management Capability
  - Permits standard method of defining anti-malware indicators.
  - Linkages to other MAEC entities where appropriate. E.g. objects for specifying indicator used in detection.
- Relationship Support
  - Allows defining simple relationships between MAEC entities in an easy to use fashion. Examples: ParentOf, ChildOf, PrecededBy, etc.
- Many new enumerated types
  - Actions, Effects, Relationships, etc.

MAEC & CybOX

- Before (MAEC 1.x)



- After (MAEC 2.0 and up)



MAEC v1.1 Objects

- File System (File, Directory, Named Pipe)
- GUI (Window, Dialog)
- IPC (Thread, Mutex)
- Internet (URL)
- Module
- Registry (Key, Key/Value Pair)
- Process
- Memory
- Network (Socket, Port, IP Address)
- Daemon (Service)

MAEC v2.0 Objects (imported from CybOX)

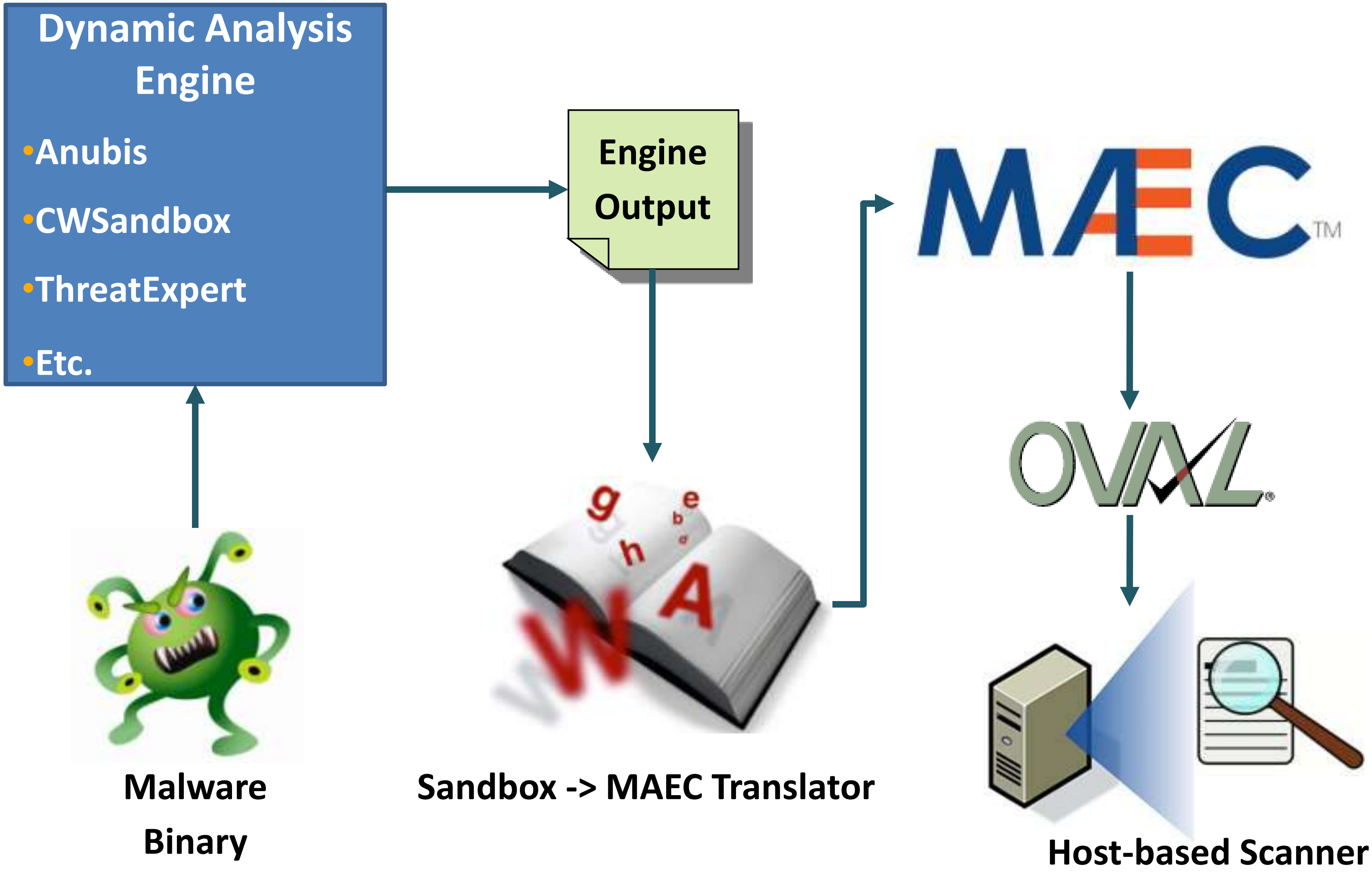
- Account
- Disk
- Disk Partition
- DNS Cache
- Email Message
- File
- GUI
- Library
- Package
- Memory
- Network Connection
- Network Route
- Linux Package
- Product
- Service
- Socket
- System
- User Session
- Volume
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Kernel
- Win 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)

MÆC™ & Security Automation

MAEC & Host Based Detection I



Dynamic Analysis Engine

- Anubis
- CWSandbox
- ThreatExpert
- Etc.

Engine Output

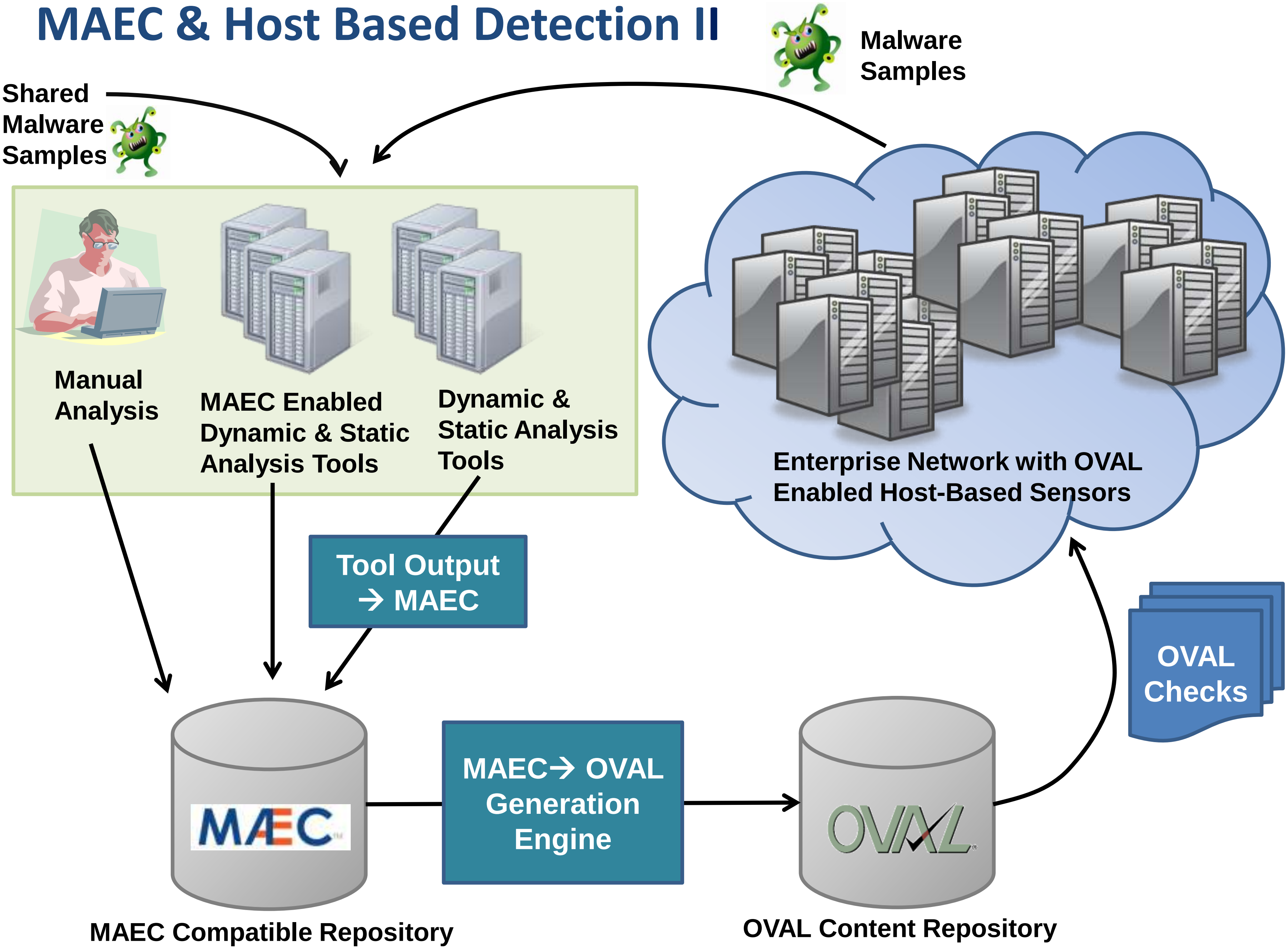
Malware Binary

Sandbox -> MAEC Translator

Host-based Scanner

MITRE

MAEC & Host Based Detection II



Malware Samples

Shared Malware Samples

Manual Analysis

MAEC Enabled Dynamic & Static Analysis Tools

Dynamic & Static Analysis Tools

Enterprise Network with OVAL Enabled Host-Based Sensors

Tool Output → MAEC

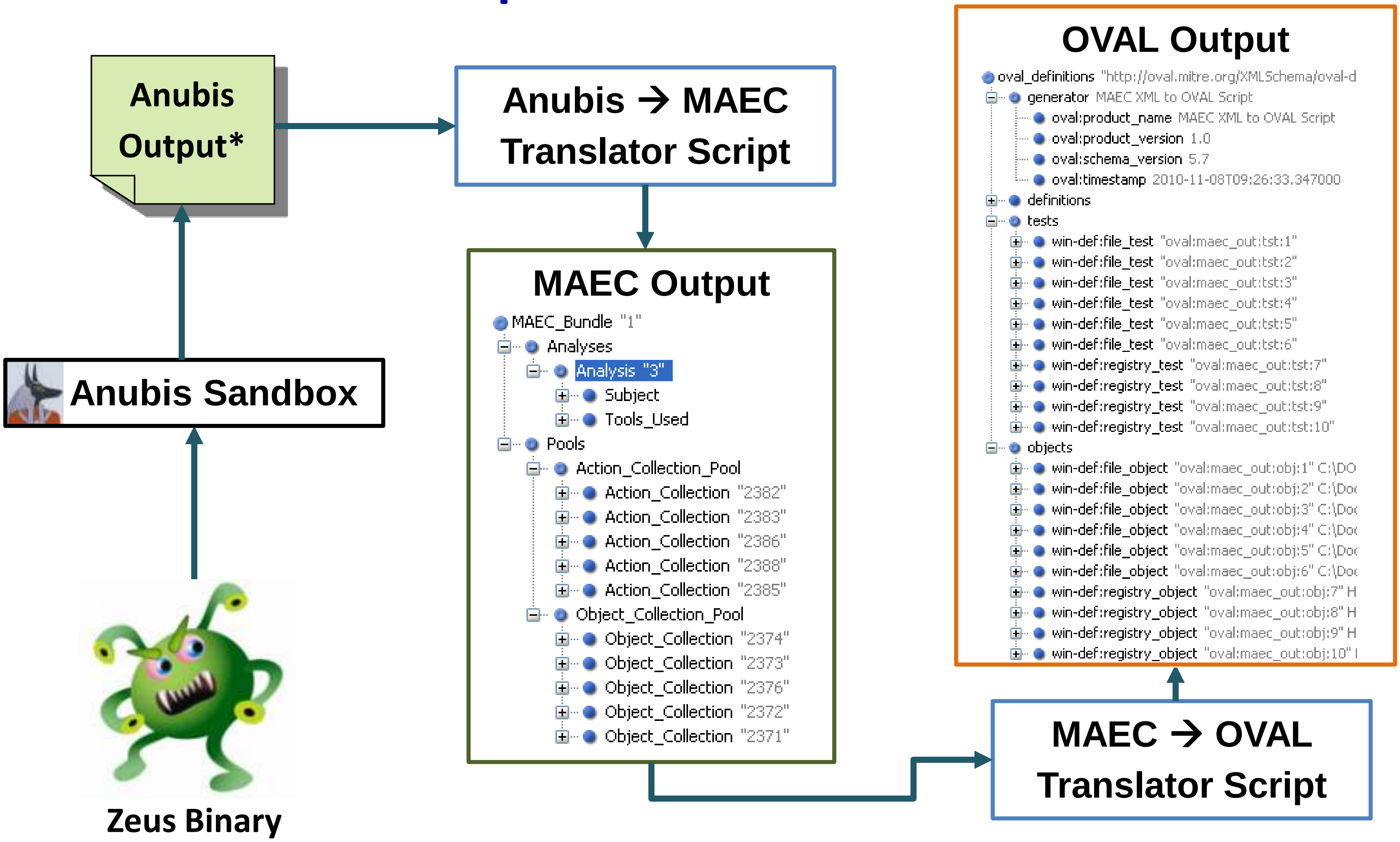
OVAL Checks

MAEC→ OVAL Generation Engine

MAEC Compatible Repository

OVAL Content Repository

Real World Example: MAEC & Zeus Bot



Anubis Output*

Anubis → MAEC Translator Script

Anubis Sandbox

Zeus Binary

MAEC Output

```
MAEC_Bundle "1"
⊟ Analyses
   ⊟ Analysis "3"
      ⊞ Subject
      ⊞ Tools_Used
⊟ Pools
   ⊟ Action_Collection_Pool
      ⊞ Action_Collection "2382"
      ⊞ Action_Collection "2383"
      ⊞ Action_Collection "2386"
      ⊞ Action_Collection "2388"
      ⊞ Action_Collection "2385"
   ⊟ Object_Collection_Pool
      ⊞ Object_Collection "2374"
      ⊞ Object_Collection "2373"
      ⊞ Object_Collection "2376"
      ⊞ Object_Collection "2372"
      ⊞ Object_Collection "2371"
```

MAEC → OVAL Translator Script

OVAL Output

```
oval_definitions "http://oval.mitre.org/XMLSchema/oval-d
⊟ generator MAEC XML to OVAL Script
   oval:product_name MAEC XML to OVAL Script
   oval:product_version 1.0
   oval:schema_version 5.7
   oval:timestamp 2010-11-08T09:26:33.347000
⊞ definitions
⊟ tests
   ⊞ win-def:file_test "oval:maec_out:tst:1"
   ⊞ win-def:file_test "oval:maec_out:tst:2"
   ⊞ win-def:file_test "oval:maec_out:tst:3"
   ⊞ win-def:file_test "oval:maec_out:tst:4"
   ⊞ win-def:file_test "oval:maec_out:tst:5"
   ⊞ win-def:file_test "oval:maec_out:tst:6"
   ⊞ win-def:registry_test "oval:maec_out:tst:7"
   ⊞ win-def:registry_test "oval:maec_out:tst:8"
   ⊞ win-def:registry_test "oval:maec_out:tst:9"
   ⊞ win-def:registry_test "oval:maec_out:tst:10"
⊟ objects
   ⊞ win-def:file_object "oval:maec_out:obj:1" C:\DO
   ⊞ win-def:file_object "oval:maec_out:obj:2" C:\Doc
   ⊞ win-def:file_object "oval:maec_out:obj:3" C:\Doc
   ⊞ win-def:file_object "oval:maec_out:obj:4" C:\Doc
   ⊞ win-def:file_object "oval:maec_out:obj:5" C:\Doc
   ⊞ win-def:file_object "oval:maec_out:obj:6" C:\Doc
   ⊞ win-def:registry_object "oval:maec_out:obj:7" H
   ⊞ win-def:registry_object "oval:maec_out:obj:8" H
   ⊞ win-def:registry_object "oval:maec_out:obj:9" H
   ⊞ win-def:registry_object "oval:maec_out:obj:10" I
```

*http://anubis.iseclab.org/?action=result&task_id=1167a57d1aa905e949df5d5478ab23bf9

MAEC & Malware Indicators/Signatures I

- MAEC 2.0 supports Boolean constructs around objects

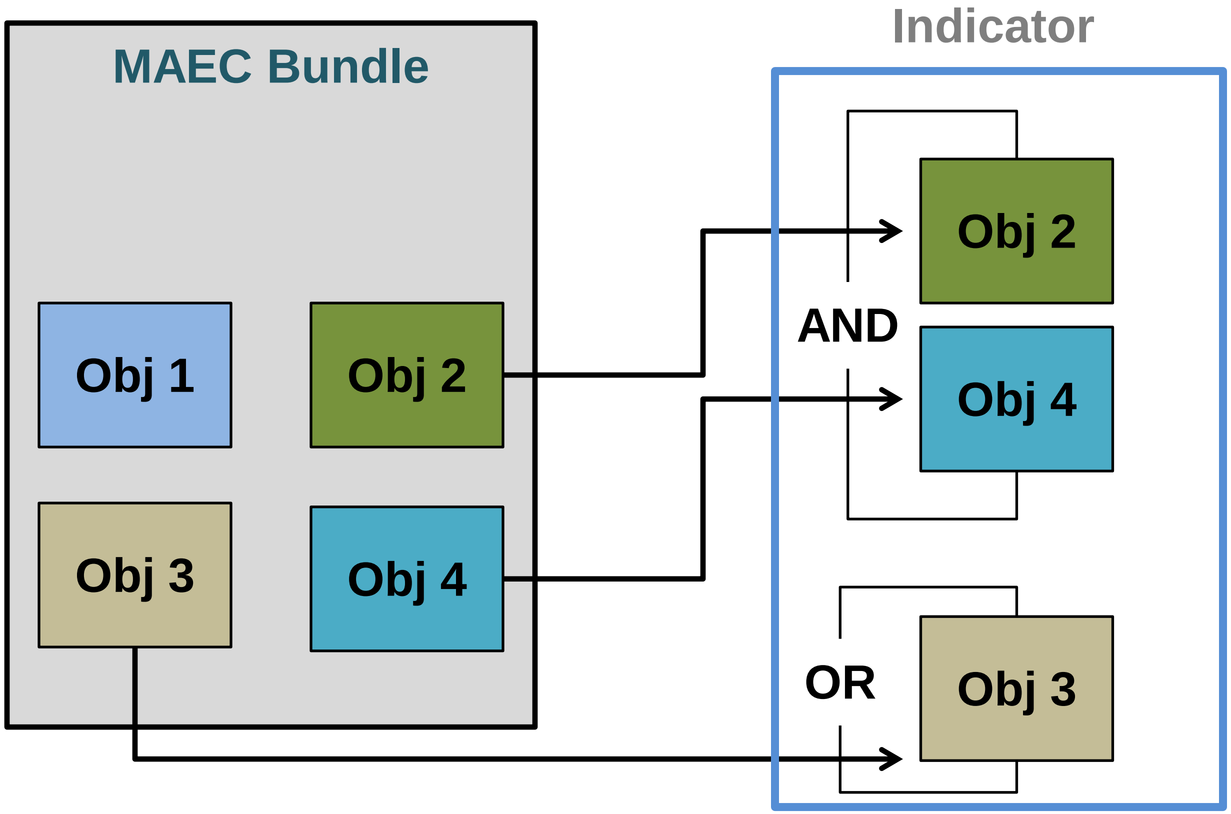
```
<maec:Object id="maec:tst:obj:1">
    <observables:Defined_Object xsi:type="fileObject:File_Object_Type">
     <fileObject:FilePath>C:\Windows\</fileObject:FilePath>
     <fileObject:FileName>wincom.dll</fileObject:FileName>
    </observables:Defined_Object>
  </maec:Object>
```

OR

```
<maec:Object id="maec:tst:obj:2">
    <observables:Defined_Object xsi:type="fileObject:File_Object_Type">
     <fileObject:FilePath>C:\Windows\System32</fileObject:FilePath>
     <fileObject:FileName>spooldr.dll</fileObject:FileName>
    </observables:Defined_Object>
  </maec:Object>
```

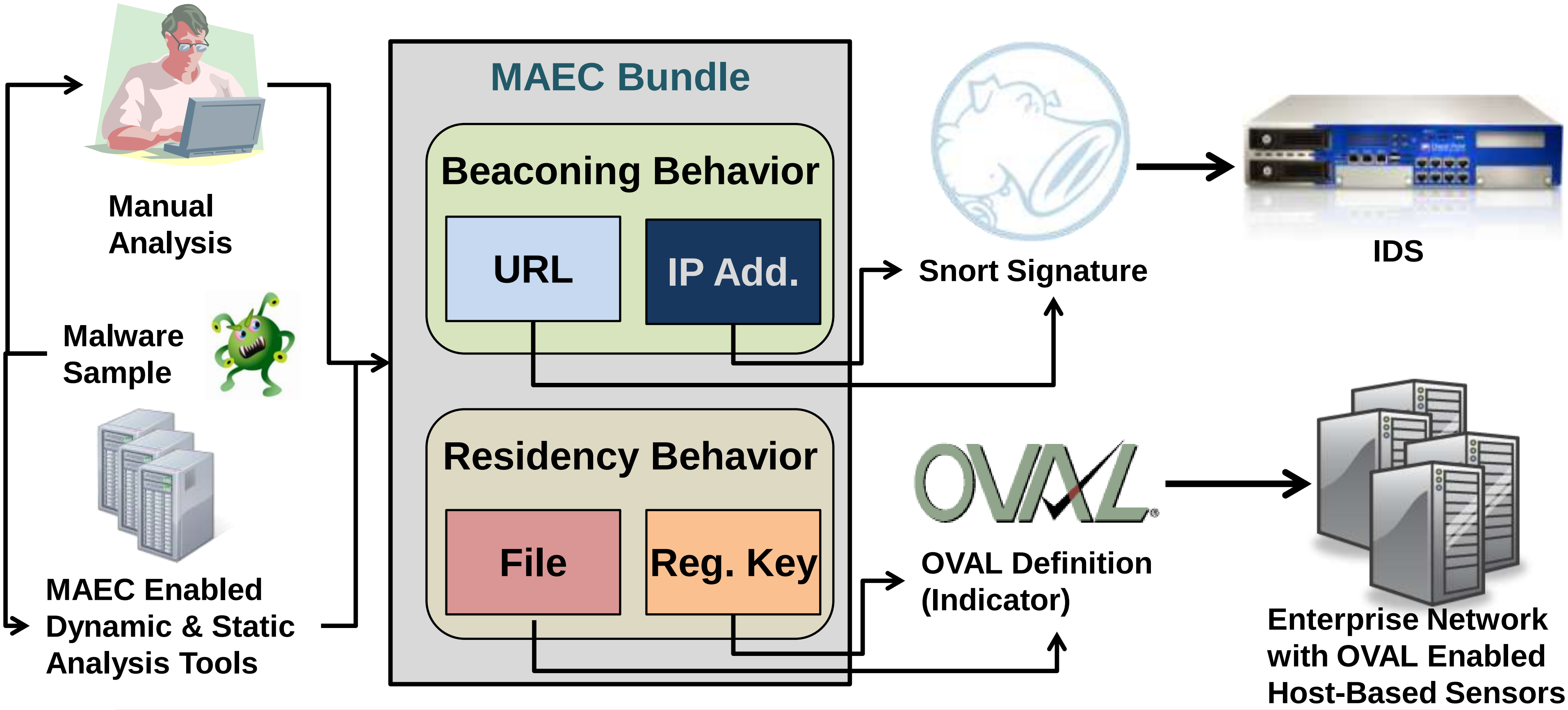
MAEC & Malware Indicators/Signatures II

- Permits construction of generic malware indicators
- Can be constructed from existing MAEC data (i.e. MAEC bundle)



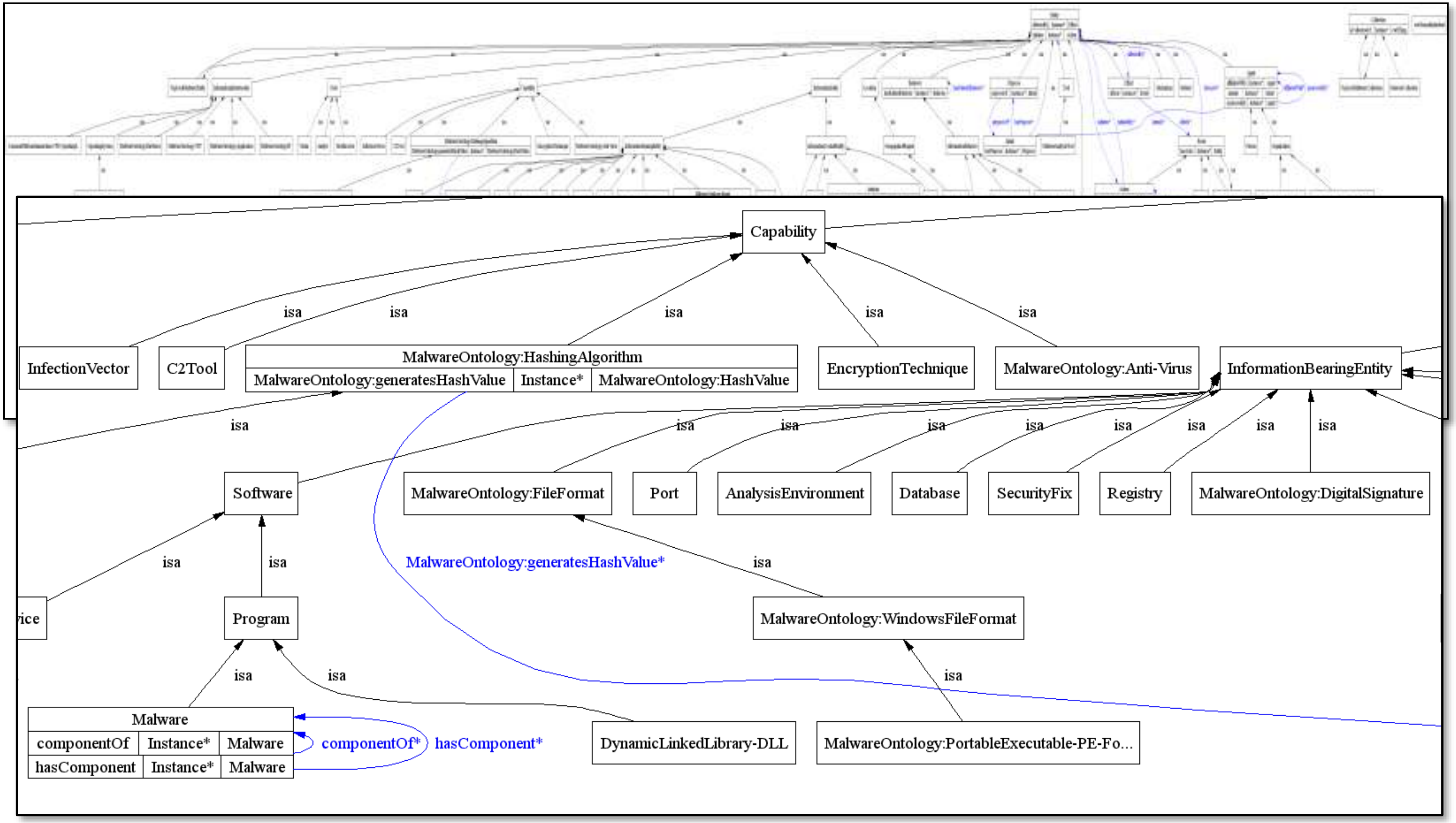
MAEC & Malware Indicators/Signatures III

- **MAEC enables comprehensive malware descriptions, allowing various components of a MAEC bundle to be used as signatures and indicators in the enterprise**

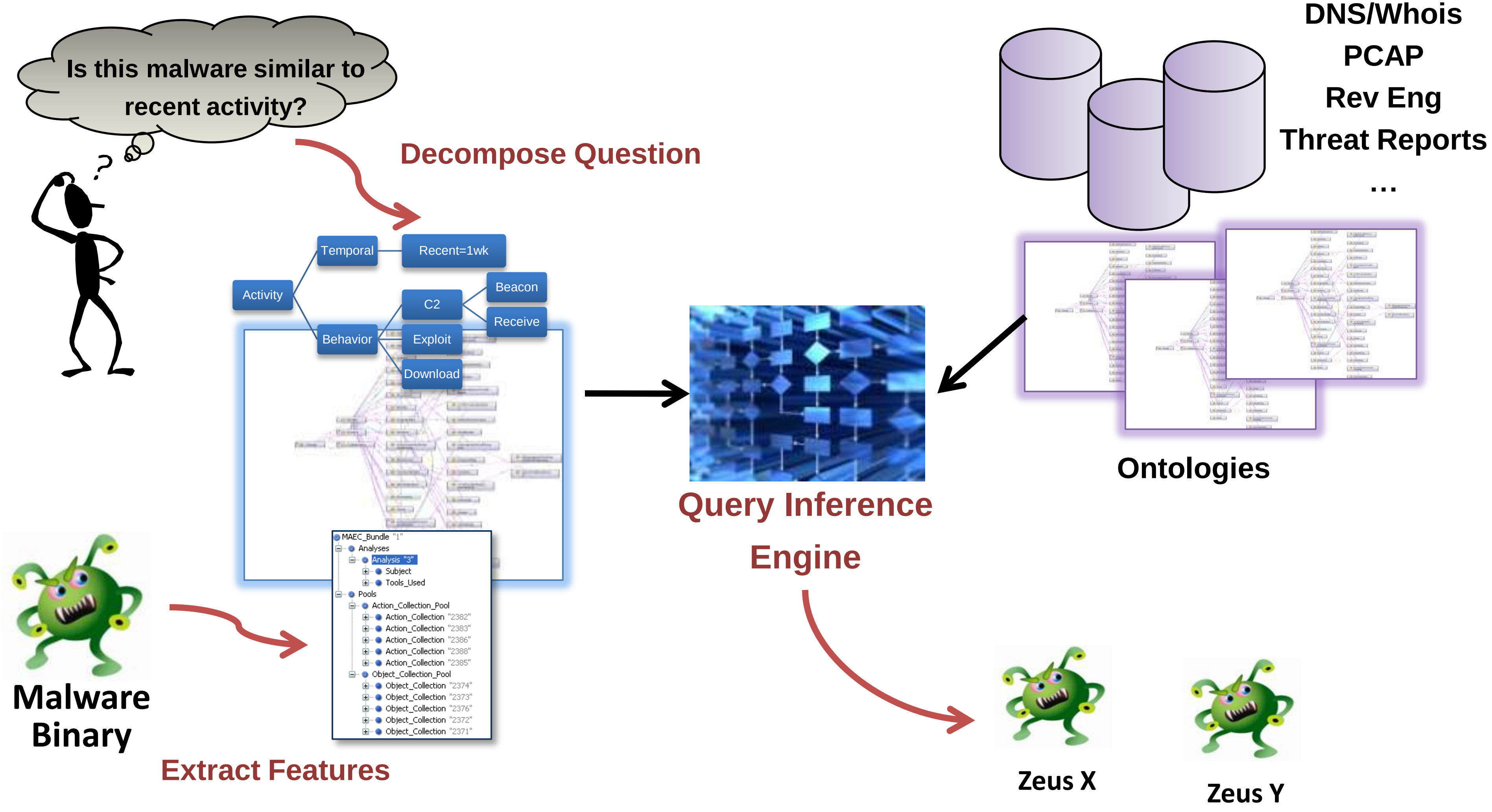

Manual Analysis
Malware Sample
MAEC Enabled Dynamic & Static Analysis Tools
MAEC Bundle
Beaconing Behavior
URL
IP Add.
Residency Behavior
File
Reg. Key
Snort Signature
IDS
OVAL
OVAL Definition (Indicator)
Enterprise Network with OVAL Enabled Host-Based Sensors

MÆC™ Future Directions

Malware Ontology (OWL)


Capability
isa
isa
isa
isa
isa
InfectionVector
C2Tool
MalwareOntology:HashingAlgorithm
MalwareOntology:generatesHashValue | Instance* | MalwareOntology:HashValue
EncryptionTechnique
MalwareOntology:Anti-Virus
InformationBearingEntity
isa
isa
isa
isa
isa
isa
isa
isa
isa
isa
Software
MalwareOntology:FileFormat
Port
AnalysisEnvironment
Database
SecurityFix
Registry
MalwareOntology:DigitalSignature
isa
isa
MalwareOntology:generatesHashValue*
isa
vice
Program
MalwareOntology:WindowsFileFormat
isa
isa
isa
Malware
componentOf | Instance* | Malware
hasComponent | Instance* | Malware
componentOf*
hasComponent*
DynamicLinkedLibrary-DLL
MalwareOntology:PortableExecutable-PE-Fo...

Use Case: Data Fusion & Correlation



Is this malware similar to recent activity?

Decompose Question

Activity

Temporal

Recent=1wk

Behavior

C2

Beacon

Receive

Exploit

Download

DNS/Whois

PCAP

Rev Eng

Threat Reports

…

Ontologies

Query Inference Engine

Malware Binary

Extract Features

```
MAEC_Bundle "1"
  Analyses
    Analysis "3"
      Subject
      Tools_Used
  Pools
    Action_Collection_Pool
      Action_Collection "2382"
      Action_Collection "2383"
      Action_Collection "2386"
      Action_Collection "2388"
      Action_Collection "2385"
    Object_Collection_Pool
      Object_Collection "2374"
      Object_Collection "2373"
      Object_Collection "2376"
      Object_Collection "2372"
      Object_Collection "2371"
```

Zeus X

Zeus Y

MITRE

Future Schema Work

- Expand Behavioral Characterization Capability
  - Add conditional constructs
  - Refine to make more amenable to human construction
- Expand effects types, object types, action types
- Add generic signature type
  - Based on CIDSS?
- Continuously refine based on user feedback
  - Feedback loop!

MAEC & IEEE ICSG

- IEEE Industry Connections Security Group (ICSG)
  - Malware Working Group developed an exchange schema to facilitate the sharing of sample data between AV product vendors
      - MAEC imports the IEEE ICSG Malware Metadata exchange schema
  - Recently established Malware Metadata Exchange Format WG
    - Initial Focus:
      - Adding capability to MMDEF schema for profiling clean (non-malicious) files, including software packages
      - Aimed at sharing information about clean files for reducing AV detection false positives
    - Primary Focus:
      - Adding capability to MMDEF schema for capturing blackbox behavioral metadata about malware
      - Will likely import MAEC/CybOX, especially MAEC Objects and Actions
    - Potentially transition to a new IEEE standard

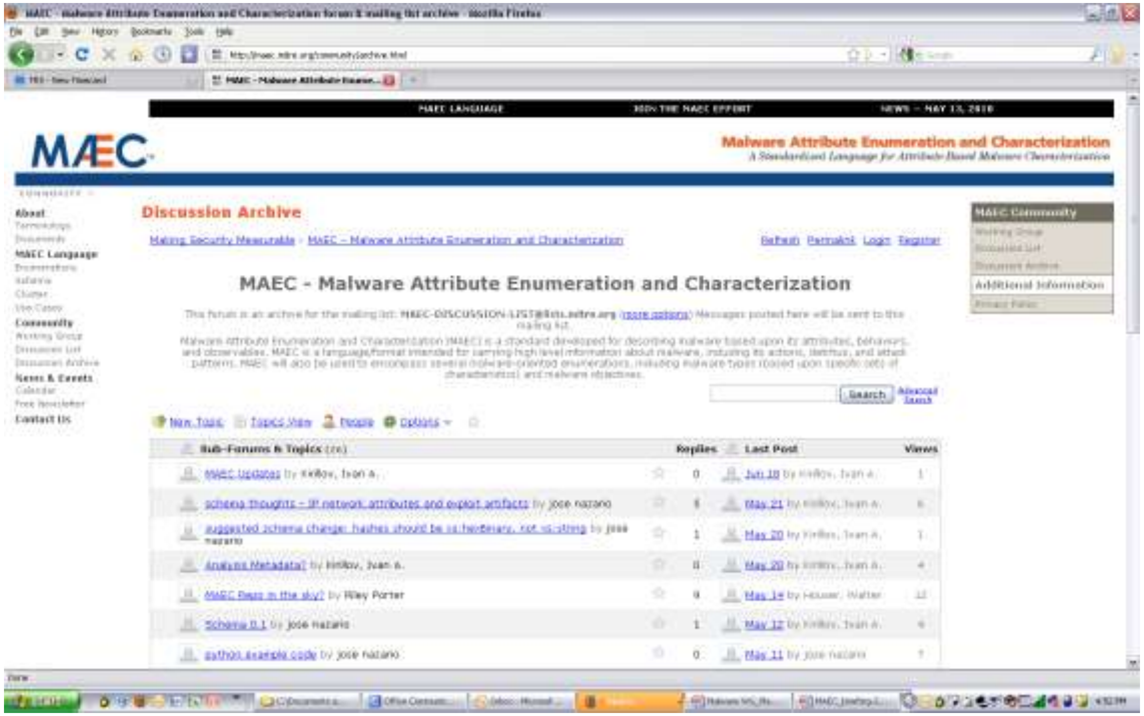
MÆC™ Community Outreach

Community Engagement

- Industry Collaborations
  - Working with Mandiant on MAEC <-> openIOC
  - Tool vendors supported our development of MAEC translators:
    - CWSandbox : GFI Software
    - ThreatExpert : Symantec
    - Anubis : International Secure Systems (Isec) Lab
  - Discussions with tool vendors about adopting MAEC as a native output format (under NDAs)
  - Malware analysts experimenting with MAEC (e.g., to compare multiple tool output)
  - Several organizations prototyping using MAEC as a common malware analysis storage format

MAEC Community: Discussion List

- Request to join: http://maec.mitre.org/community/discussionlist.html
- Archives available



MAEC - Malware Attribute Enumeration and Characterization forum & mailing list archive - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://maec.mitre.org/community/archive.html
MAEC - Malware Attribute Enume...
MAEC LANGUAGE
JOIN THE MAEC EFFORT
NEWS – MAY 13, 2010
MAEC
Malware Attribute Enumeration and Characterization
A Standardized Language for Attribute-Based Malware Characterization
About
Terminology
Documents
MAEC Language
Documentation
Schema
Charter
Use Cases
Community
Working Group
Discussion List
Discussion Archive
News & Events
Calendar
Free Newsletter
Contact Us
MAEC Community
Working Group
Discussion List
Discussion Archive
Additional Information
Privacy Policy
Making Security Measurable › MAEC – Malware Attribute Enumeration and Characterization
Refresh Permalink Login Register
Search
Advanced Search
New Topic
Topics View
People
Options

Discussion Archive

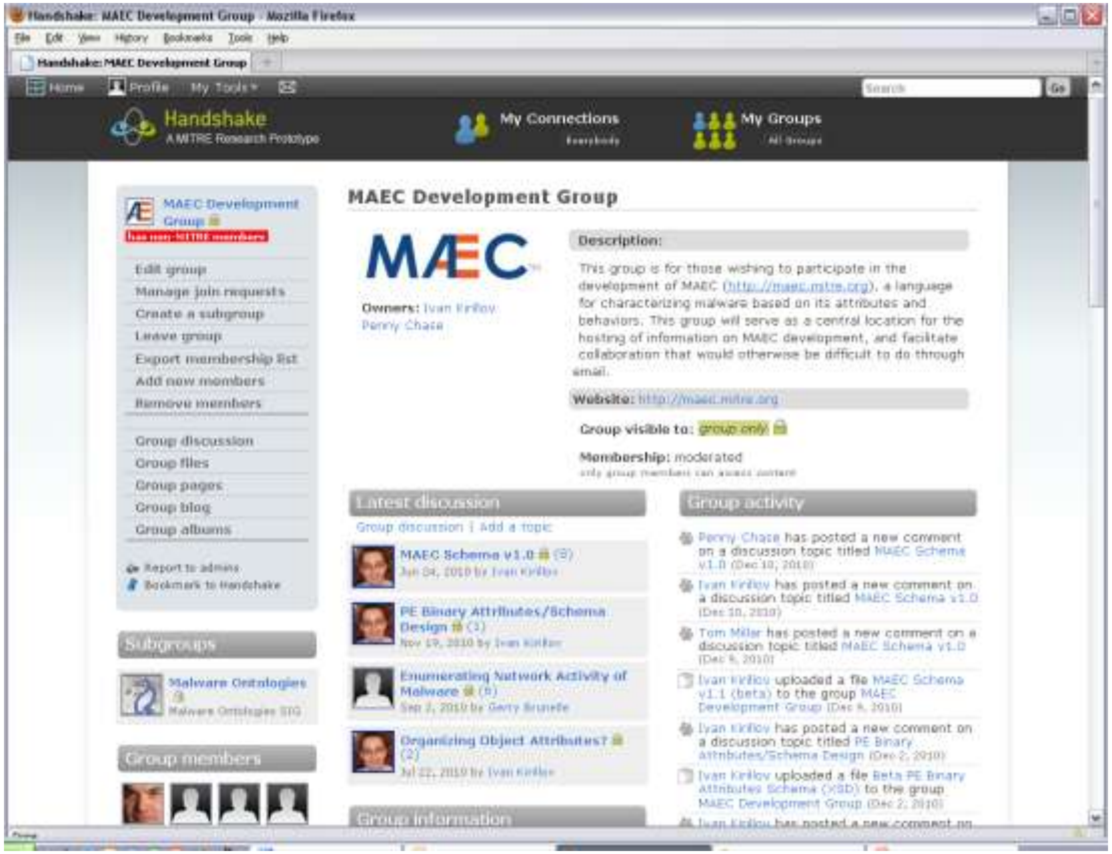
MAEC - Malware Attribute Enumeration and Characterization

This forum is an archive for the mailing list: MAEC-DISCUSSION-LIST@lists.mitre.org (more options) Messages posted here will be sent to this mailing list.

Malware Attribute Enumeration and Characterization (MAEC) is a standard developed for describing malware based upon its attributes, behaviors, and observables. MAEC is a language/format intended for carrying high level information about malware, including its actions, [illegible], and attack patterns. MAEC will also be used to encompass several malware-oriented enumerations, including malware types (based upon specific sets of characteristics) and malware objectives.

Sub-Forums & Topics (26)	Replies	Last Post	Views
MAEC Updates by Kirillov, Ivan A.	0	Jun 18 by Kirillov, Ivan A.	1
schema thoughts – IP network attributes and exploit artifacts by jose nazario	5	May 21 by Kirillov, Ivan A.	6
suggested schema change: hashes should be xs:hexBinary, not xs:string by jose nazario	1	May 20 by Kirillov, Ivan A.	1
Analysis Metadata? by Kirillov, Ivan A.	0	May 20 by Kirillov, Ivan A.	4
MAEC Repo in the sky? by Riley Porter	9	May 14 by Heuser, Walter	12
Schema 0.1 by jose nazario	1	May 12 by Kirillov, Ivan A.	6
python example code by jose nazario	0	May 11 by jose nazario	7

MAEC Community: MAEC Development Group on Handshake



MAEC Development Group

Owners: Ivan Kirillov, Penny Chase

Description:

This group is for those wishing to participate in the development of MAEC (http://maec.mitre.org), a language for characterizing malware based on its attributes and behaviors. This group will serve as a central location for the hosting of information on MAEC development, and facilitate collaboration that would otherwise be difficult to do through email.

Website: http://maec.mitre.org

Group visible to: group only

Membership: moderated
only group members can access content

Latest discussion

- MAEC Schema v1.0 (8)
  Jun 04, 2010 by Ivan Kirillov
- PE Binary Attributes/Schema Design (1)
  Nov 19, 2010 by Ivan Kirillov
- Enumerating Network Activity of Malware (5)
  Sep 2, 2010 by Gerry Brunelle
- Organizing Object Attributes? (2)
  Jul 22, 2010 by Ivan Kirillov

Group activity

- Penny Chase has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 10, 2010)
- Ivan Kirillov has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 10, 2010)
- Tom Miller has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 9, 2010)
- Ivan Kirillov uploaded a file MAEC Schema v1.1 (beta) to the group MAEC Development Group (Dec 9, 2010)
- Ivan Kirillov has posted a new comment on a discussion topic titled PE Binary Attributes/Schema Design (Dec 2, 2010)
- Ivan Kirillov uploaded a file Beta PE Binary Attributes Schema (XSD) to the group MAEC Development Group (Dec 2, 2010)
- Ivan Kirillov has posted a new comment on

- MITRE hosts a social networking collaboration environment: https://handshake.mitre.org
- Supplement to mailing list to facilitate collaborative schema development
- Malware Ontologies SIG Subgroup

MAEC Community: MAEC Handshake Development Group Resources

- Anubis → MAEC Translator (Python)
- ThreatExpert → MAEC Translator (Python)
- MAEC → OVAL Translator (Python)
- MAEC → HTML Transform (XSL)
- MAEC Comparator Script (Python)
  - Provided by Blake Hartstein

Summary

- MAEC is attempting to address many of the issues that are integral to accurate and unambiguous communication about malware

- The adoption of MAEC will facilitate new methods of correlation and automation against malware

- MAEC is an open, collaborative effort. It needs expertise and input from various parties in order to be successful

Questions?

http://maec.mitre.org