Penny Chase

(Sean Barnum, Desiree Beck, Ivan Kirillov, Bob Martin)

26 March 2012

MITRE

© 2012 The MITRE Corporation. All rights reserved.

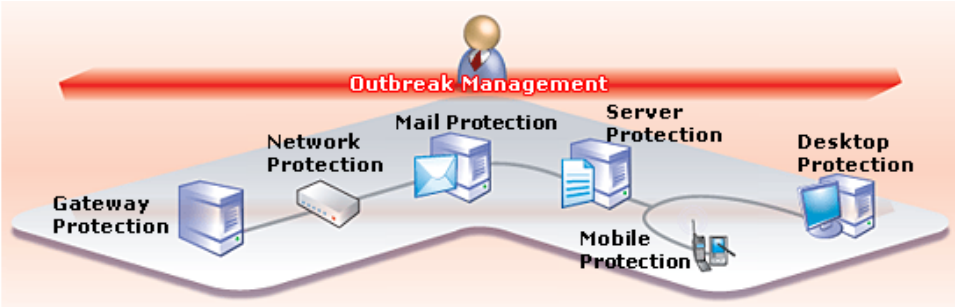
Agenda

- Overview
- MAEC V 2.0 Changes
- Use Cases:
  - Malware Triage and Analysis
  - Malware Detection
- Community Outreach
- Future Directions

© 2012 The MITRE Corporation. All rights reserved.

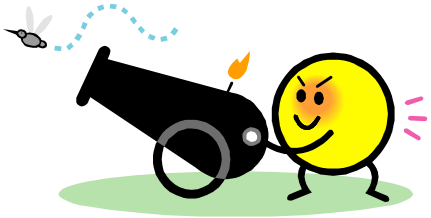
Why Do We Need to Develop Standards for Malware?

Multiple layers of protection



Lots of products

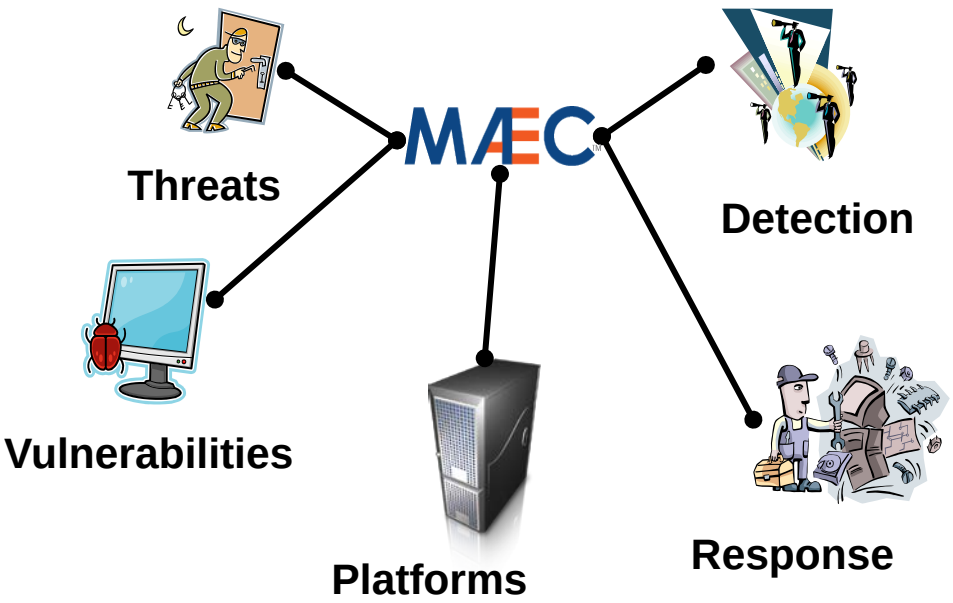
Inconsistent reports



There's an arms race

© 2012 The MITRE Corporation. All rights reserved.

Malware Attribute Enumeration and Characterization (MAEC)

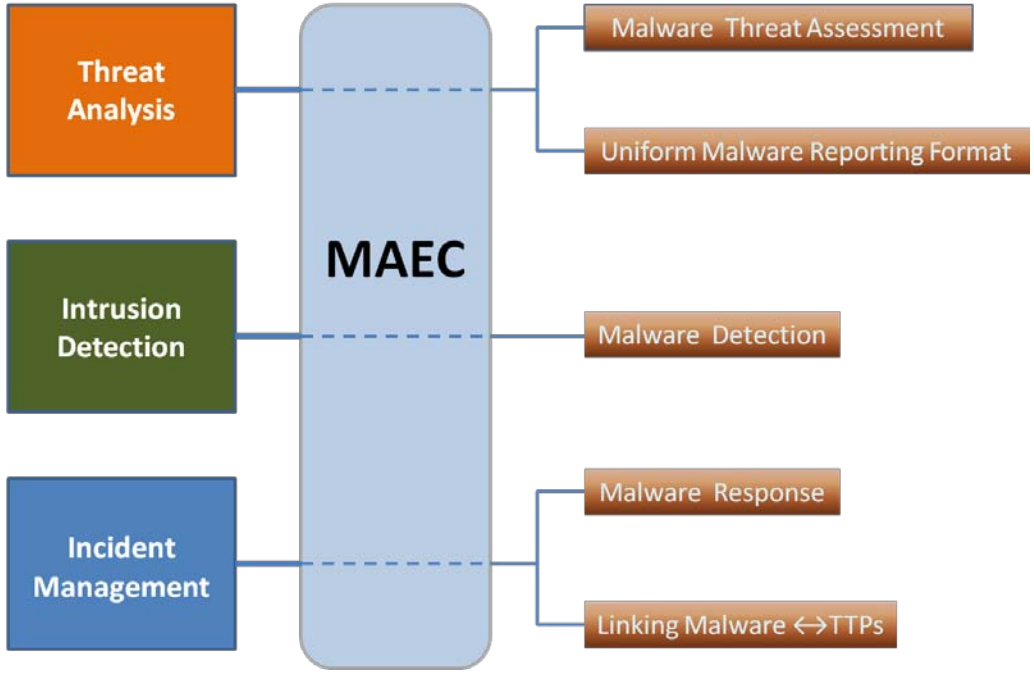


- Language for sharing structured information about malware
  - Grammar (Schema)
  - Vocabulary (Enumerations)
  - Collection Format (Bundle)
- Focus on attributes and behaviors
- Enable correlation, integration, and automation

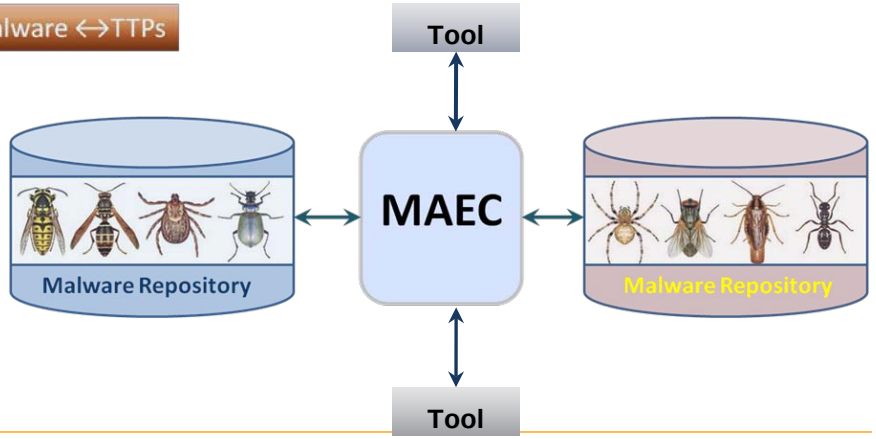
© 2012 The MITRE Corporation. All rights reserved.

MAEC Use Cases

- **Operational**



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



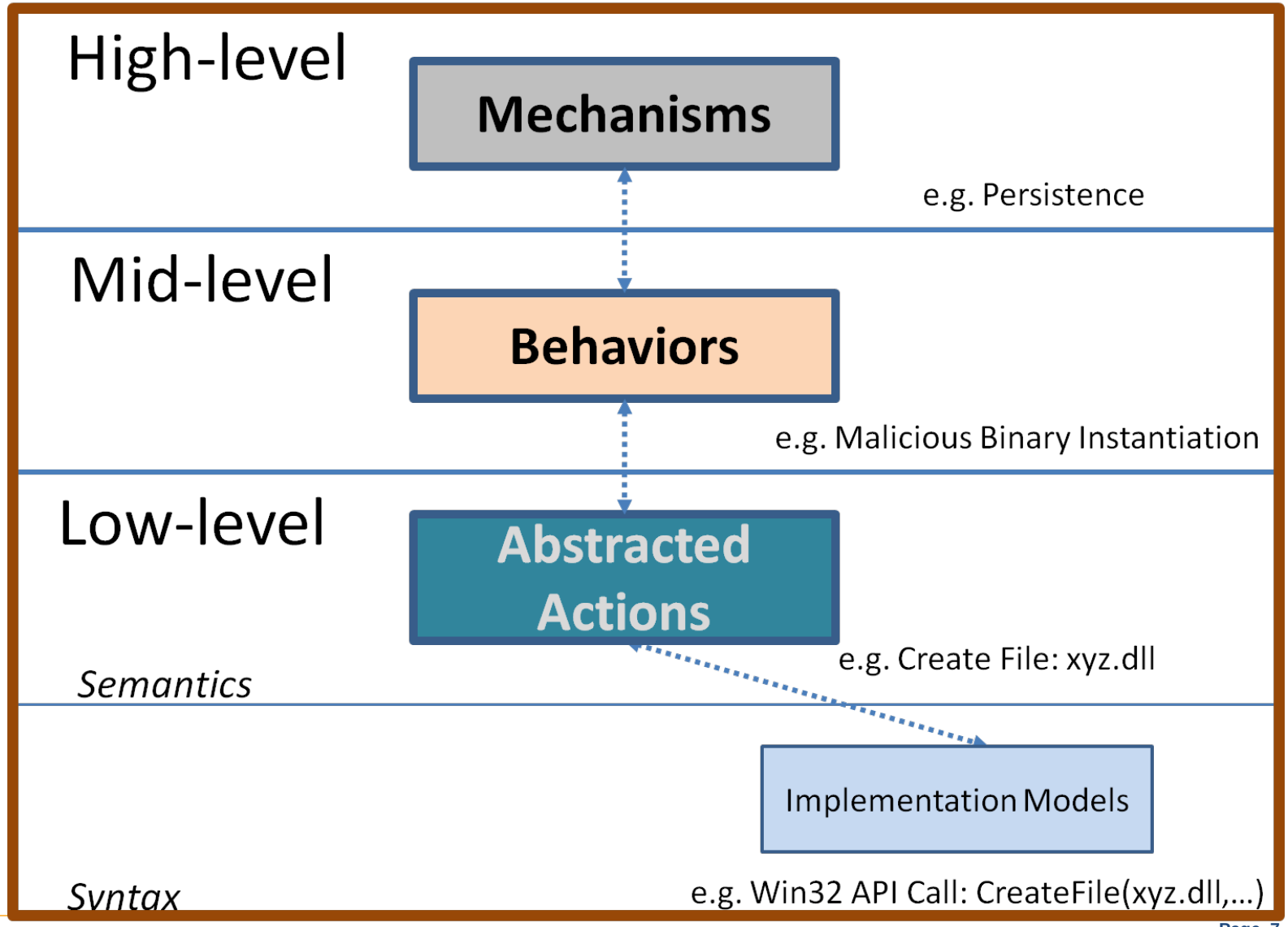
© 2012 The MITRE Corporation. All rights reserved.

MAEC Development

- Collaboration between industry and government
- Leverage existing resources, such as
  - IEEE Industry Connections Security Group's Malware Metadata Exchange Format schema v 1
  - Mandiant's openIOC
  - Government malware metadata requirements
- Participate in standards efforts
  - IEEE ICSG Malware Metadata Exchange Format WG
    - Adding capability to MMDEF schema for capturing blackbox behavioral metadata about malware
    - Will likely import MAEC/CybOX, especially MAEC Objects and Actions
  - IETF Managed Incident Lightweight Exchange (MILE) WG
    - MAEC will be part of the MILE Structured Cybersecurity Information RFC (extensions to IODEF)

© 2011 The MITRE Corporation. All rights reserved.

MAEC Structure Overview



© 2012 The MITRE Corporation. All rights reserved.

MAEC v 2.0

- XSD Schema Evolution
  - 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 – January 2012
    - MAEC object model replaced with CybOX
    - ActionType simplified
    - EffectType refined
    - Lots of ‘under the hood’ tweaks and minor additions

© 2012 The MITRE Corporation. All rights reserved.

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.**

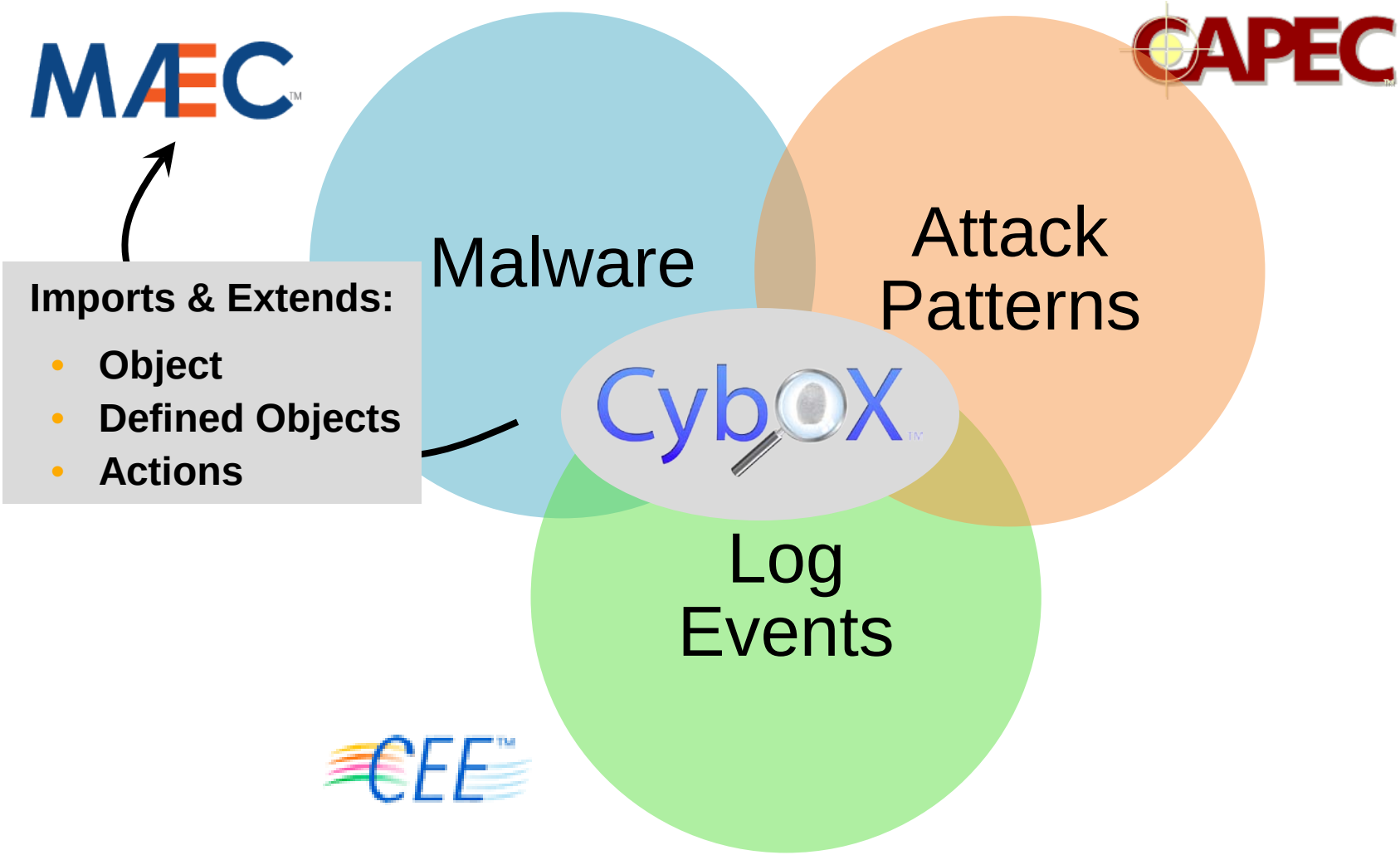
- **Many new enumerated types**
  - **Actions, Effects, Relationships, etc.**

© 2012 The MITRE Corporation. All rights reserved.

CybOX™

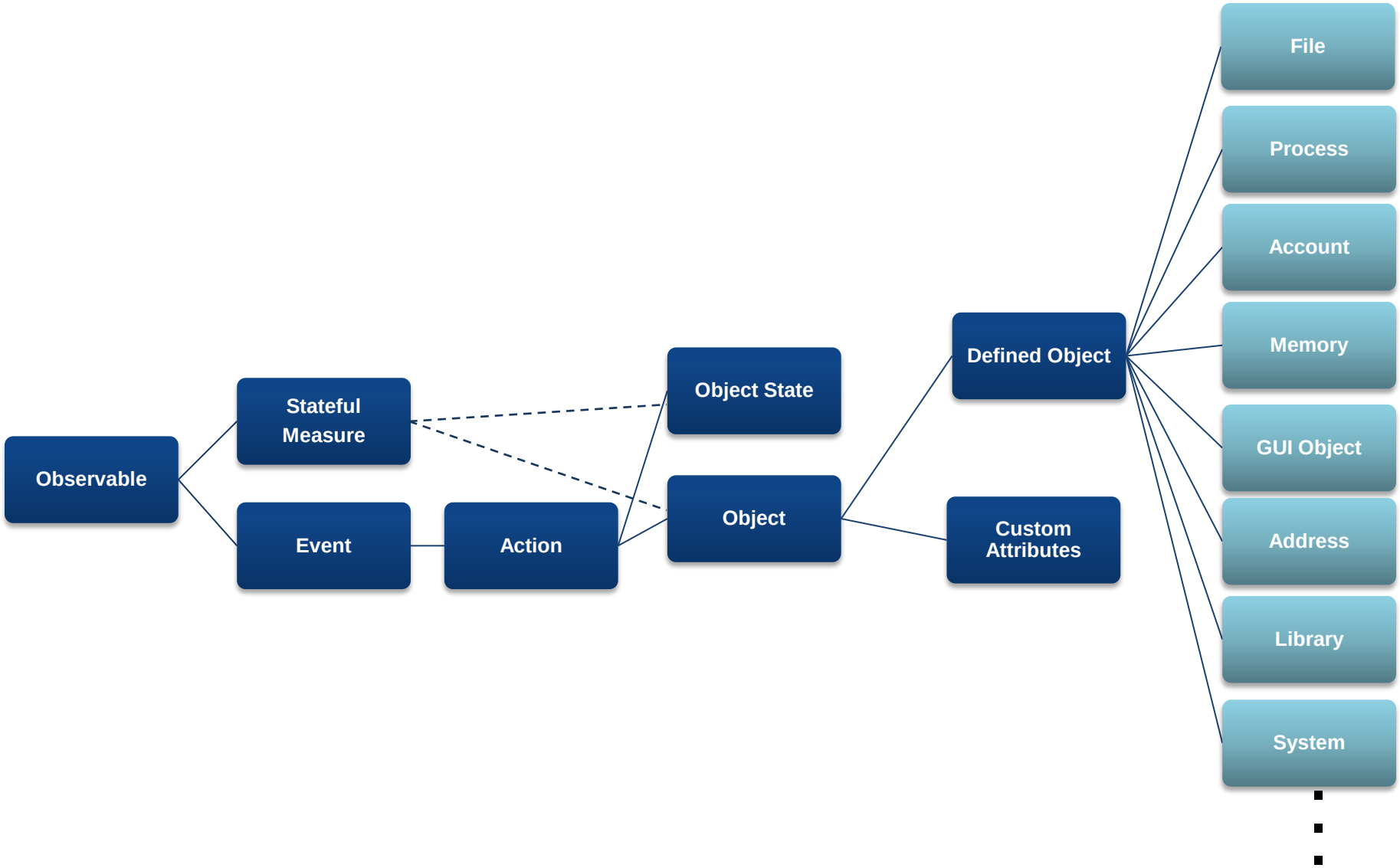
- What is a cyber observable?
  - a measurable event or stateful property in the cyber domain
    - Some measurable events: a registry key is created, a file is deleted, an http GET is received, …
    - Some stateful properties: MD5 hash of a file, value of a registry key, existence of a mutex, …
- Cyber Observable eXpression (CybOX) is a standardized language for encoding and communicating information about cyber observables
- Supports a wide range of use cases, e.g.
  - Detection and indicator generation
  - Sharing of information about incidents, malware, etc.
  - Correlation

© 2011 The MITRE Corporation. All rights reserved.



© 2011 The MITRE Corporation. All rights reserved.

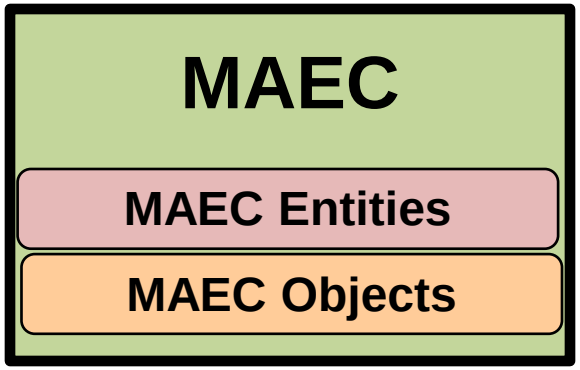
Cyber Observable eXpression (CybOX) Schema Simple Overview



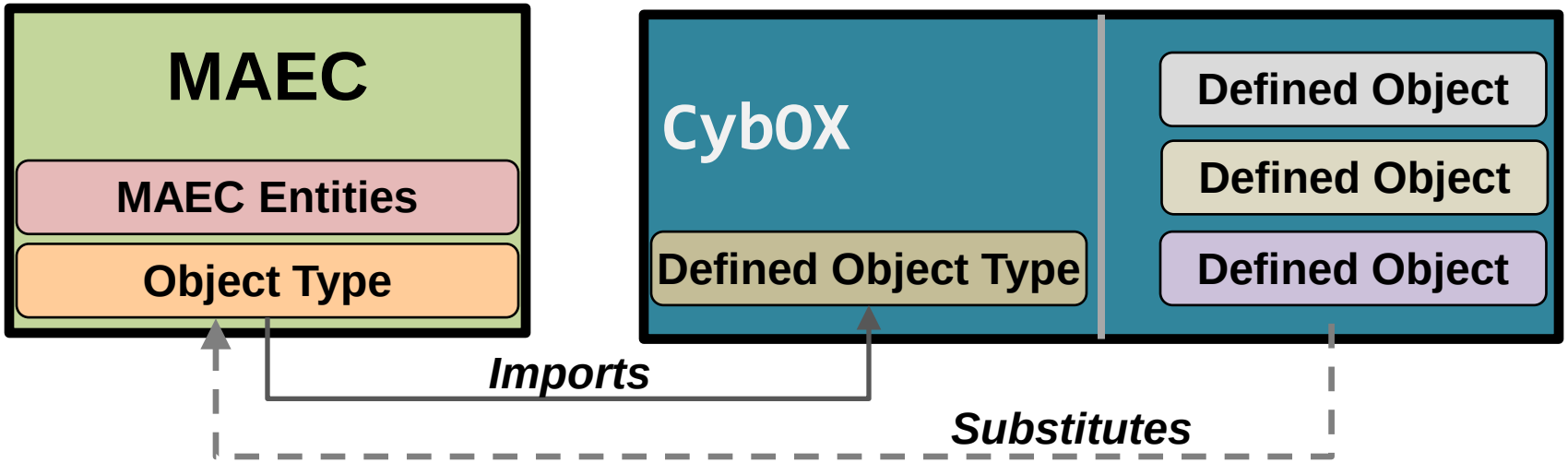
© 2011 The MITRE Corporation. All rights reserved.

MAEC & CybOX

- Before (MAEC 1.x)



- After (MAEC 2.0 and up)



© 2011 The MITRE Corporation. All rights reserved.

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)

© 2011 The MITRE Corporation. All rights reserved.

MAEC v2.0 Objects (imported from CybOX 0.7)

- 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)

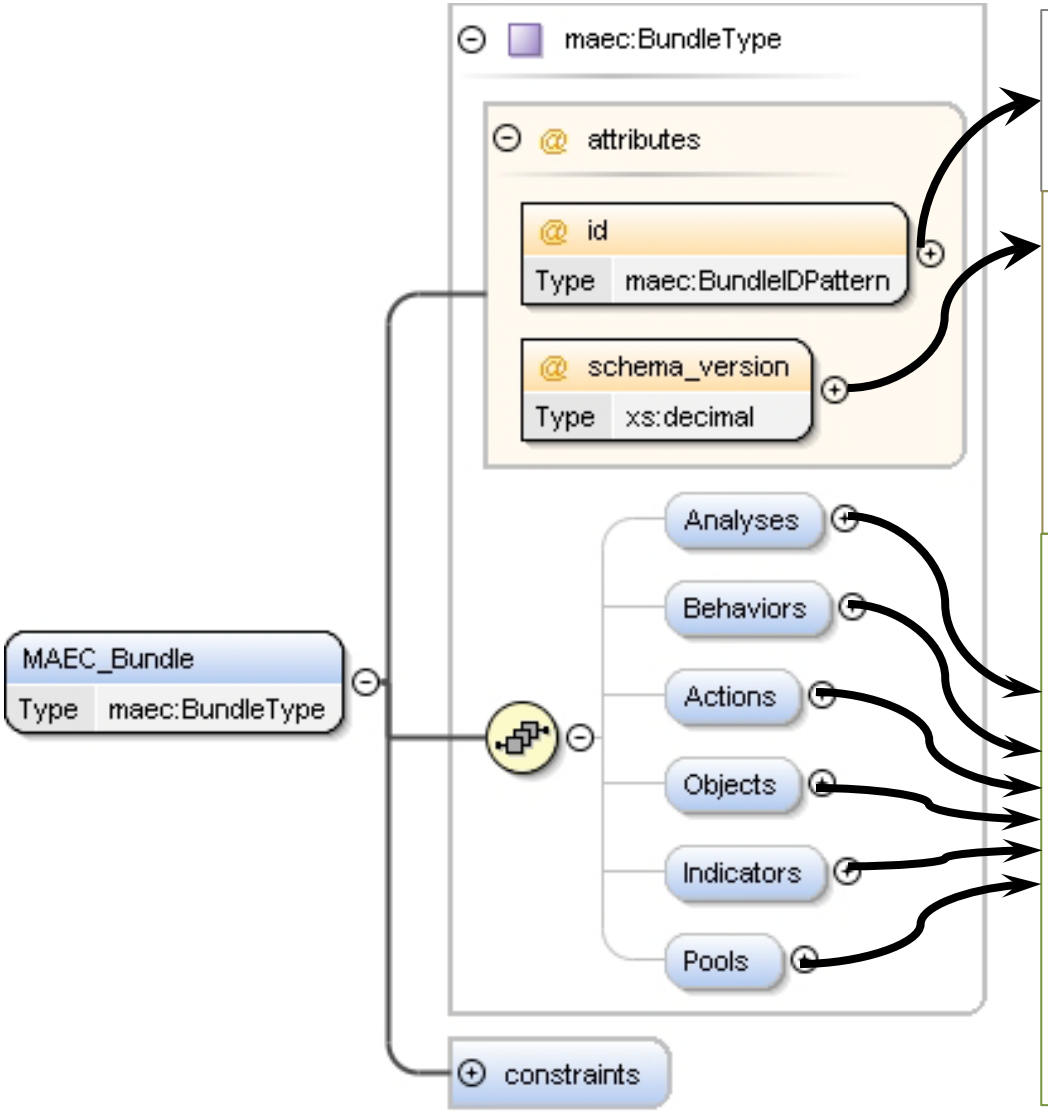
© 2011 The MITRE Corporation. All rights reserved.

MAEC™ Use Cases

- Malware Triage & Analysis
- Malware Detection

© 2011 The MITRE Corporation. All rights reserved.

MAEC's Bundle



MAEC Bundle ID

- Globally unique identifier

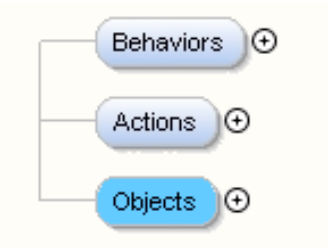
Schema Version

- Version of schema used to create bundle
- Used for validation

MAEC Components

- Attributes and metadata of a particular malware instance, family, class, etc.
- All optional
- Identified through various forms of malware analysis

© 2011 The MITRE Corporation. All rights reserved.

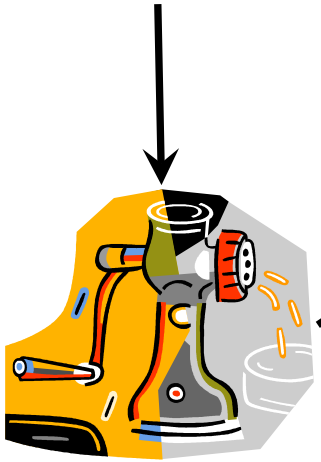


MAEC & Malware Analysis Process I

Stage One: Pre-Screen / StaticTriage

11010101001

Malware Binary (PE)



1. Imports
   Exports
   Resources
   Strings
   etc

2.
```
<maec:Object id="maec:tst:obj:1">
...
</maec:Object>
```

3.

MAEC Bundle

Behaviors

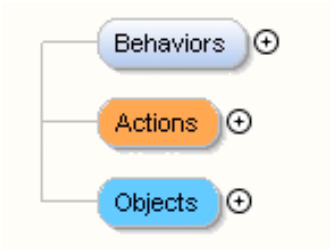
Actions

Objects

Obj 1

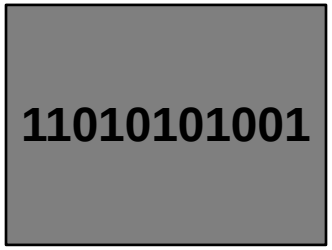
1. Features Extracted
2. MAEC Object Created
3. Object Added to Bundle

© 2011 The MITRE Corporation. All rights reserved.



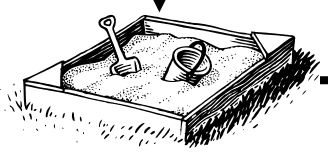
MAEC & Malware Analysis Process II

Stage Two: Dynamic Analysis Triage



Malware Binary

1.



2.

Files Created:

C:\Temp\loader.exe

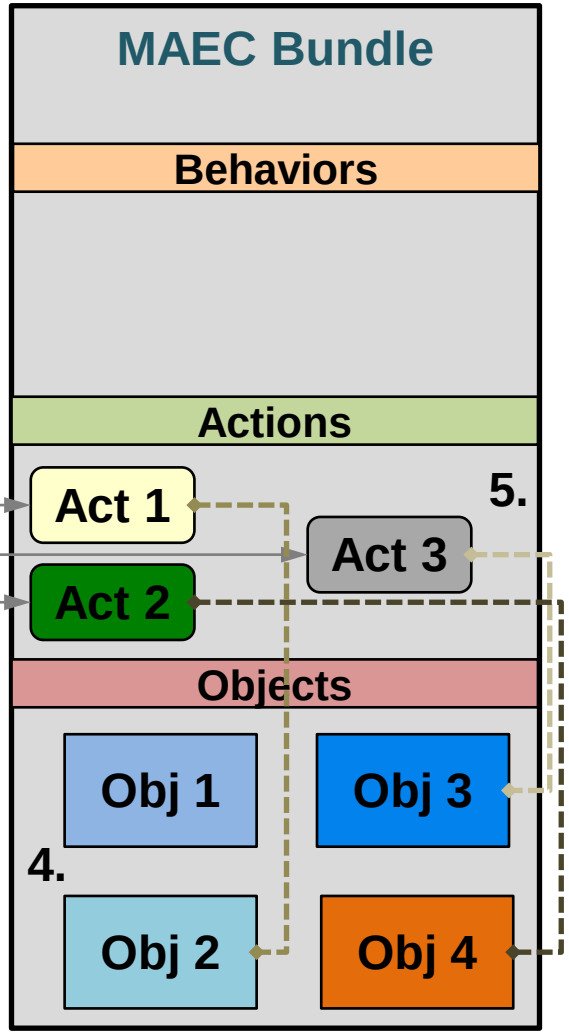
C:\Windows\rtkit.dll

Registry Key/Value Created:

Key: *…\Programs\Startup*

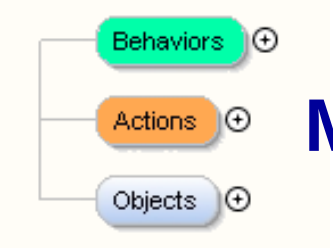
Value: *…\loader.exe*

3.



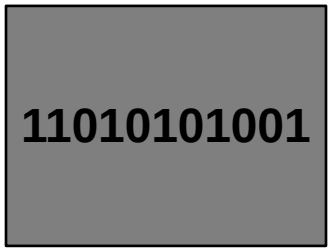
1. Malware Executed on Sandbox
2. Execution Report Generated
3. Actions Added
4. Objects Added
5. Action/Object Relationships Added

© 2011 The MITRE Corporation. All rights reserved.



MAEC & Malware Analysis Process III

Stage Three: In-depth Manual Analysis



Malware Binary

1.

2. Actions:

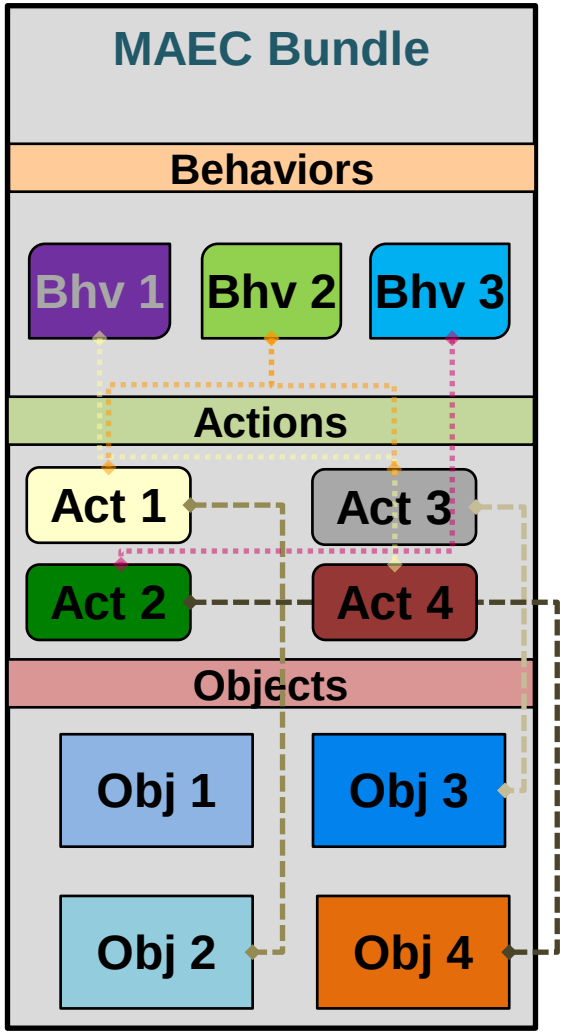
Start Winsock

3. Behaviors:

Winsock Startup

Malicious Binary Instantiation

Registry Persistence



1. Malware Analyzed Manually
2. New Actions Extracted and Added
3. Behaviors Extracted and Added

© 2011 The MITRE Corporation. All rights reserved.

MAEC™ Use Cases

Malware Triage & Analysis
Malware Detection

© 2011 The MITRE Corporation. All rights reserved.

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>
```

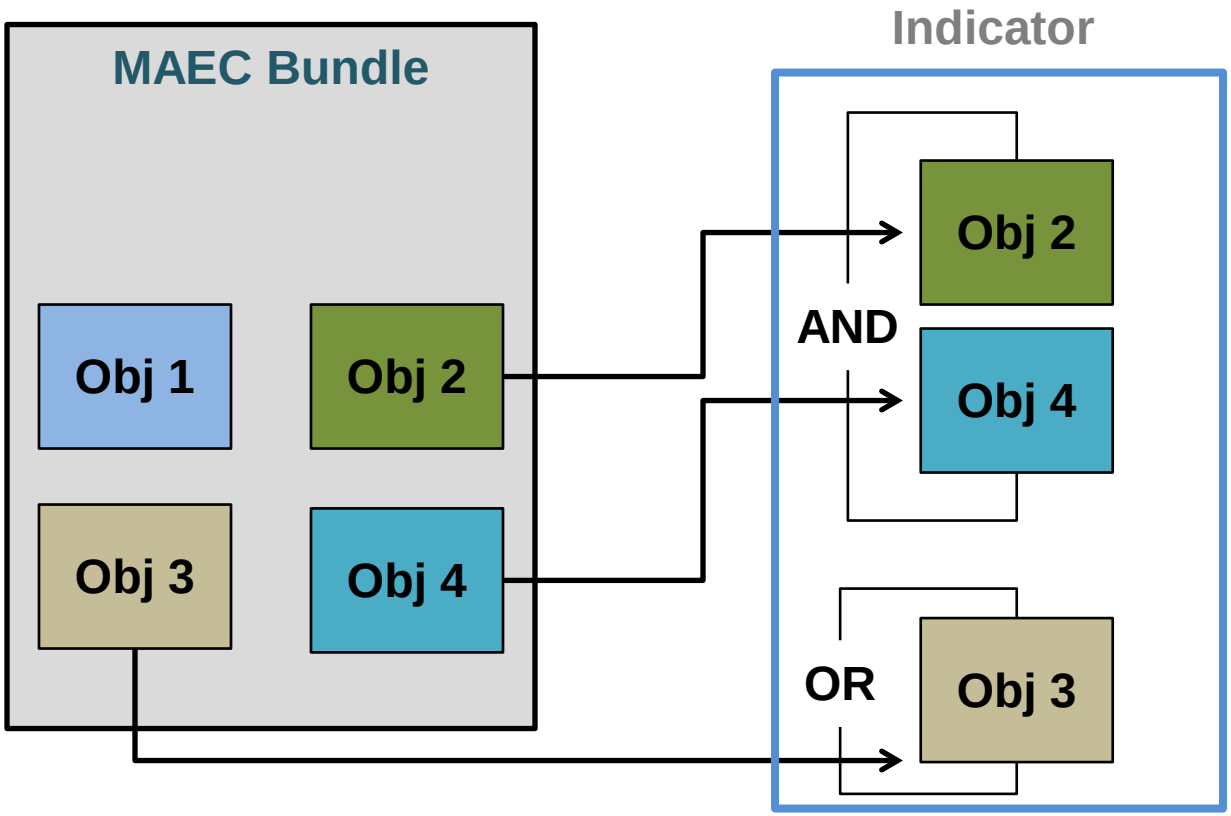
OR

```
<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>
```


© 2011 The MITRE Corporation. All rights reserved.

MAEC & Malware Indicators/Signatures II

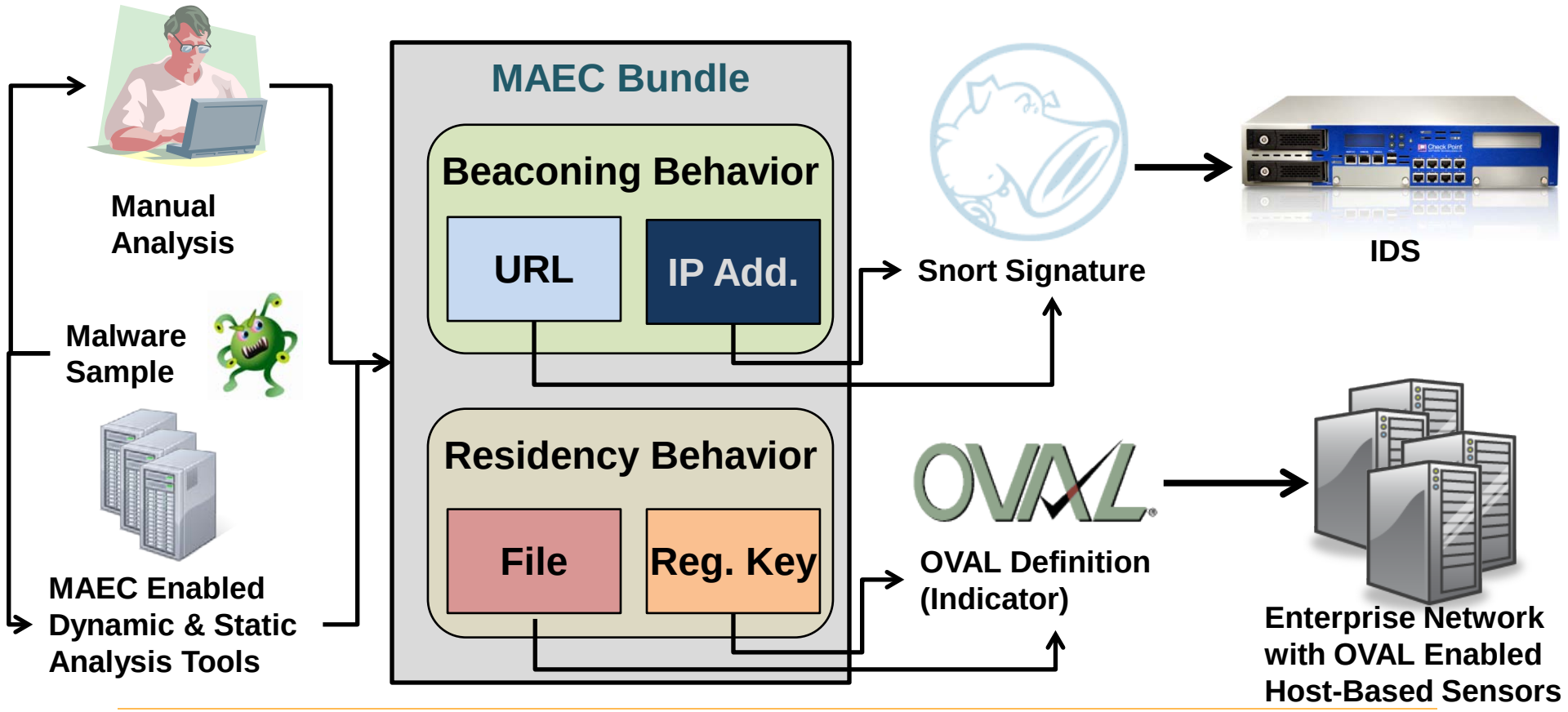
- Permits construction of generic malware indicators
- Can be constructed from existing MAEC data (i.e. MAEC bundle)



© 2011 The MITRE Corporation. All rights reserved.

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



© 2011 The MITRE Corporation. All rights reserved.

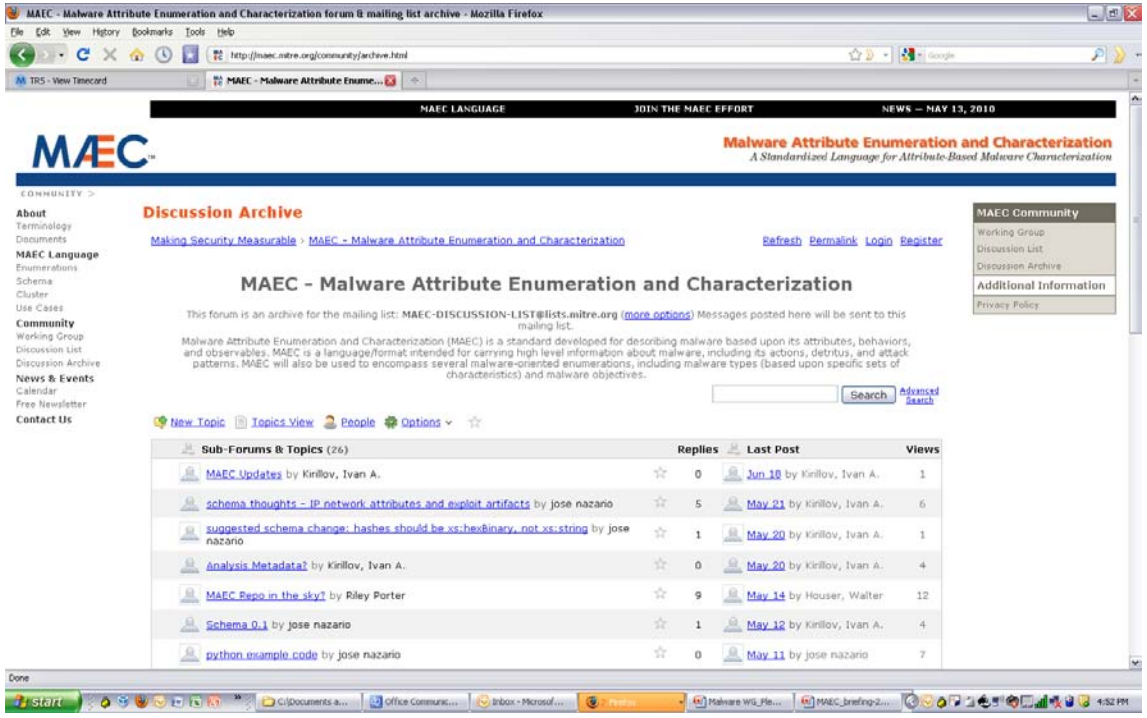
Industry Outreach and Collaboration

- Tool vendors supported our development of MAEC translators:
  - GFI Sandbox : GFI Software
  - ThreatExpert : Symantec
  - Anubis : International Secure Systems (Isec) Lab
  - FireEye (in process)
- Discussions with tool vendors about adopting MAEC as a native output format (e.g., GFI, Norman, FireEye)
- Open Source projects
  - Honeynet.org honeyclient project (thug)
  - Cuckoobox sandbox
- Organizations using MAEC internally to compare multiple tool output, as a common malware analysis storage format, etc.

© 2012 The MITRE Corporation. All rights reserved.

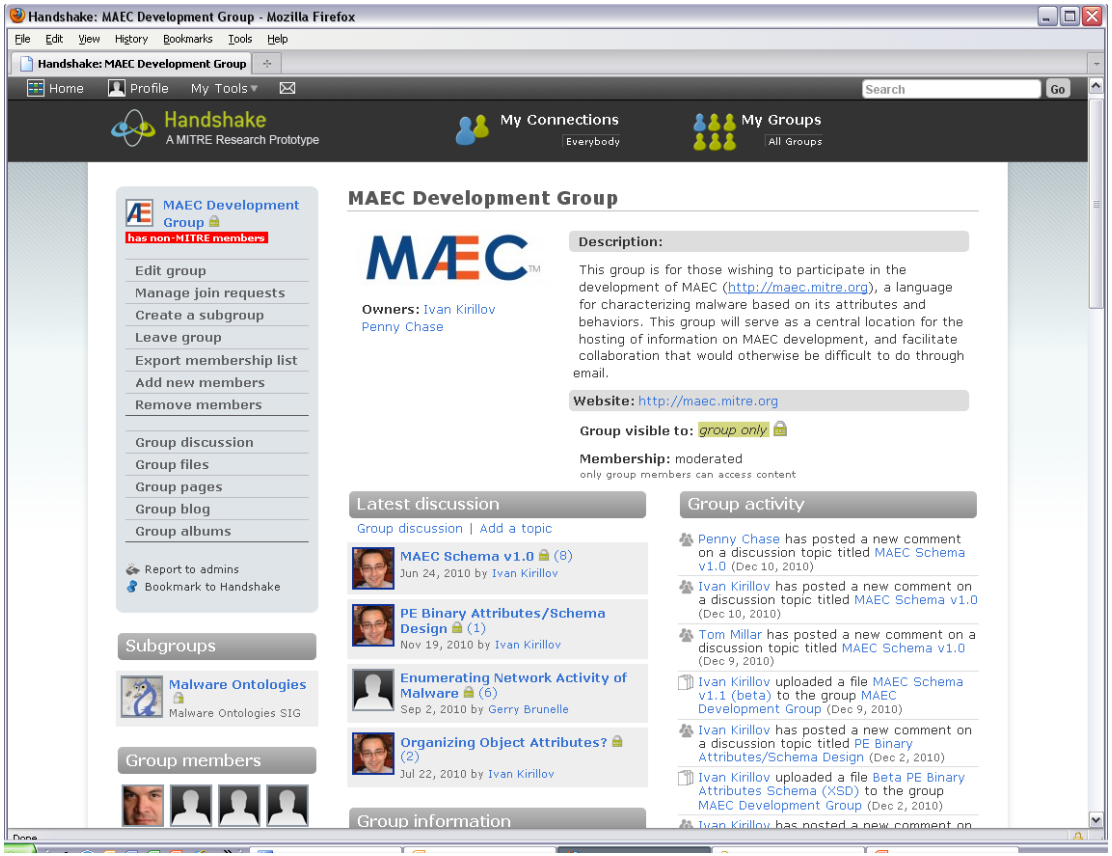
MAEC Community: Discussion List

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



© 2012 The MITRE Corporation. All rights reserved.

MAEC Community: MAEC Development Group on Handshake



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

© 2012 The MITRE Corporation. All rights reserved.

MAEC Development Resources

- Resources
  - Python bindings for schema elements
  - Prototype utilities (to provide examples of working with MAEC)
    - Anubis → MAEC Translator (Python)
    - ThreatExpert → MAEC Translator (Python)
    - Pefile.py → MAEC Generator (Python)
    - MAEC → OVAL Translator (Python)
    - MAEC → HTML Transform (XSL)
    - MAEC Comparator Script (Python)
      - Provided by Blake Hartstein
- Availaiblity
  - Handshake MAEC Development Group
  - Github (coming soon)

© 2012 The MITRE Corporation. All rights reserved.

MAEC Roadmap

V 1.1
- Dynamic Analysis
- Screening /Static Analysis

Jan 2011

V 2.0
- Incorporates CybOX 0.7
- Relationships
- Indicator management

Jan 2012

V 2.1
- Incorporates CybOX 1.0 (adds network objects)

Apr 2012

V 2.x
- Bundle management

Q3 2012

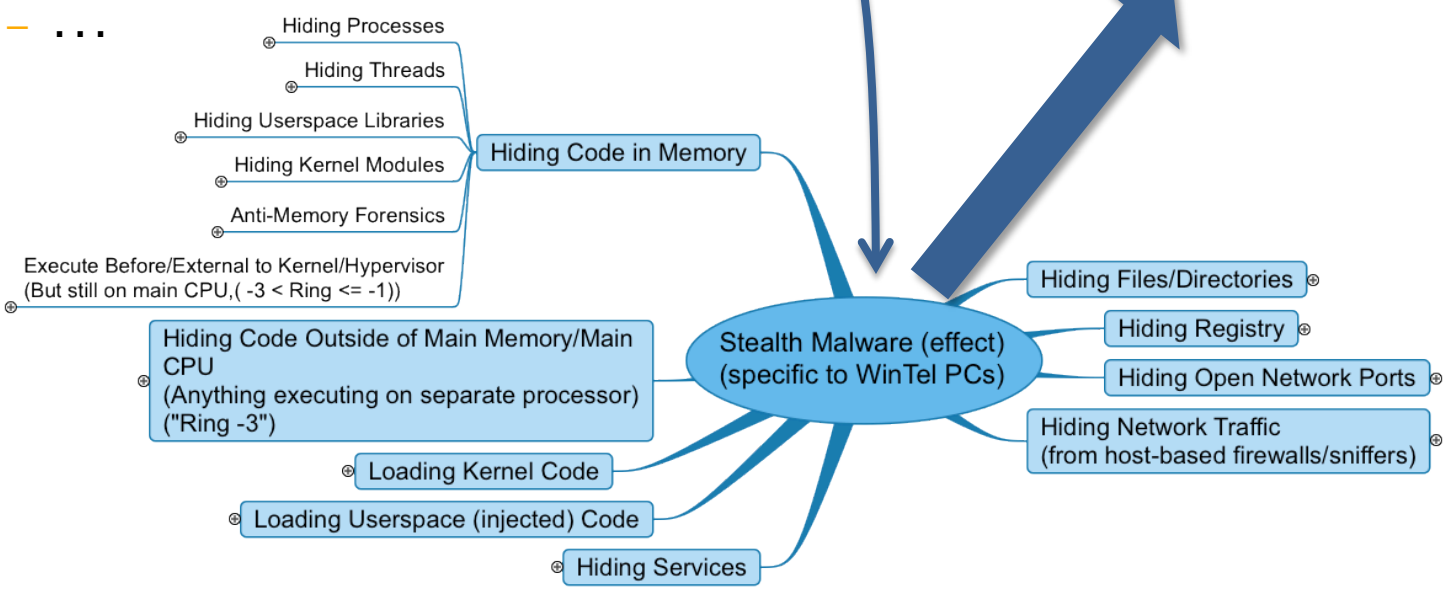
V 3.0
- Mechanism and behavior taxonomies
- Dictionaries
- Schema integration

© 2011 The MITRE Corporation. All rights reserved.

Mechanisms and Behaviors

- Enumerations
  - Exploit/Infect
  - Stealth
  - Self-Protection
  - Code Obfuscation
  - Persistence
  - Propagation
  - Command and Control
  - Information Stealing
  - Disruption
  - . . .

- Stealth Mechanism Schema
  - ID
  - Name
  - Parent
  - Children
  - Privilege Level
  - Objects
  - . . .



© 2011 The MITRE Corporation. All rights reserved.