HS SEDI
Homeland Security Systems Engineering and
Development Institute

MAEC™

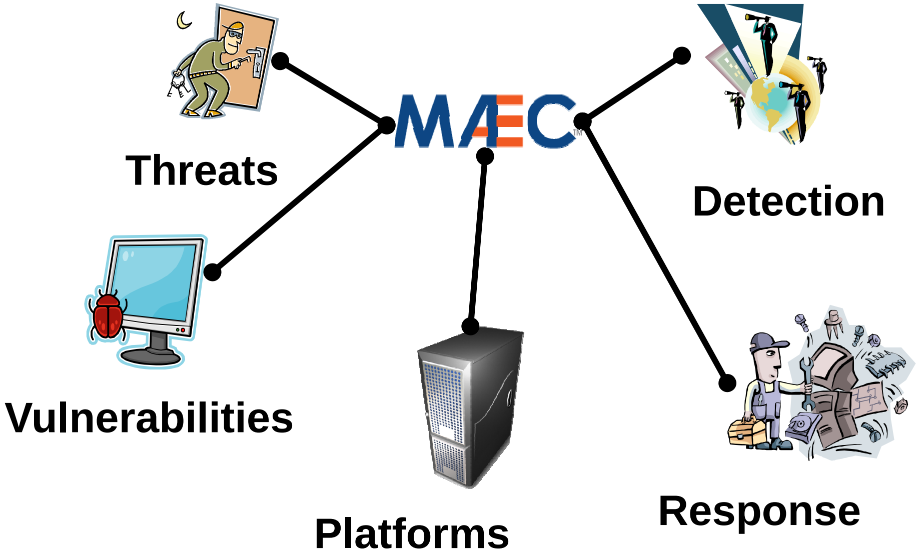
Penny Chase

Ivan Kirillov – Desiree Beck – Robert Martin

Homeland
Security

HS SEDI is a trademark of the U.S. Department of Homeland Security (DHS).
The HS SEDI FFRDC is managed and operated by The MITRE Corporation for DHS.

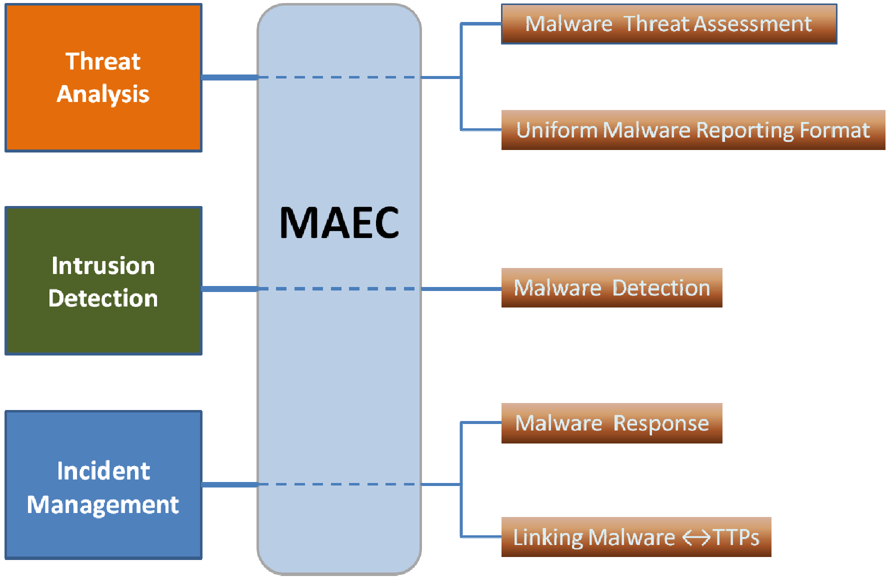
Malware Attribute Enumeration and Characterization (MAEC)



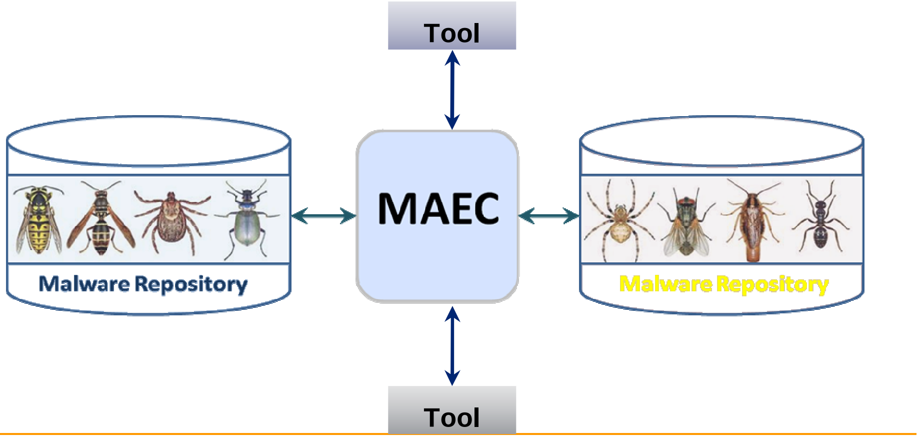
- Language for sharing structured information about malware
  - Grammar (Schema)
  - Vocabulary (Enumerations)
  - Collection Format (Bundle)
- Focus on attributes and behaviors
- Enable correlation, integration, and automation

MAEC Use Cases

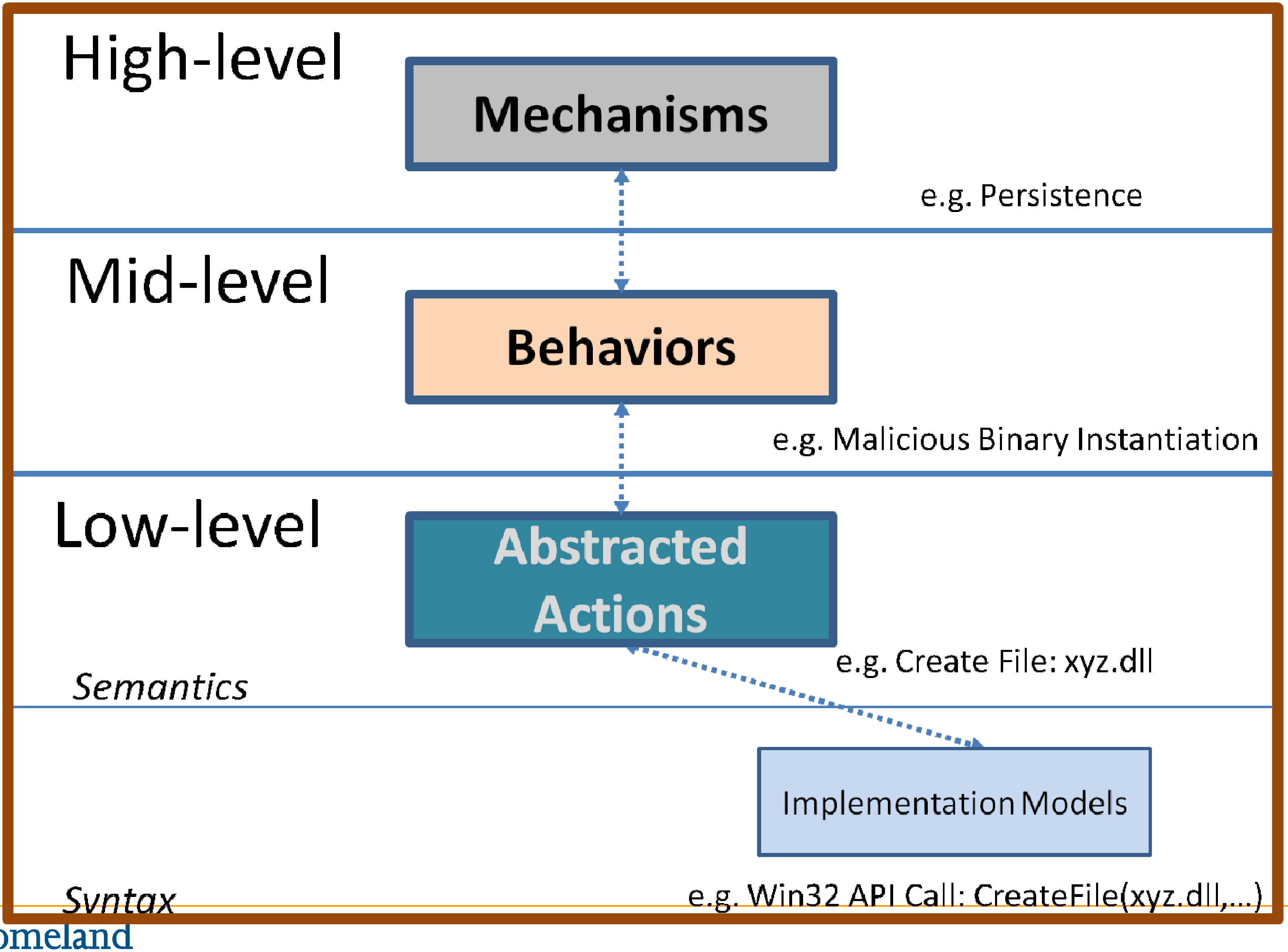
- Operational



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



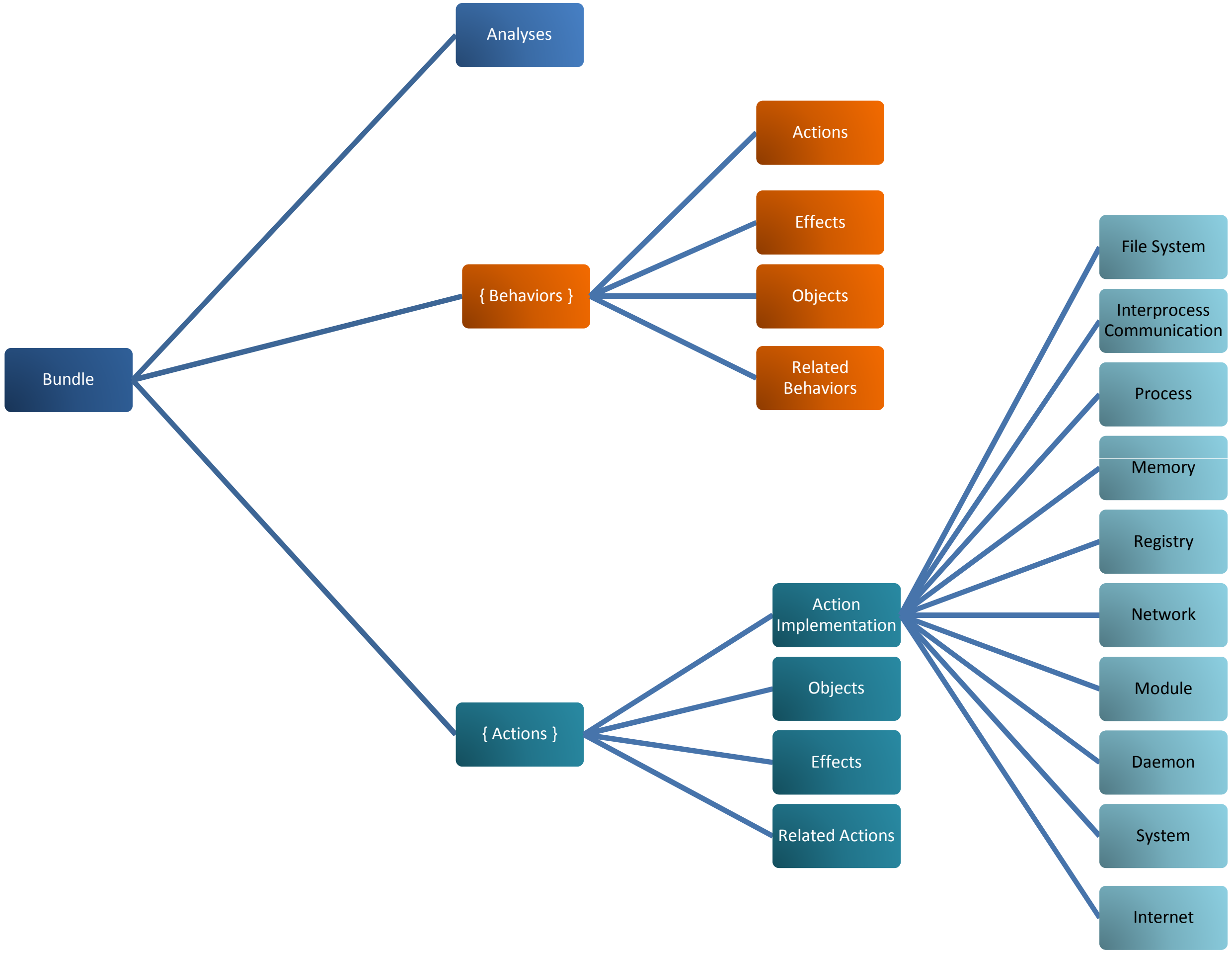
MAEC Overview



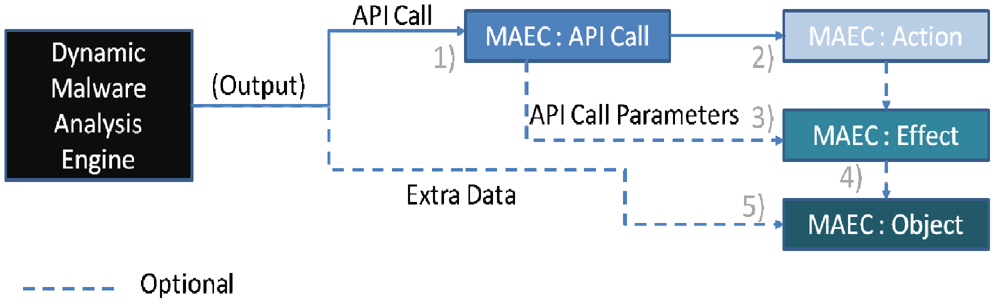
MAEC Activities

- **Released Schema v 1.0**
- **Developing Schema v 1.1**
- **Developed reference implementations**
  - Transform Dynamic Analysis tool output to MAEC
  - Generate OVAL definitions from MAEC descriptions
- **Malware Ontologies development**
- **MAEC Collaboration and Outreach**

MAEC Schema v 1.0 Overview



Dynamic Malware Analysis → MAEC



Dynamic Malware Analysis Engine

(Output)

API Call

1)

MAEC : API Call

2)

MAEC : Action

API Call Parameters

3)

MAEC : Effect

4)

Extra Data

5)

MAEC : Object

Optional

Process

1) An API call is captured by the analysis engine and mapped to MAEC's enumeration of API calls.
2) The MAEC enumerated call is mapped to its corresponding action.
3) The MAEC defined action is mapped to a corresponding MAEC effect (as necessary), which is populated by the parameters of the call.
4) The MAEC effect is linked to a MAEC object (as necessary).
5) Any extra data output (e.g. file attributes, network capture, etc.) from the analysis engine is mapped to its corresponding object (as necessary).

- **Demonstrate the ability to generate MAEC XML descriptions from dynamic analysis tools**
- **Developed proof-of-concept translators for:**
  - CW Sandbox (Sunbelt)
  - ASAT (MITRE)
  - Anubis
  - ThreatExpert

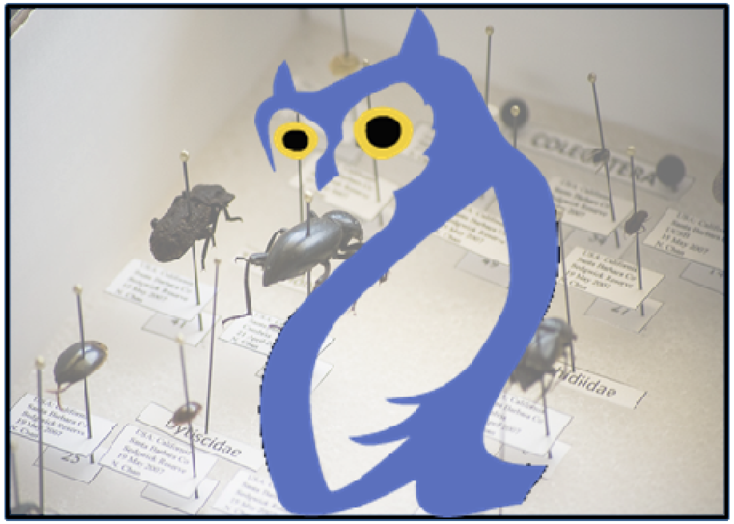
MAEC™ → OVAL®

- **MAEC XML to OVAL XML Converter**
  - Extracts MAEC Objects (defined as being created by malware)
  - Converts Objects into OVAL Representations
  - Creates definitions and tests to check for the existence of these objects

- **Capabilities/Use cases**
  - When used with an OVAL interpreter, it permits the automated testing of the existence of malware artifacts on any host system
  - Facilitates the interconnection of malware analysis and malware response

- **Currently supported artifacts:**
  - (Windows) Files/Directories/Named Pipes
  - Registry Keys

Malware Ontologies



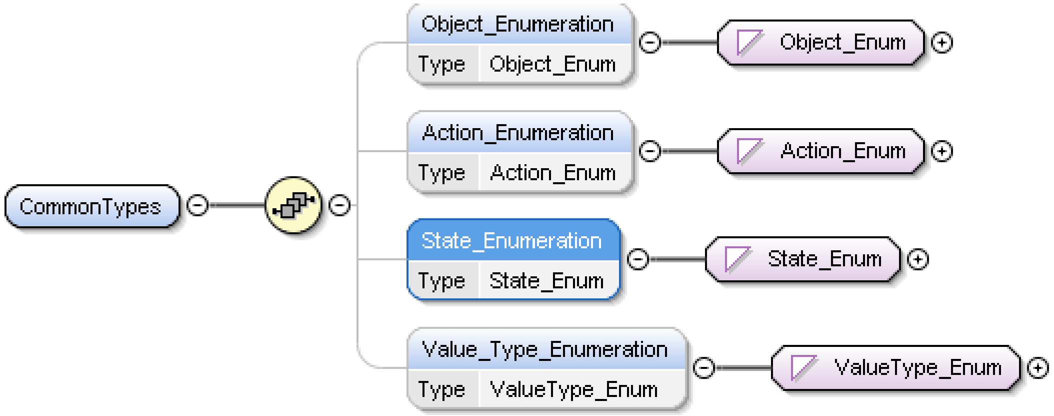
- **Started to develop a semantic web version of MAEC using NetOwl**
  - Many things we'd like to do with MAEC—express complex relationships and constraints—are awkward in XML
- **Semantic MAEC will facilitate:**
  - Correlation across multiple data sources
  - Using MAEC's multiple levels of abstraction
  - Support automation

Collaboration (1/2)

- **IEEE ICSG Malware Working Group**
  - Developed Malware Metadata exchange schema to facilitate the sharing of sample data between AV product vendors
    - Attributes for AV classifications, source (URIs), object properties (file hashes, registry keys), boolean properties (isKernel, isPolymorphic)
  - MAEC currently imports the IEEE ICSG Malware Metadata exchange schema
  - In the future, the IEEE schema may import certain MAEC elements
- **Industry /Government**
  - Although non-standardized, there has been some related work in this realm done by industry and government
  - We are actively collaborating with several companies on how to best leverage each other's efforts
  - Likewise, we are planning on leveraging the work done by government in the anti-malware space

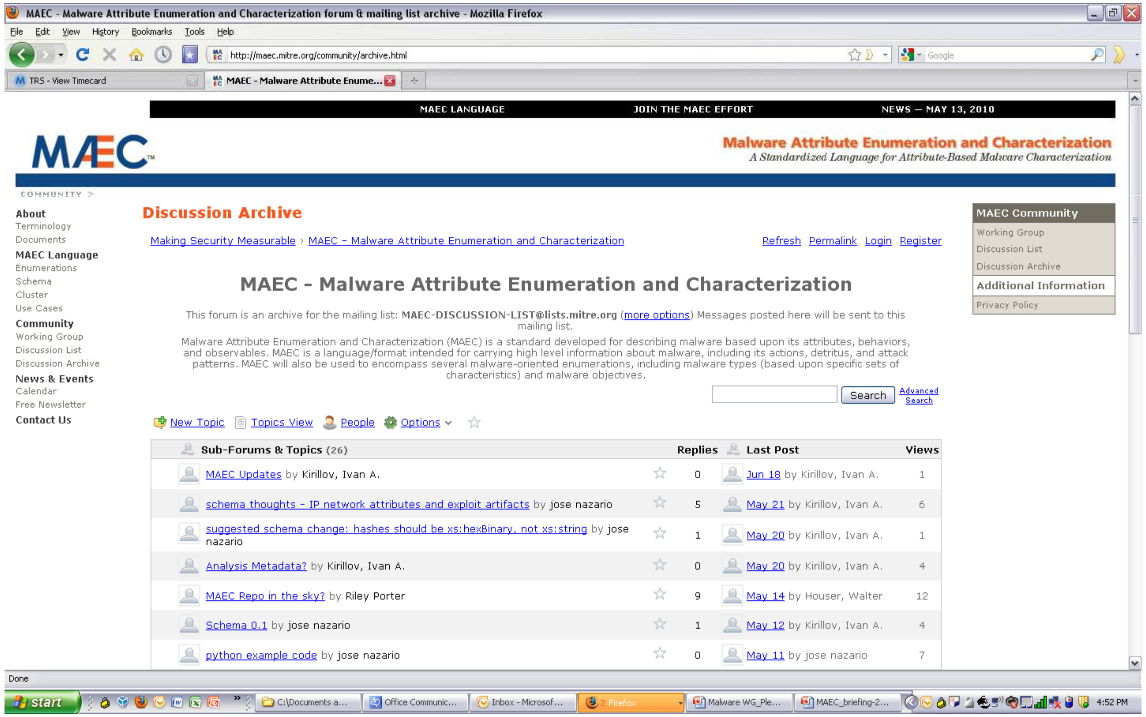
Collaboration (2/2)

- **Related Making Security Measurable Efforts**
  - There is significant overlap between MAEC, CAPEC, and CEE in describing observed actions, objects, and states.
  - As such, we're working on developing a common schematic structure of observables for use in these efforts:



MAEC Community: Discussion List

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



Discussion Archive

Making Security Measurable › MAEC - Malware Attribute Enumeration and Characterization

Refresh Permalink Login Register

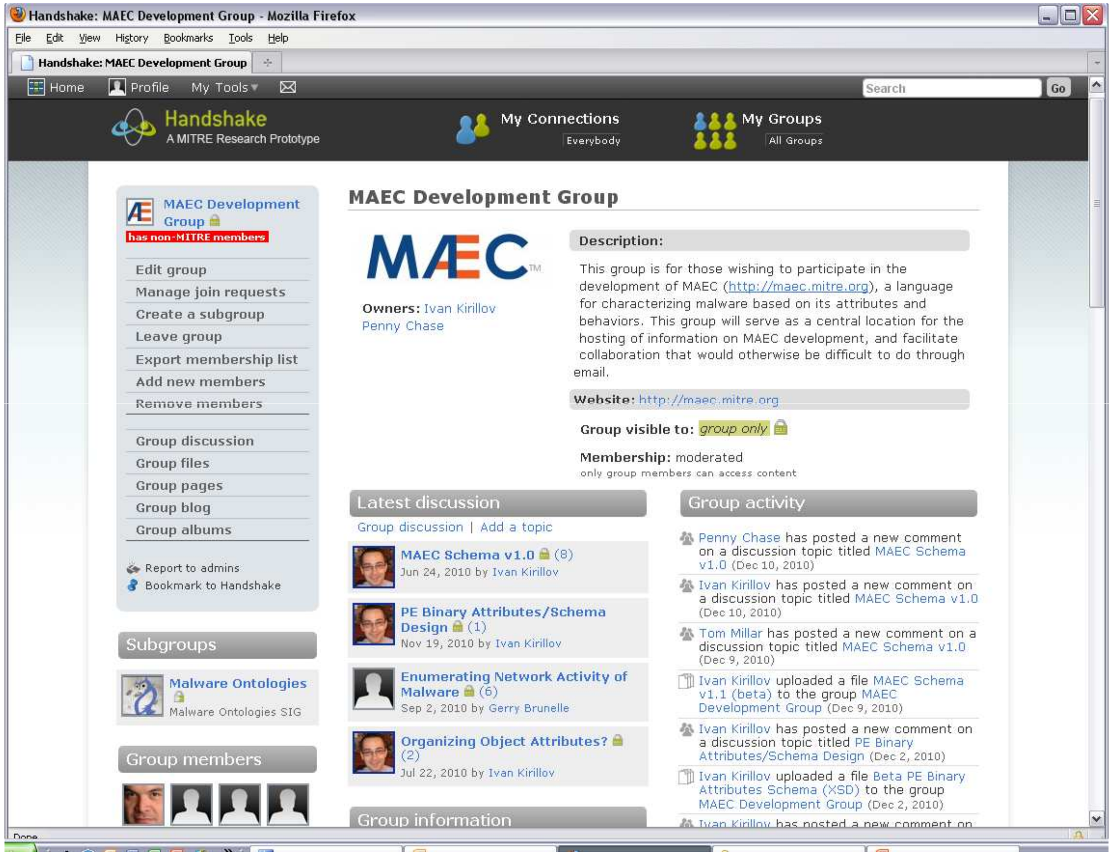
MAEC - Malware Attribute Enumeration and Characterization

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, detritus, 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 Houser, Walter	12
Schema 0.1 by jose nazario	1	May 12 by Kirillov, Ivan A.	4
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 24, 2010 by Ivan Kirillov

PE Binary Attributes/Schema Design (1)
Nov 19, 2010 by Ivan Kirillov

Enumerating Network Activity of Malware (6)
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 Millar 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)

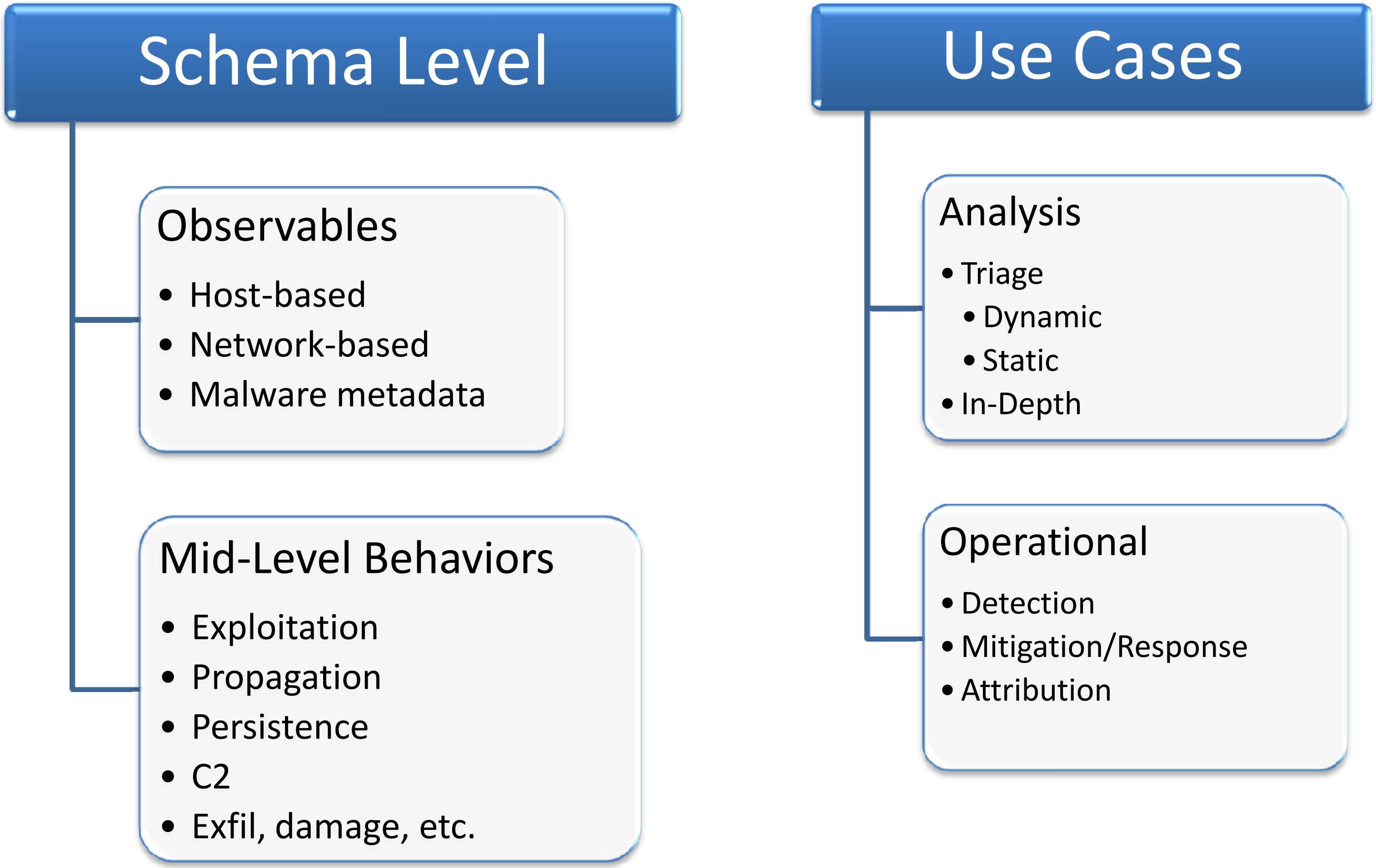
Ivan Kirillov has posted a new comment on a discussion topic titled PE Binary Attributes/Schema Design (Dec 2, 2010)

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 Schema Dimensions



Schema Level

Observables

- Host-based
- Network-based
- Malware metadata

Mid-Level Behaviors

- Exploitation
- Propagation
- Persistence
- C2
- Exfil, damage, etc.

Use Cases

Analysis

- Triage
  - Dynamic
  - Static
- In-Depth

Operational

- Detection
- Mitigation/Response
- Attribution

Expressiveness
Abstraction

MAEC Schema Roadmap

- **MAEC v 1.0**
  - Analysis: Dynamic
  - Operational: Detection (Host-based through OVAL)
  - Schema Level: Host-based observables
- **MAEC v 1.1**
  - Analysis: Static
  - Schema Level: Malware metadata
- **Future Schemas**
  - In-Depth Analysis
    - Mid-level behaviors
  - Operational
    - Signature and Indicators of Compromise (IOCs) management
    - Mitigation and response support
  - Expressiveness
    - Operators, constraints, relationships

Next Steps

- **Complete MAEC v 1.1**
- **Complete OWL ontology based on MAEC schema**
- **XSLT transformation of MAEC XML → HTML**
- **Implement common observables schema (v 1.2?)**
  - Based on MAEC/CAPEC/CEE collaboration
- **Prioritize schema roadmap**
- **Encourage and invite more participation in the development process**
  - MAEC Website: http://maec.mitre.org (contains MAEC Discussion list sign-up)
  - MAEC Handshake Group (send email to maec@mitre.org to request an invitation)
  - RSA BoF Session?