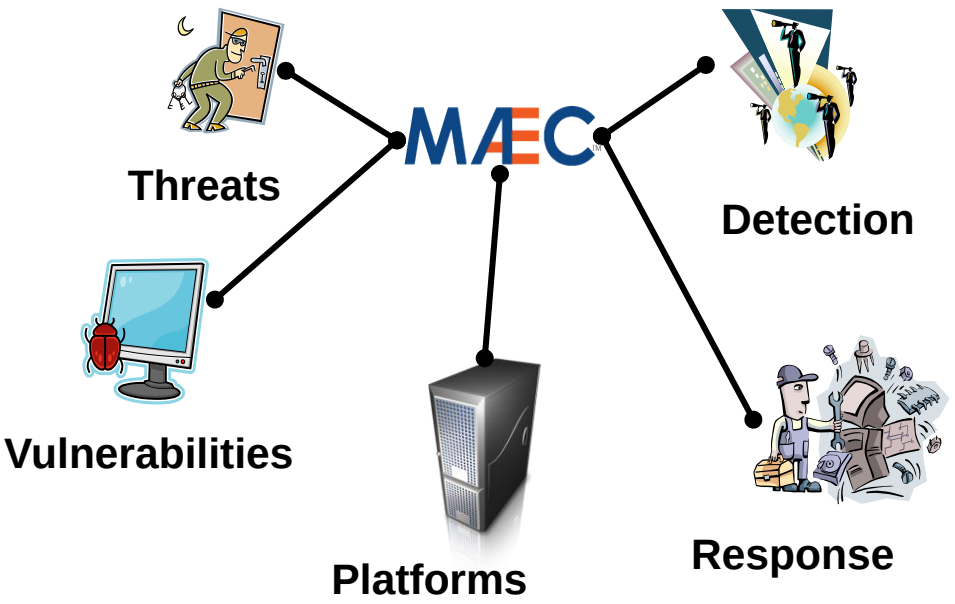
Penny Chase

13 July 2012

MITRE

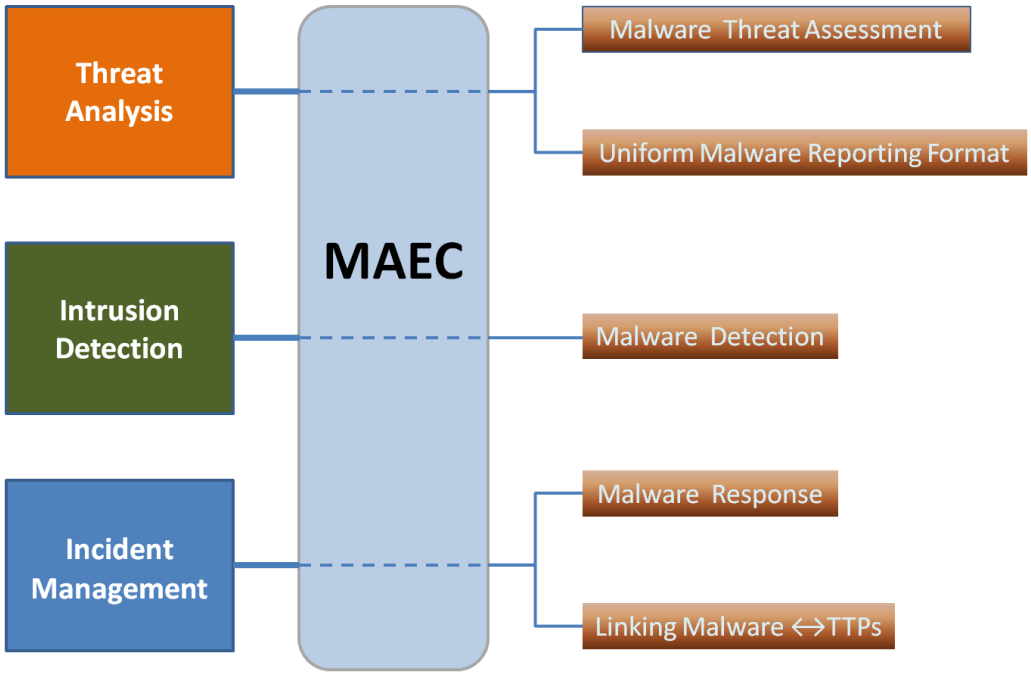
Malware Attribute Enumeration and Characterization (MAEC)



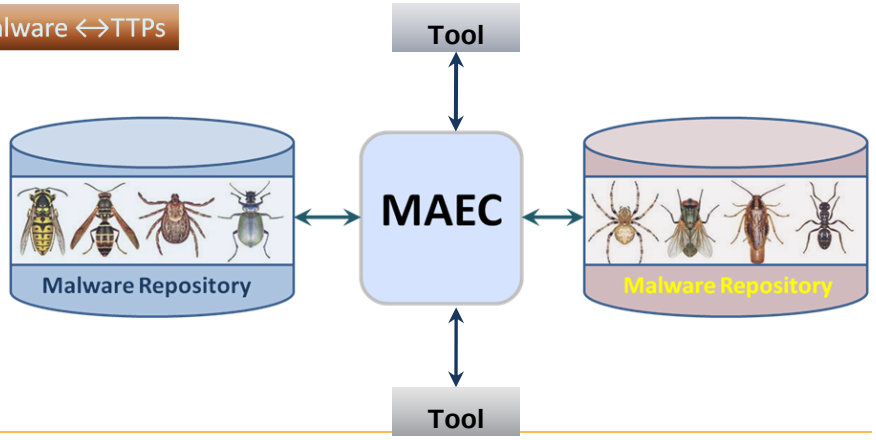
- Language for sharing structured information about malware
  - Grammar (Schema)
  - Vocabulary (Enumerations)
  - Collection Format (Bundle)
- Focus on attributes and behaviors
- Enable correlation, integration, and automation

MAEC Use Cases

- **Operational**

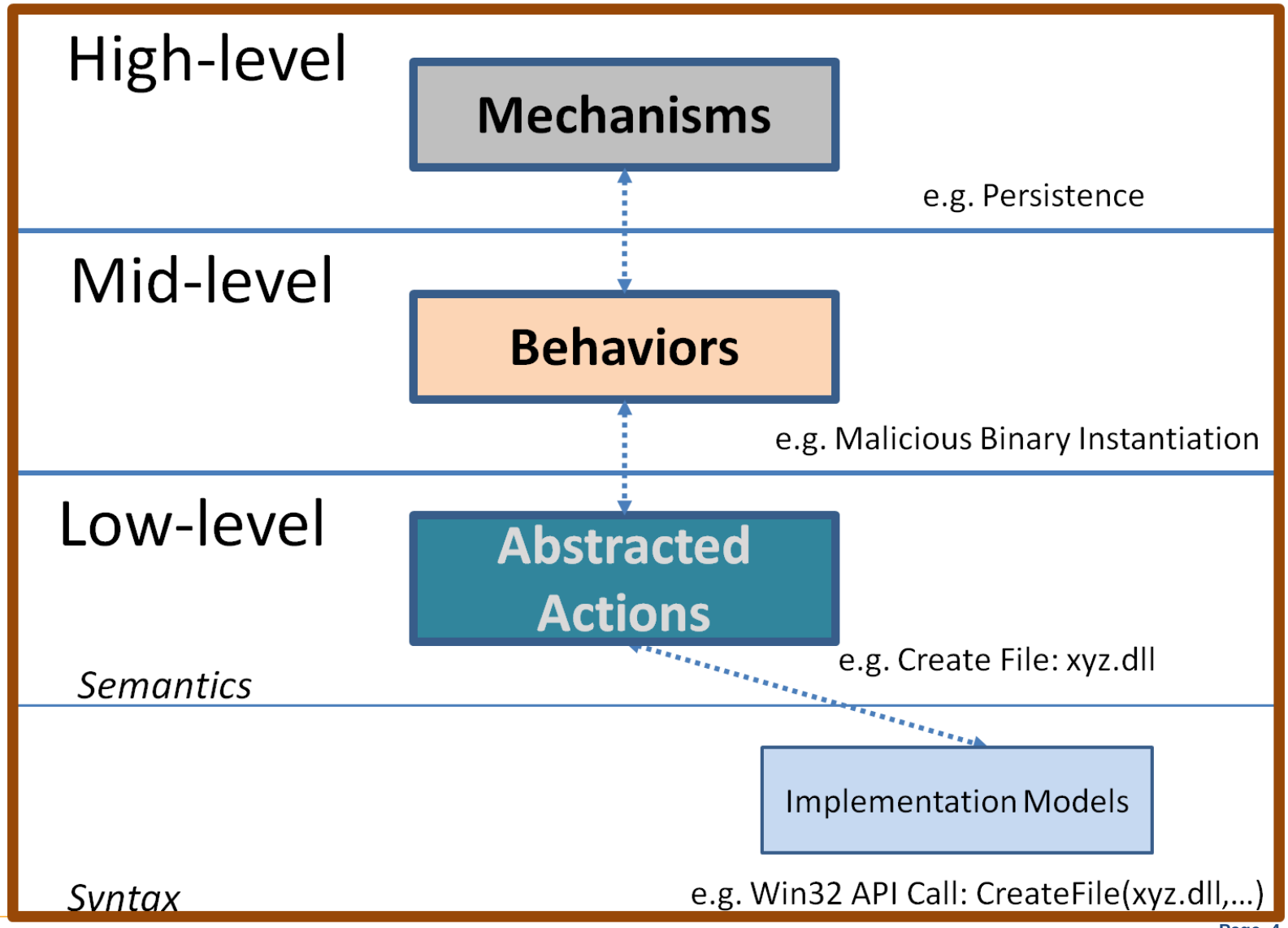


- **Analysis**
  - Help Guide Analysis Process
  - Standardized Tool Output
  - Malware Repositories



MITRE

MAEC Structure Overview



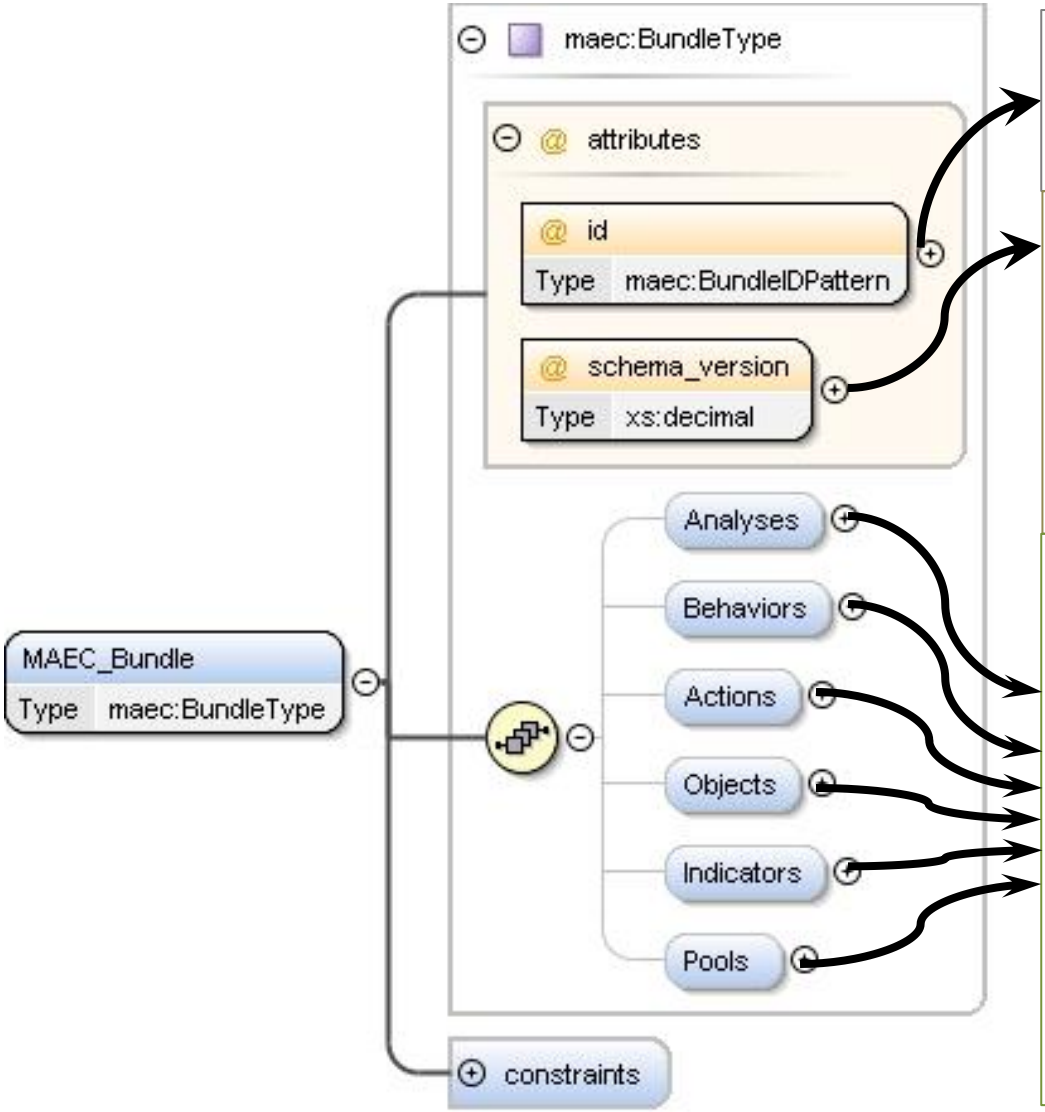
MITRE

MAEC and CybOX

Analysis and Characterization of Malware (MAEC)
- Mechanisms
- Behaviors
- Indicators
- Analysis Context

Cyber Observable Characterization (CybOX)
- Actions
- Objects

MAEC's Bundle



MAEC Bundle ID

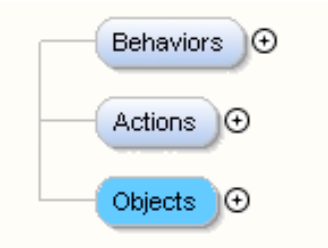
- Globally unique identifier

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



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>

MAEC Bundle

Behaviors

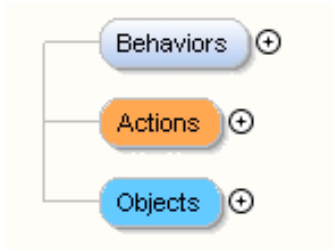
Actions

Objects

3. Obj 1

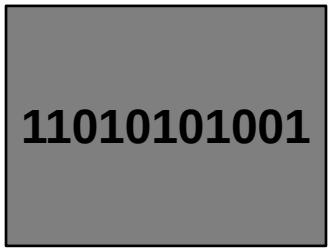
1. Features Extracted
2. MAEC Object Created
3. Object Added to Bundle

MITRE



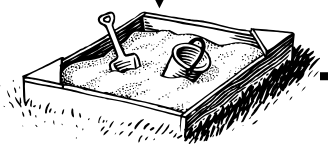
MAEC & Malware Analysis Process II

Stage Two: Dynamic Analysis Triage



Malware Binary

1.



2.

Files Created:

C:\Temp\loader.exe

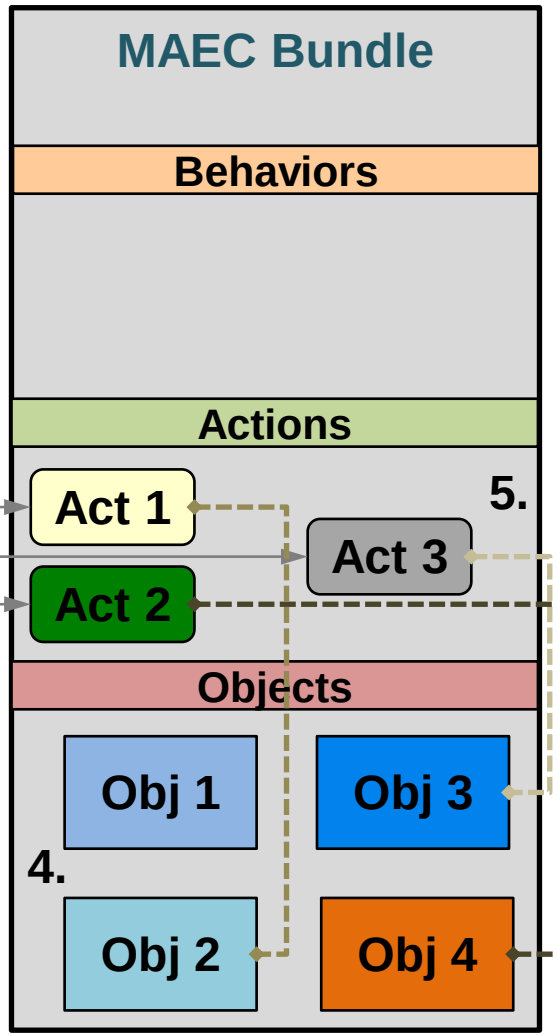
C:\Windows\rtkit.dll

Registry Key/Value Created:

Key: *…\Programs\Startup*

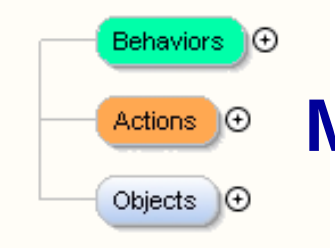
Value: *…\loader.exe*

3.



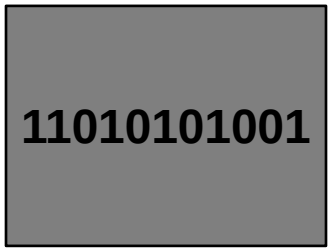
1. Malware Executed on Sandbox
2. Execution Report Generated
3. Actions Added
4. Objects Added
5. Action/Object Relationships Added

MITRE



MAEC & Malware Analysis Process III

Stage Three: In-depth Manual Analysis



Malware Binary

1. 

2. **Actions:**

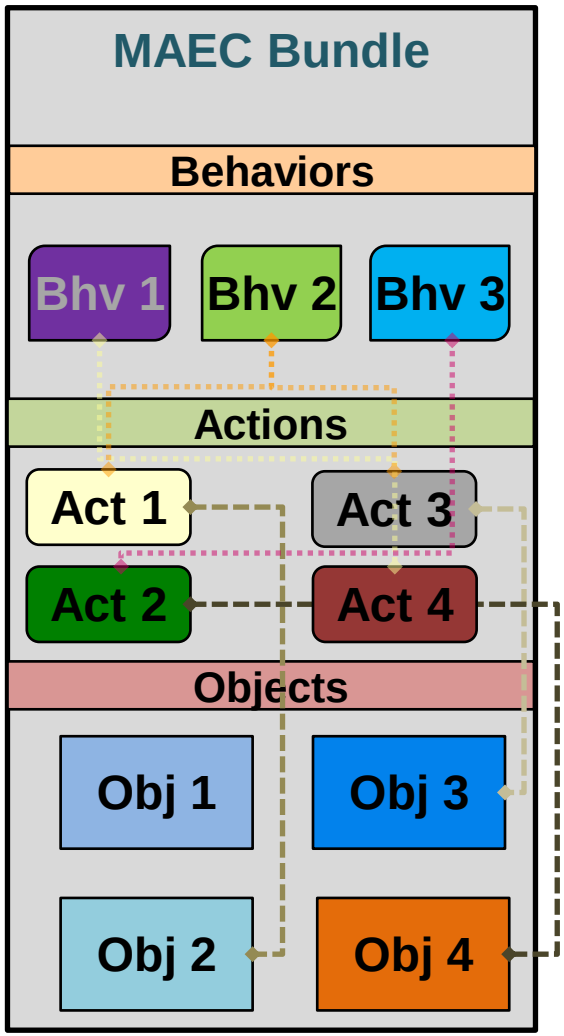
   Start Winsock

3. **Behaviors:**

   Winsock Startup

   Malicious Binary Instantiation

   Registry Persistence

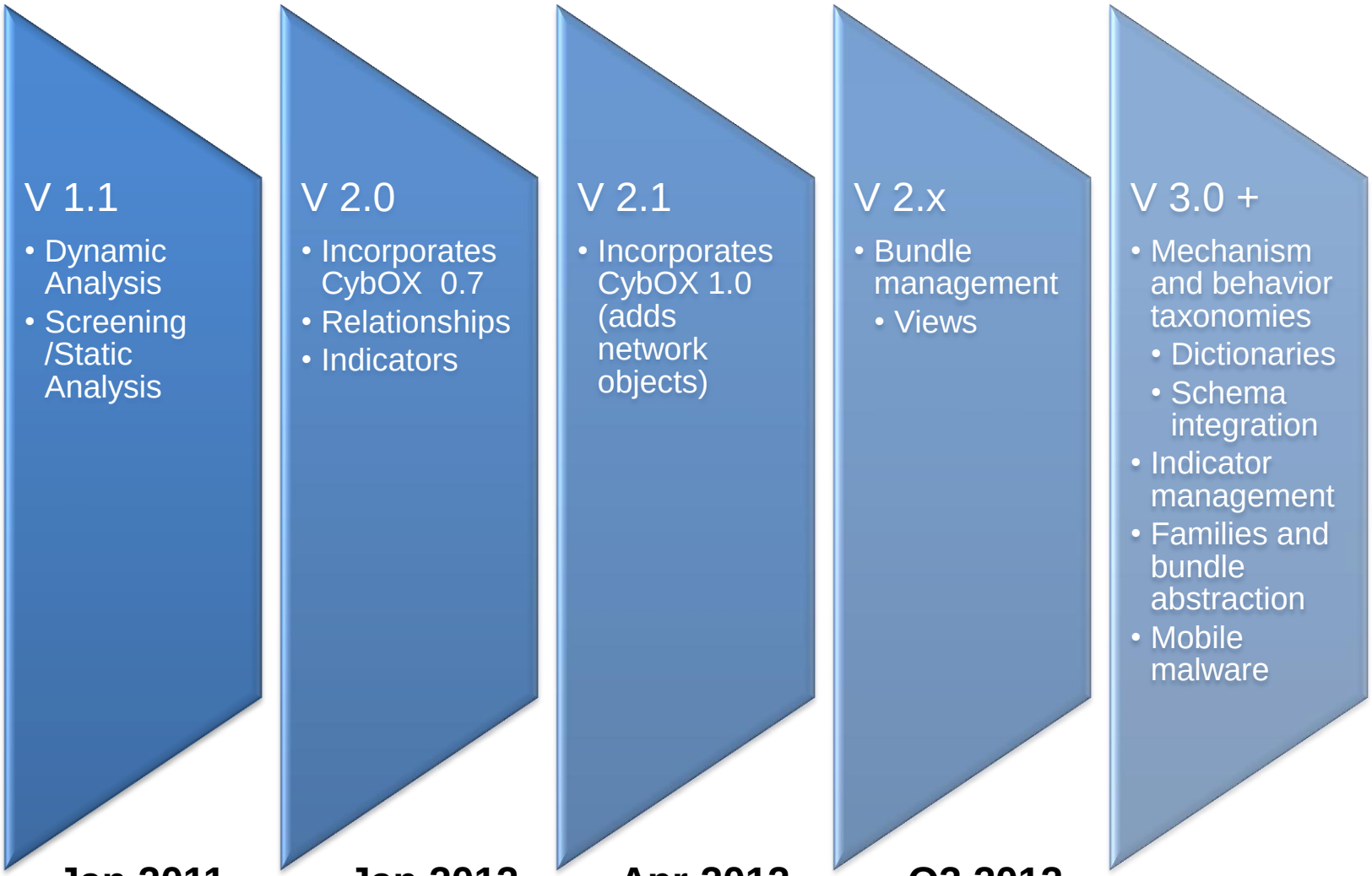


1. Malware Analyzed Manually
2. New Actions Extracted and Added
3. Behaviors Extracted and Added

MAEC Development

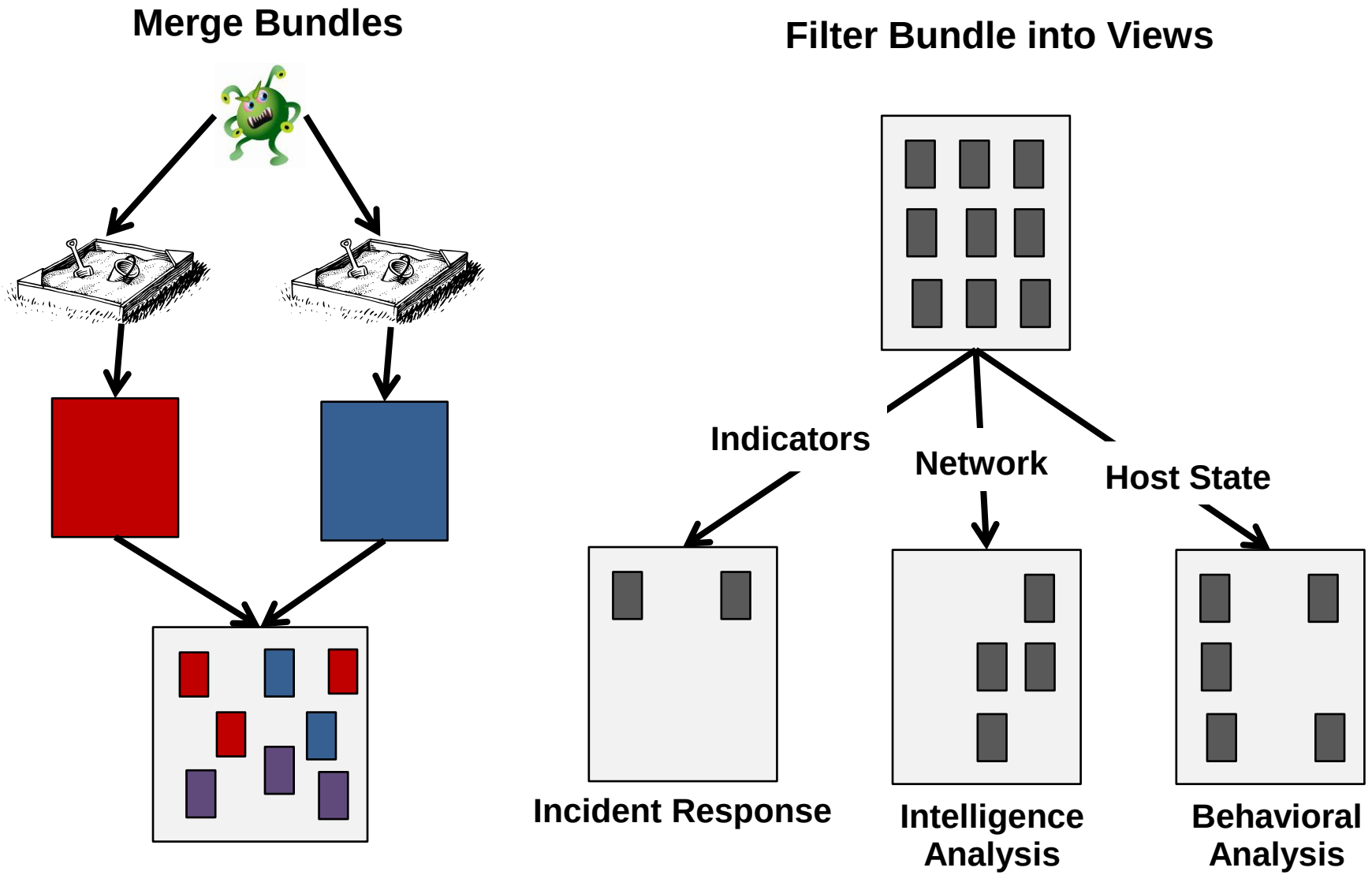
- Collaboration between industry and government
- Leverage existing resources, such as
  - IEEE Industry Connections Security Group's Malware Metadata Exchange Format schema v 1
  - Mandiant's openIOC
- Participate in standards efforts
  - IEEE ICSG Malware Metadata Exchange Format WG
    - Adding capability 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 may be part of the MILE Structured Cybersecurity Information RFC (extensions to IODEF)

MAEC Roadmap



MITRE

Bundle Management and Views

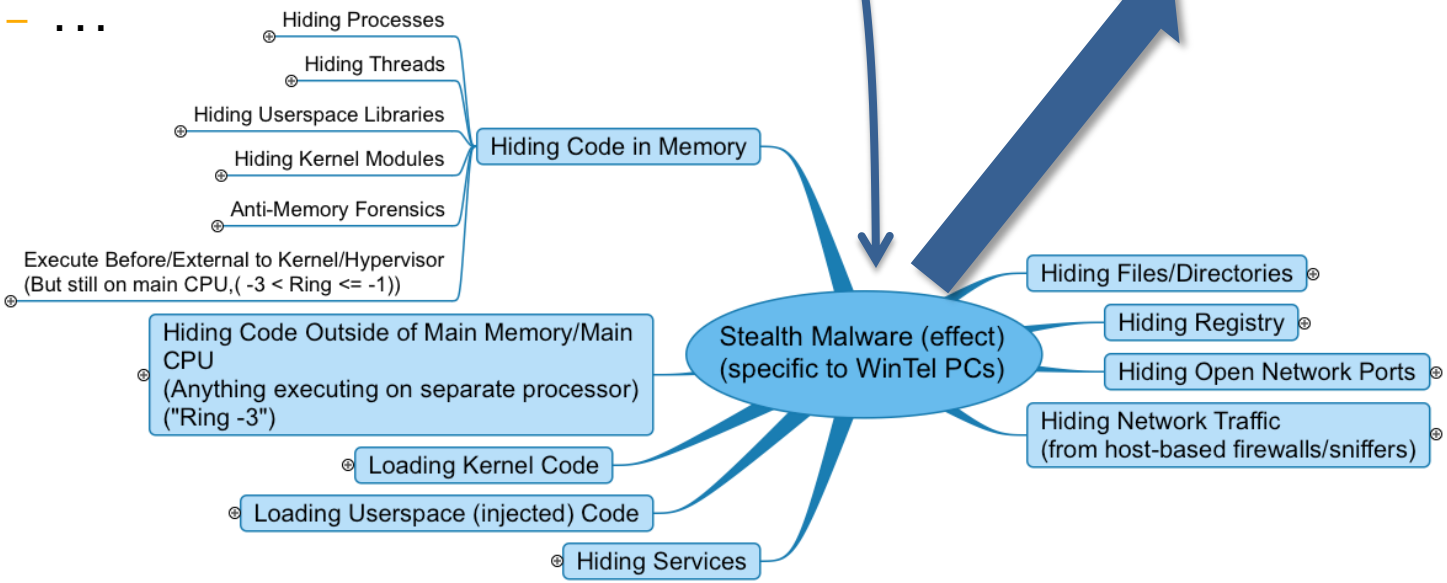


MITRE

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
  - . . .



For More Information

- **Web site: http://maec.mitre.org**
- **Mailing list: http://maec.mitre.org/community/discussionlist.html**
- **MAEC Development Group: http://handshake.mitre.org**
- **Github: https://github.com/MAECProject/Tools**