Hunting Malware With MAEC And OVAL

Ivan Kirillov

26 March 2012

MITRE

© 2012 The MITRE Corporation. All rights reserved.

Agenda

- Hunting Malware
- OVAL Introduction
- OVAL & MAEC
- Demo
- Future Direction

© 2012 The MITRE Corporation. All rights reserved.

Hunting Malware

© 2012 The MITRE Corporation. All rights reserved.

Malware Artifacts

- When malware executes on a system, it leaves behind ‘artifacts’ that can signify its presence
  - Files
  - Registry Keys
  - Mutex Objects
  - Etc.

- Knowledge of these artifacts can be used for detection
  - Especially relevant for 0-day/APT malware
  - Can be used for a malware family, malware instance, or just generic detection

© 2012 The MITRE Corporation. All rights reserved.

Malware Artifact Hunting I

- What is needed is some standard way to describe the actions malware performs on a system and the artifacts associated with them..

MAEC™

- How about some standard way to check for these artifacts on an endpoint?

OVAL®

© 2012 The MITRE Corporation. All rights reserved.

OVAL Introduction

© 2012 The MITRE Corporation. All rights reserved.

What Is OVAL?

- OVAL is a language used to standardize the representation of specific system configurations.
  - XML based
  - Used to describe vulnerable configurations, compliance with specific policy, presence of a patch, etc.
  - Encodes the actual values of registry keys, file attributes, etc. that make up the system state being tested for
  - Removes the ambiguity of textual descriptions

© 2012 The MITRE Corporation. All rights reserved.

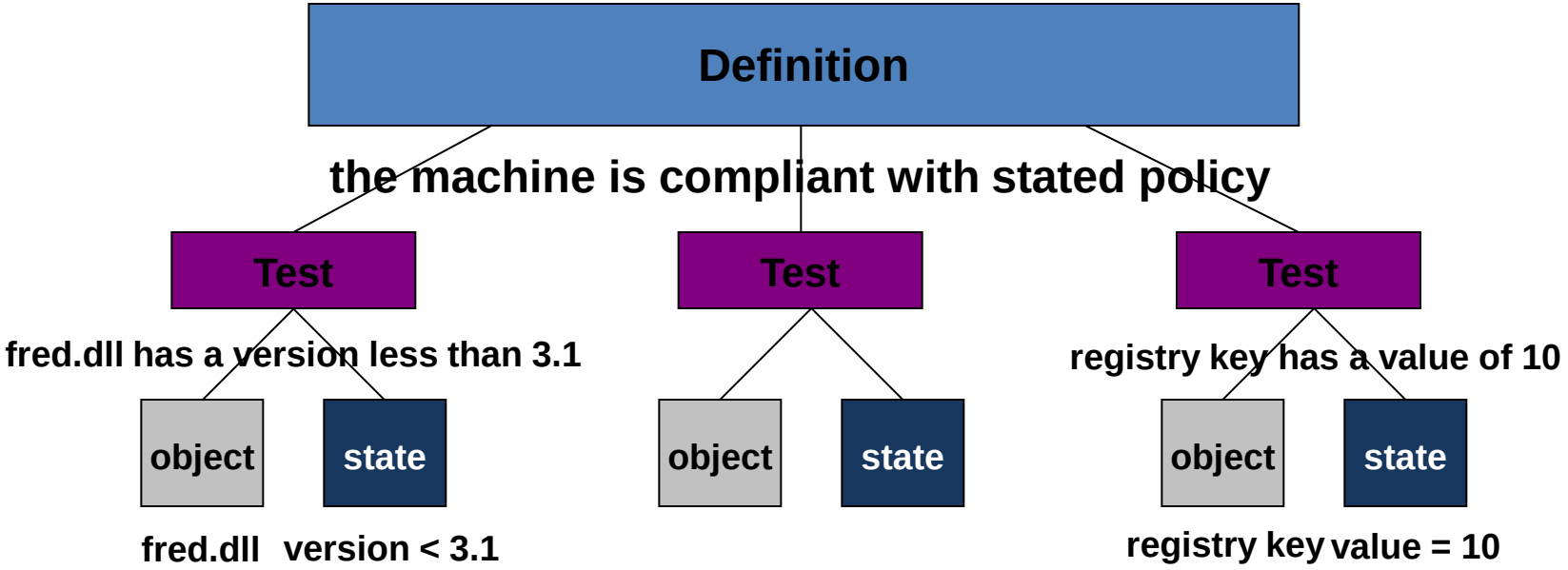
OVAL Interpreter

- Freely available reference implementation
- Demonstrates usability of the OVAL Language
- Drives the development of the OVAL Language
- Validate & test content
- A reference for developers
- Reduce the cost of OVAL adoption

http://oval.mitre.org/language/interpreter.html

© 2012 The MITRE Corporation. All rights reserved.

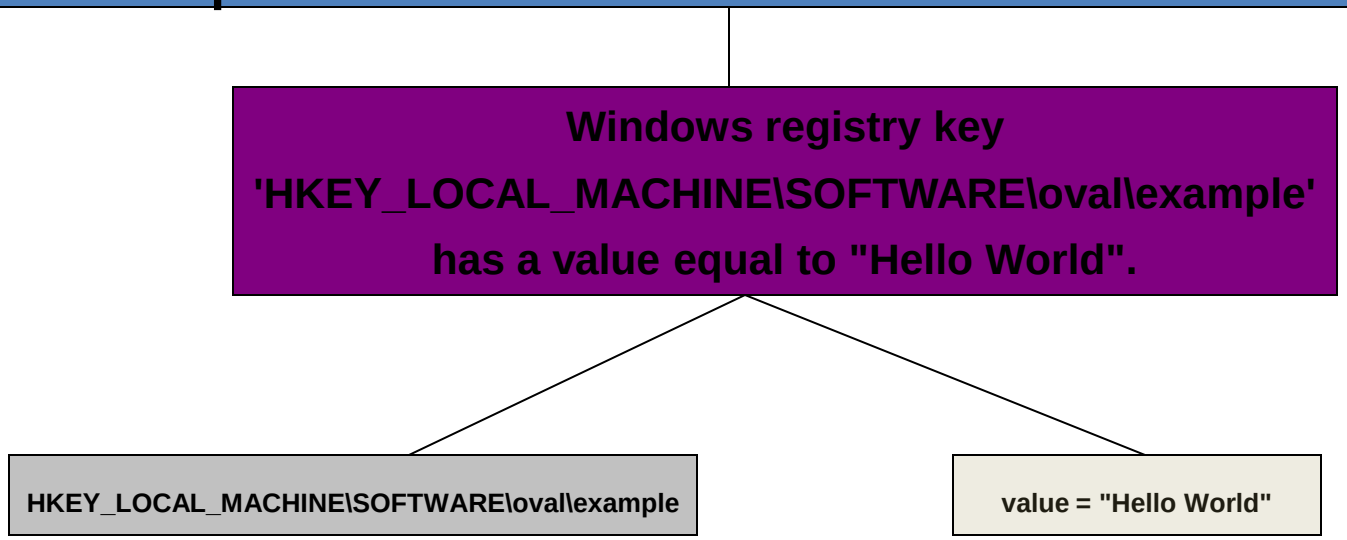
Structure of an OVAL Definition



© 2012 The MITRE Corporation. All rights reserved.

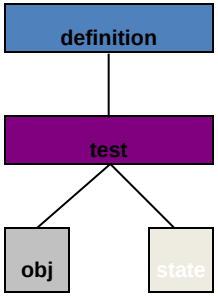
Hello World

- **Write an OVAL Definition to test that the (hypothetical) Windows registry key 'HKEY_LOCAL_MACHINE\SOFTWARE\oval\example' has a value equal to "Hello World".**



© 2012 The MITRE Corporation. All rights reserved.

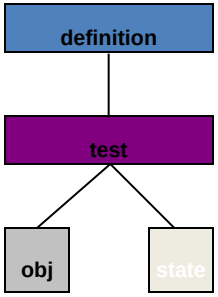
Hello World - Registry Object




```
<registry_object id="oval:com.example:obj:1">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>SOFTWARE\oval</key>
   <name>example</name>
</registry_object>
```


© 2012 The MITRE Corporation. All rights reserved.

Hello World - Registry State




```
<registry_state id="oval:com.example:ste:1">
  <value operation="equals">Hello World</value>
</registry_state>
```


© 2012 The MITRE Corporation. All rights reserved.

MAEC & OVAL

© 2012 The MITRE Corporation. All rights reserved.

Bridging the Gap

- **MAEC: Provides the intelligence about the malware, including information about associated artifacts and how they were utilized/affected**

- **OVAL: Provides the checking language and means for assessing a system for malware artifacts**

- **MAEC + OVAL: Together, these two standards allow for comprehensive and adaptable artifact-based malware detection**
  - **With the help of scripts, the entire process can be automated**
  - **OVAL on endpoints = enterprise level detection**
  - **Standards basis means information on the malware and the detection can be easily shared/consumed**

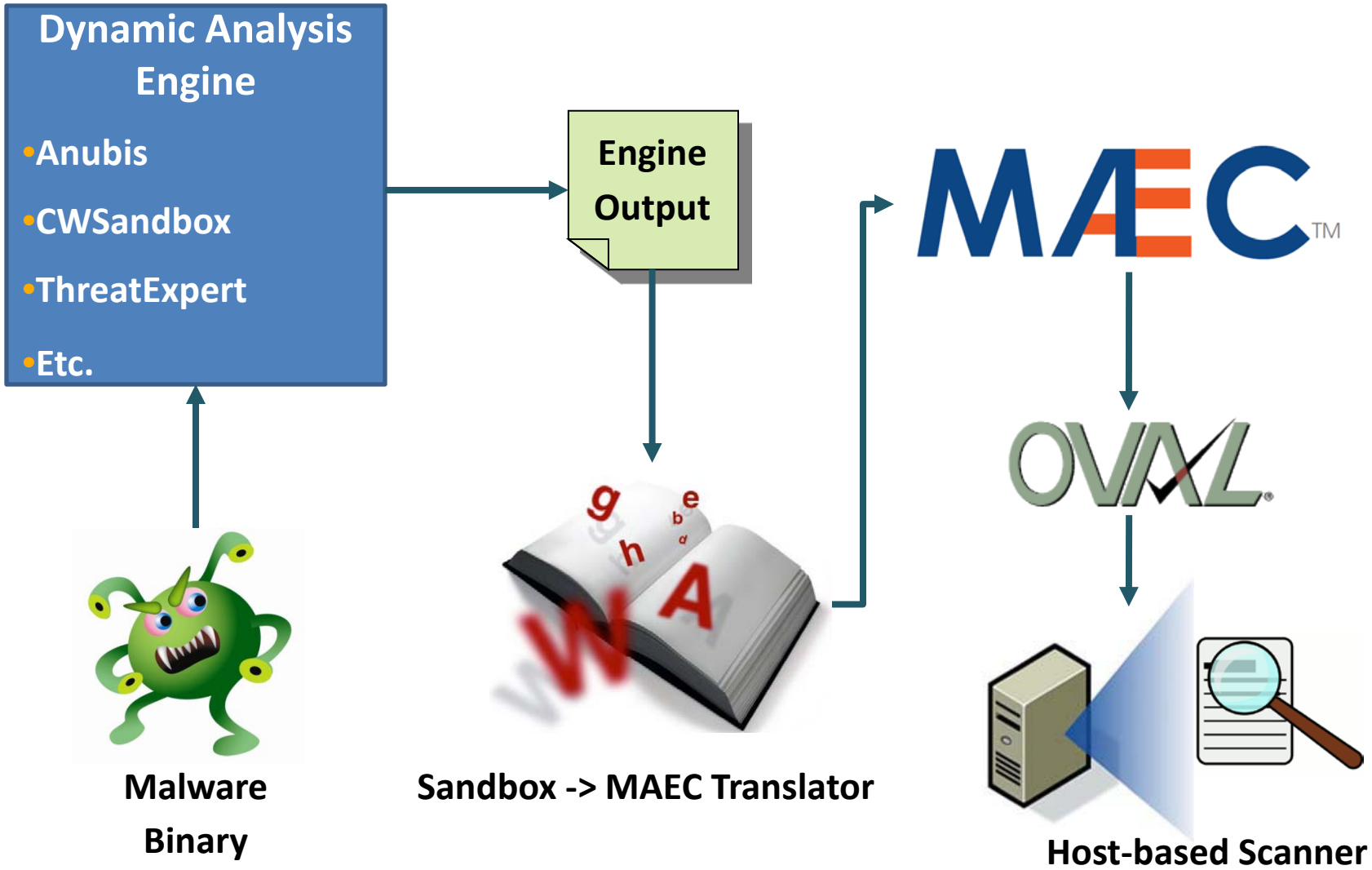
© 2012 The MITRE Corporation. All rights reserved.

Currently Supported Artifacts

- As of OVAL 5.10.1 (for Windows):
  - Files
  - Directories
  - Registry Keys
  - Processes
  - PE Header Entries
  - DNS Cache Entries
  - Ports
  - Services
  - User Accounts

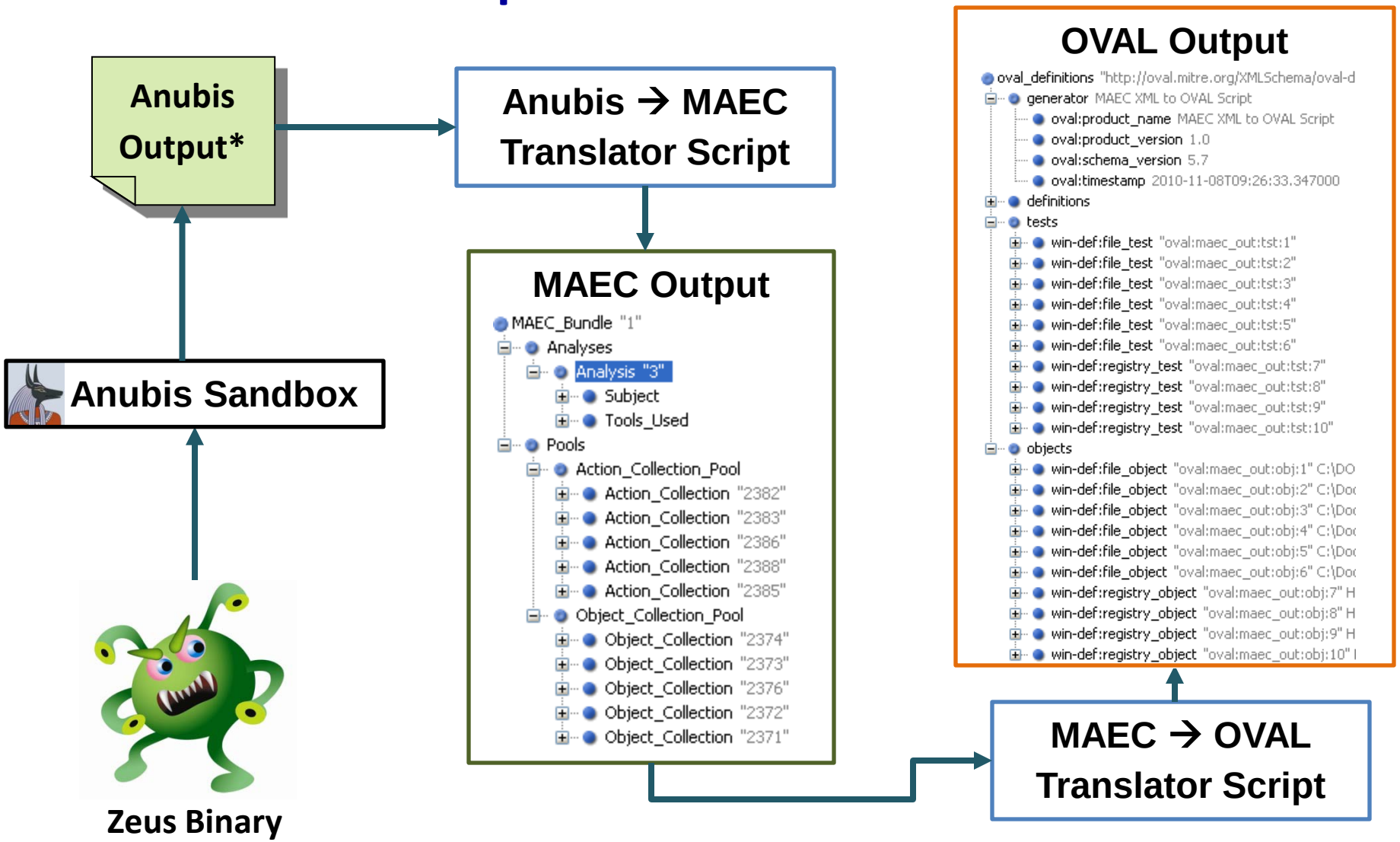
© 2012 The MITRE Corporation. All rights reserved.

MAEC & OVAL Interaction



© 2012 The MITRE Corporation. All rights reserved.

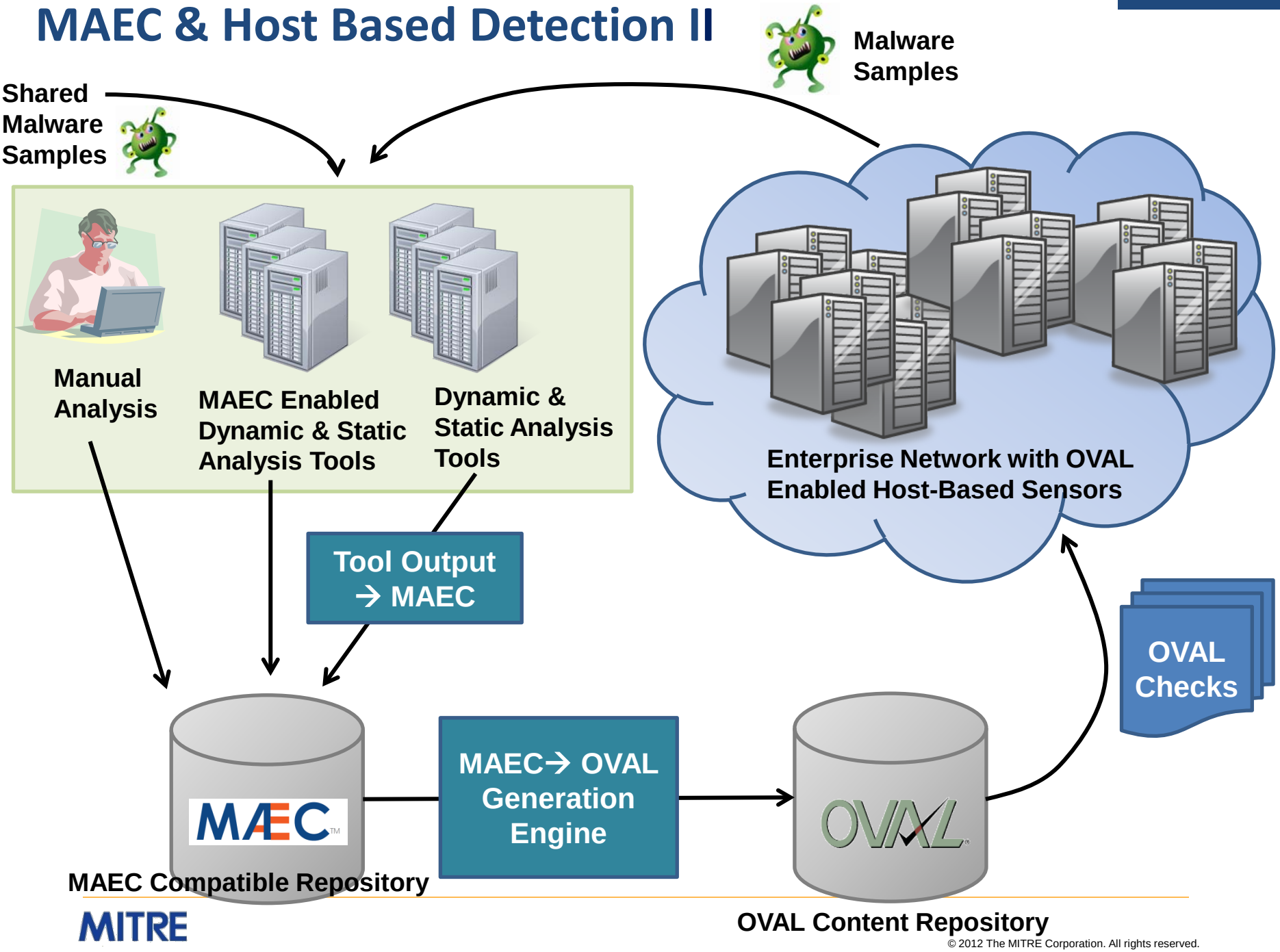
Real World Example: MAEC & Zeus Bot



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

© 2012 The MITRE Corporation. All rights reserved.

MAEC & Host Based Detection II



MITRE

© 2012 The MITRE Corporation. All rights reserved.

Demo

© 2012 The MITRE Corporation. All rights reserved.

Demo Tools

- Anubis → MAEC Translator
- MAEC → OVAL Translator
- OVAL Interpreter

© 2012 The MITRE Corporation. All rights reserved.

Future Direction

© 2012 The MITRE Corporation. All rights reserved.

Intelligent OVAL Generation

- **Challenge: Lots of noise in dynamic analysis output**
  - **Common system call usage**
  - **Dummy API calls**
  - **Randomization**
  - **Etc.**

- **We need a more intelligent way of specifying what makes a good malware indicator**
  - **Usage of MAEC Behaviors/Actions**
  - **MAEC Ontology → OVAL Generation**

© 2012 The MITRE Corporation. All rights reserved.

OVAL Artifact Hunting Extensions

- OVAL needs to expand its language to encompass more artifacts relevant for malware hunting (for Windows)
  - Mutexes
  - System Restore Objects
  - Drivers
  - Binary File Parsing

- OVAL Sandbox

© 2012 The MITRE Corporation. All rights reserved.

MAEC → OVAL Translator Script

- Support for additional objects
- Support for different translation modes
- ETA Q2 2012
  - Available on MAEC Handshake and Github

© 2012 The MITRE Corporation. All rights reserved.

Questions?

http://maec.mitre.org

http://oval.mitre.org

© 2012 The MITRE Corporation. All rights reserved.