



Penny Chase

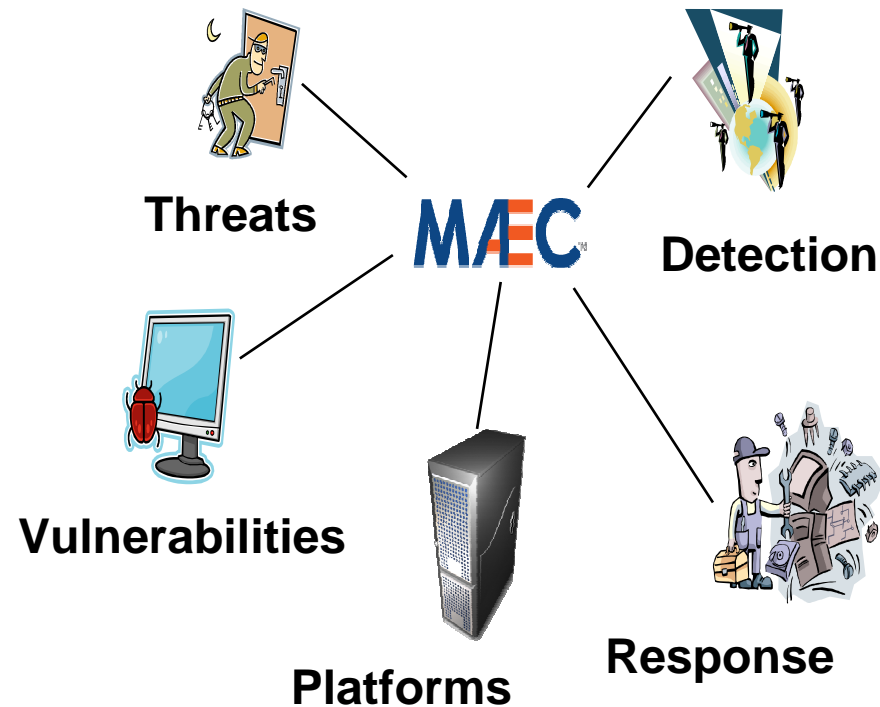
Ivan Kirillov – Desiree Beck – Robert Martin

Software Assurance Forum Malware Working Group

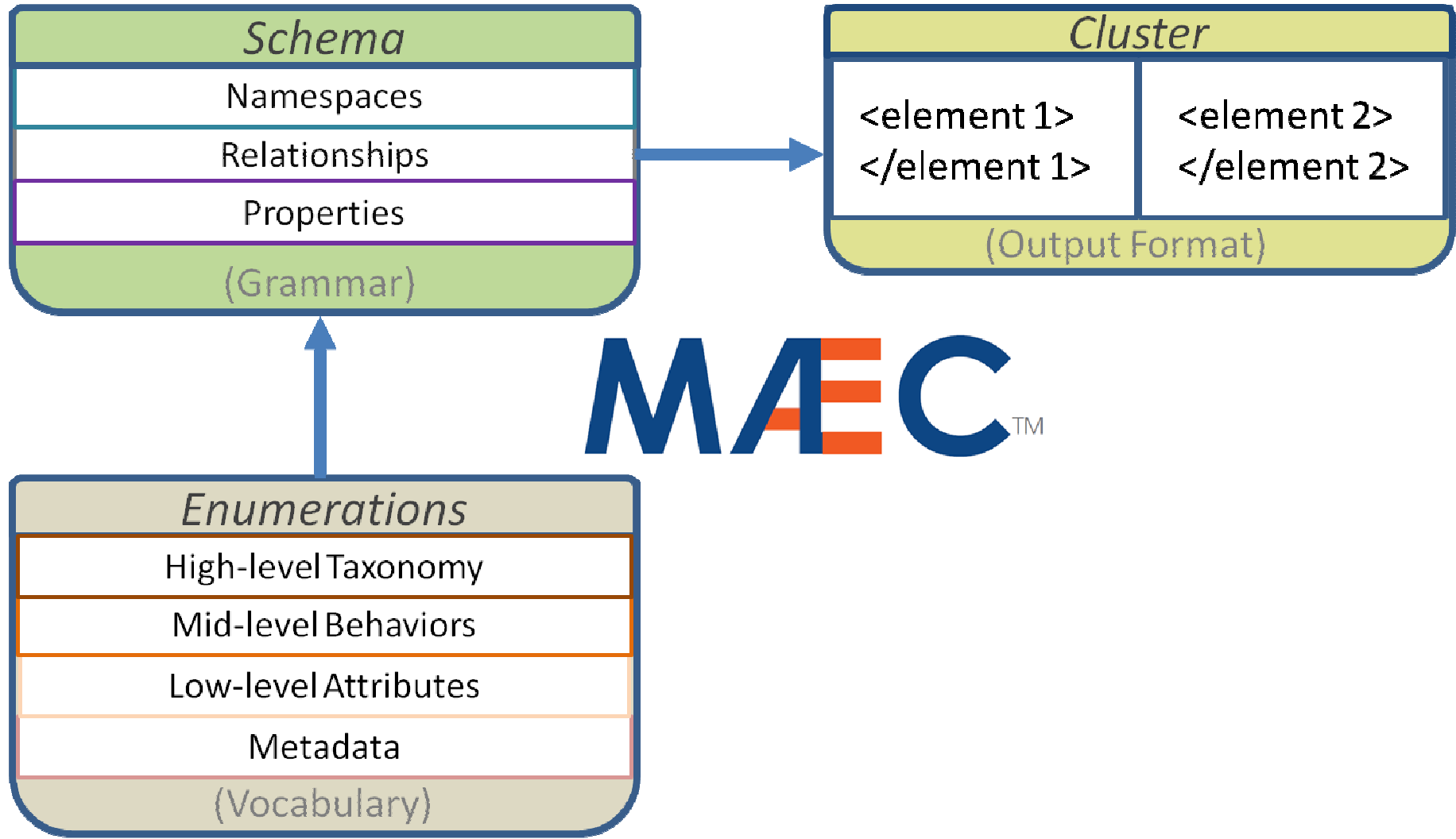
21 June 2010

Malware Working Group Goals

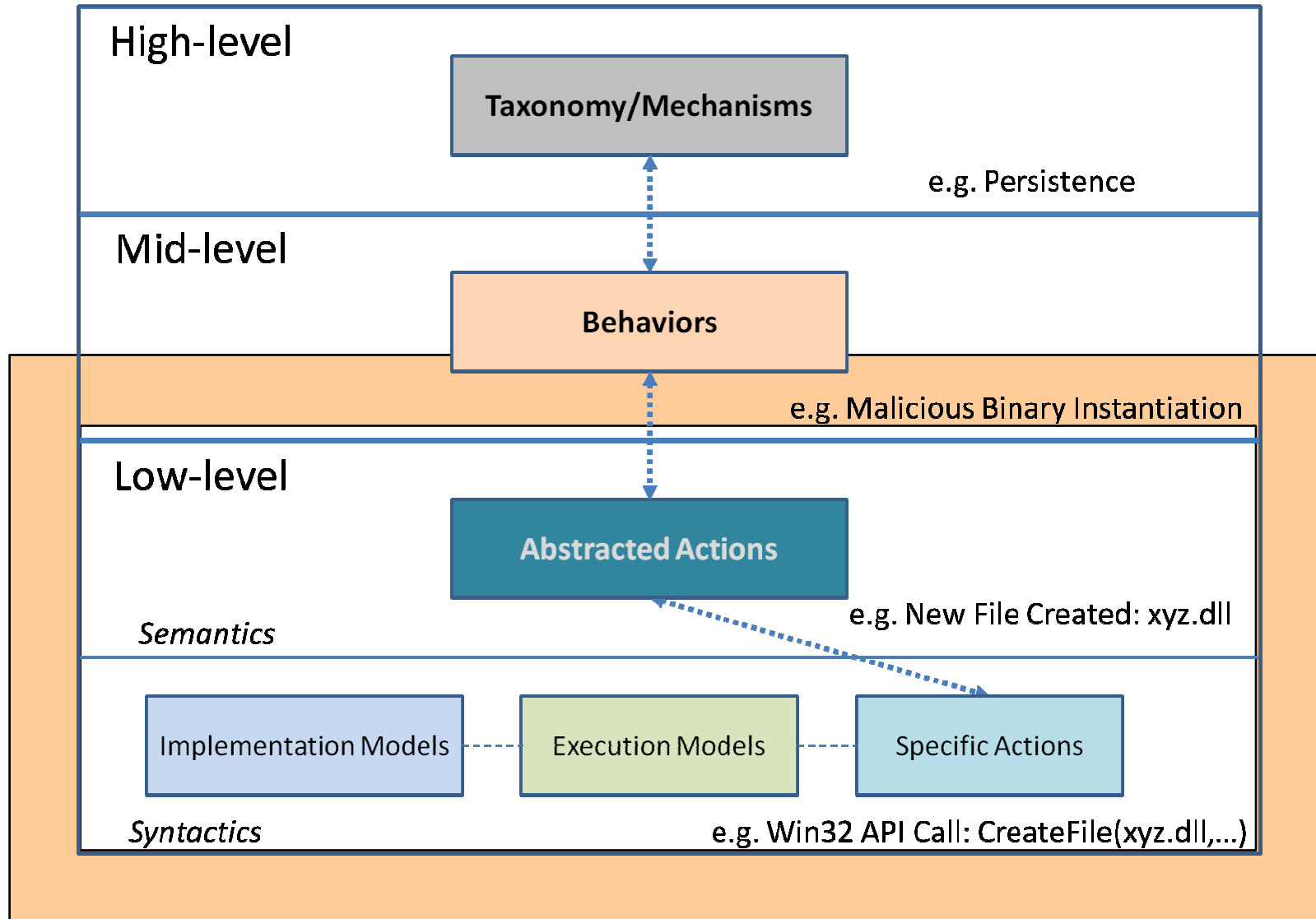
- Address concerns of potentially malicious code throughout the system lifecycle
- Develop a consensus on software that behaves in potentially malicious ways, to
 - Facilitate detection, analysis, response
 - Incorporate understanding of malware in threat and vulnerability analysis and risk assessment for system development and operational deployment
 - Enable users to make informed decisions about software



Malware Attribute Enumeration and Characterization (MAEC)

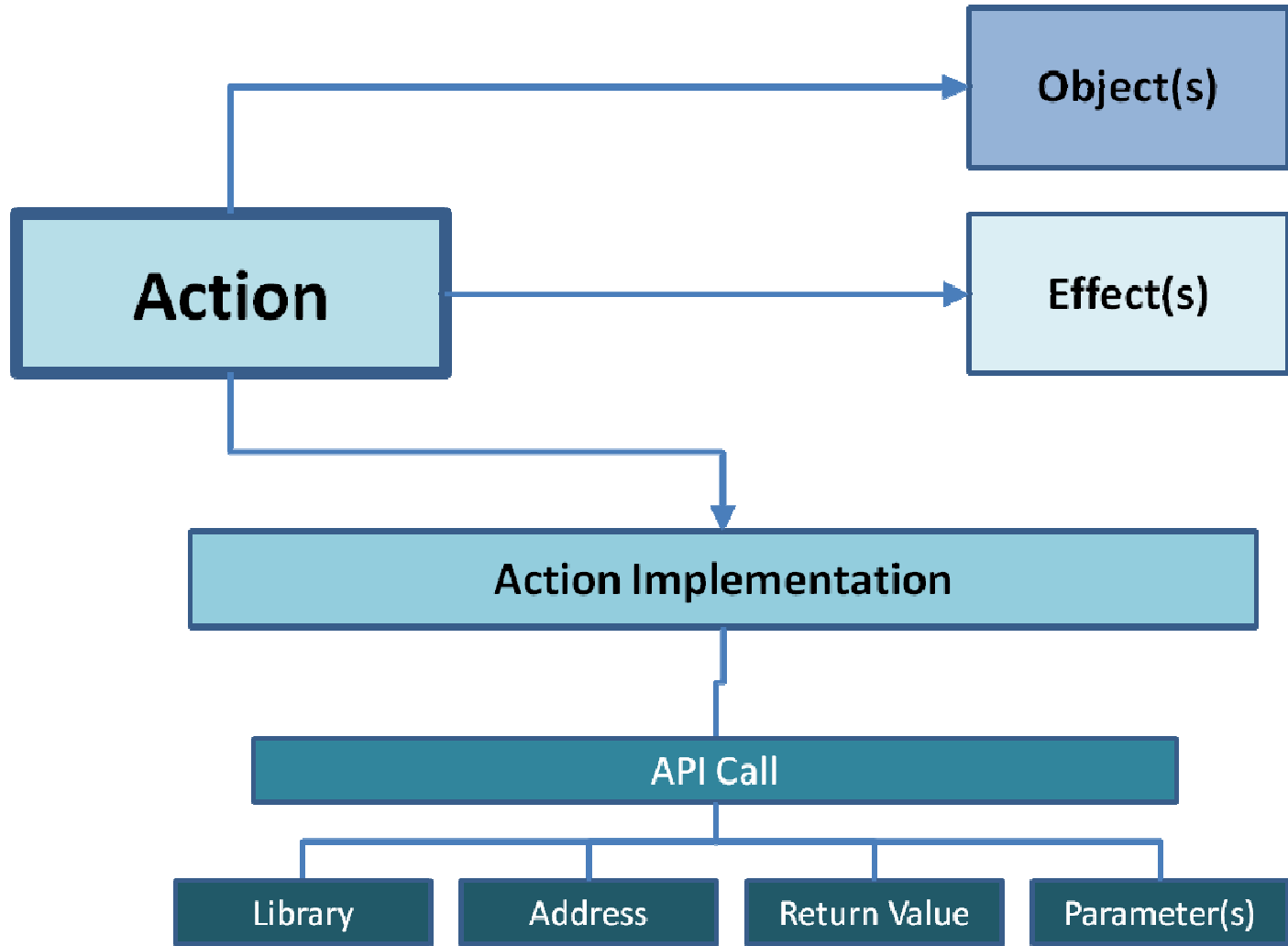


Current MAEC Overview



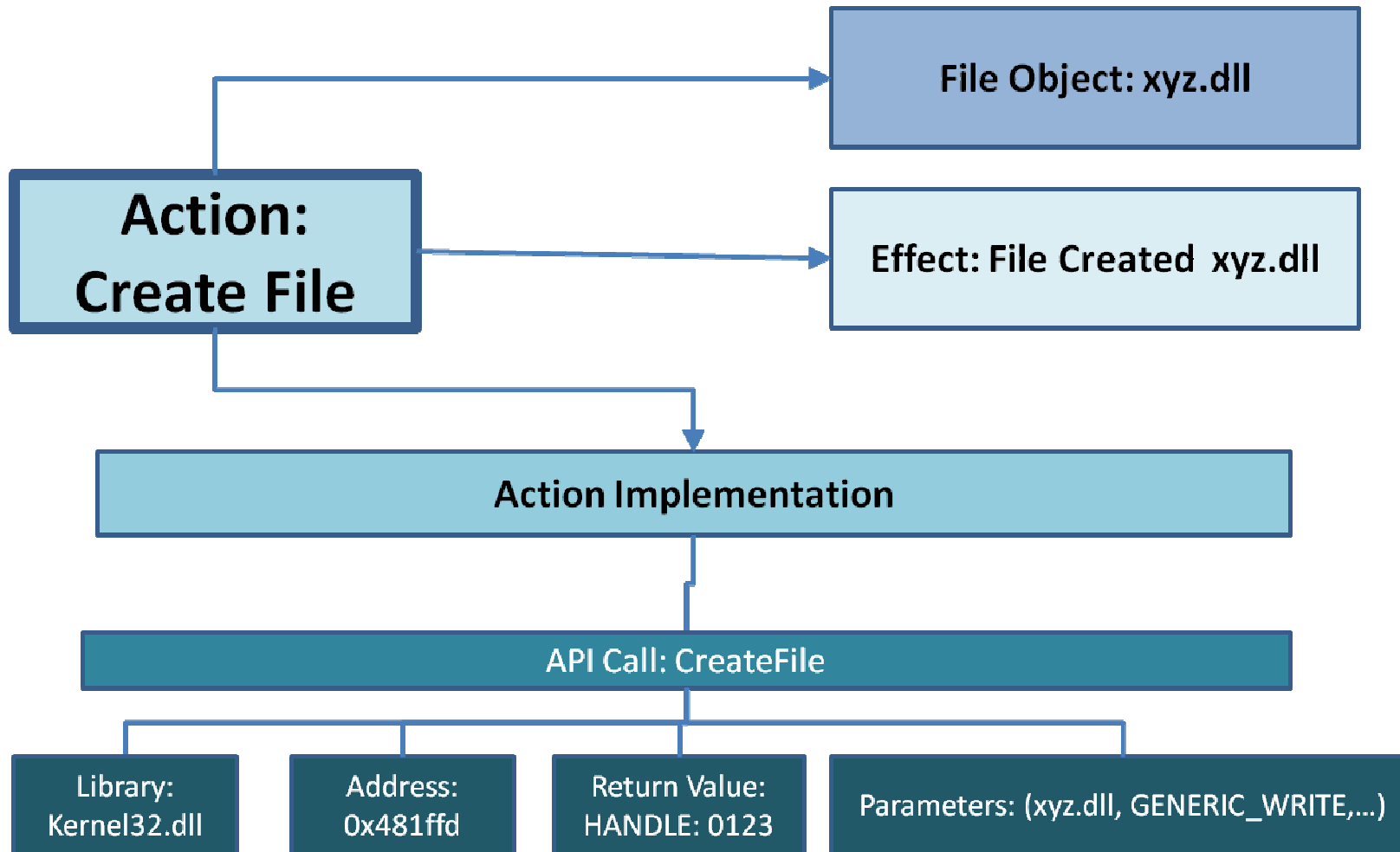


MAEC Action Model



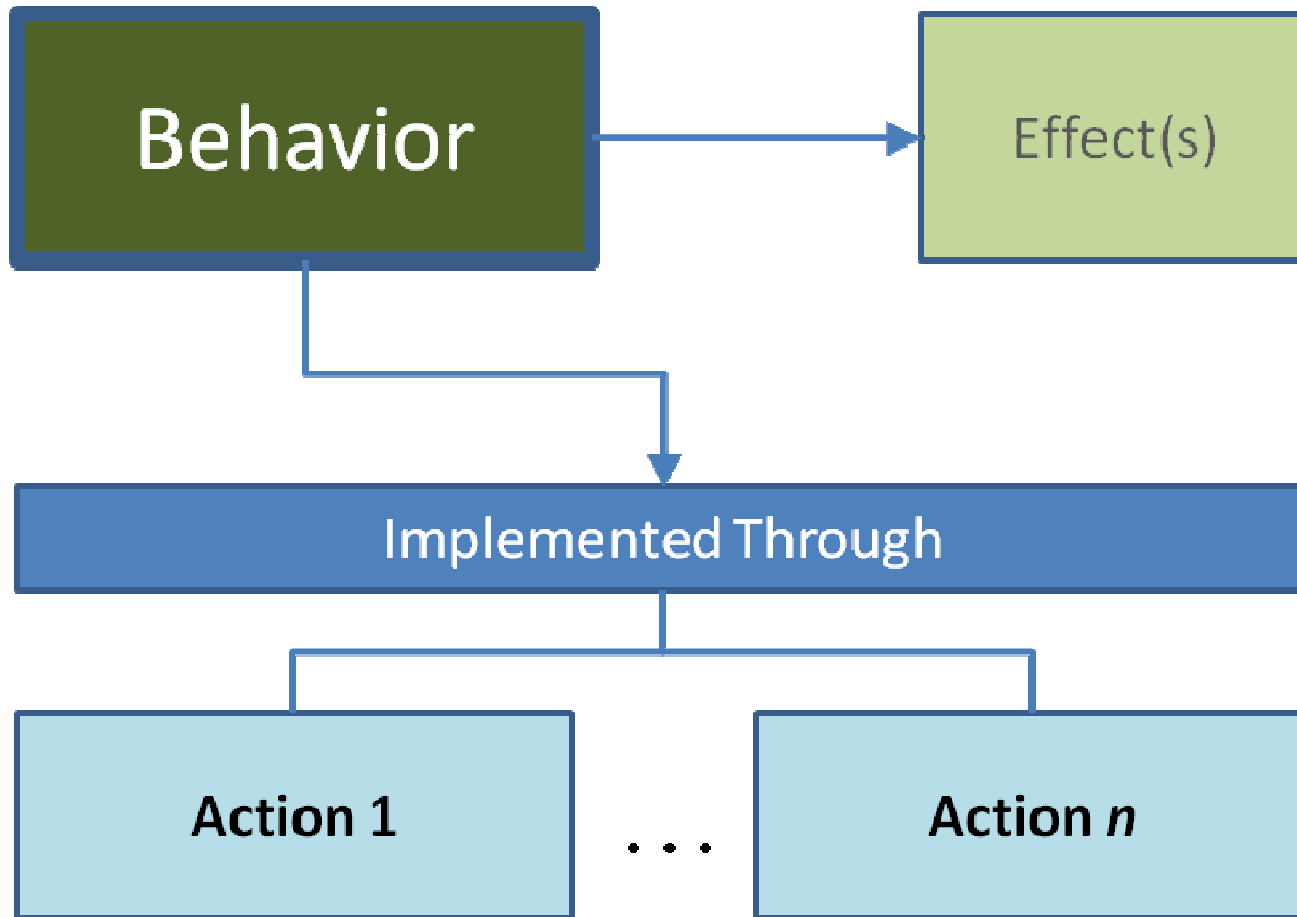


Action Example



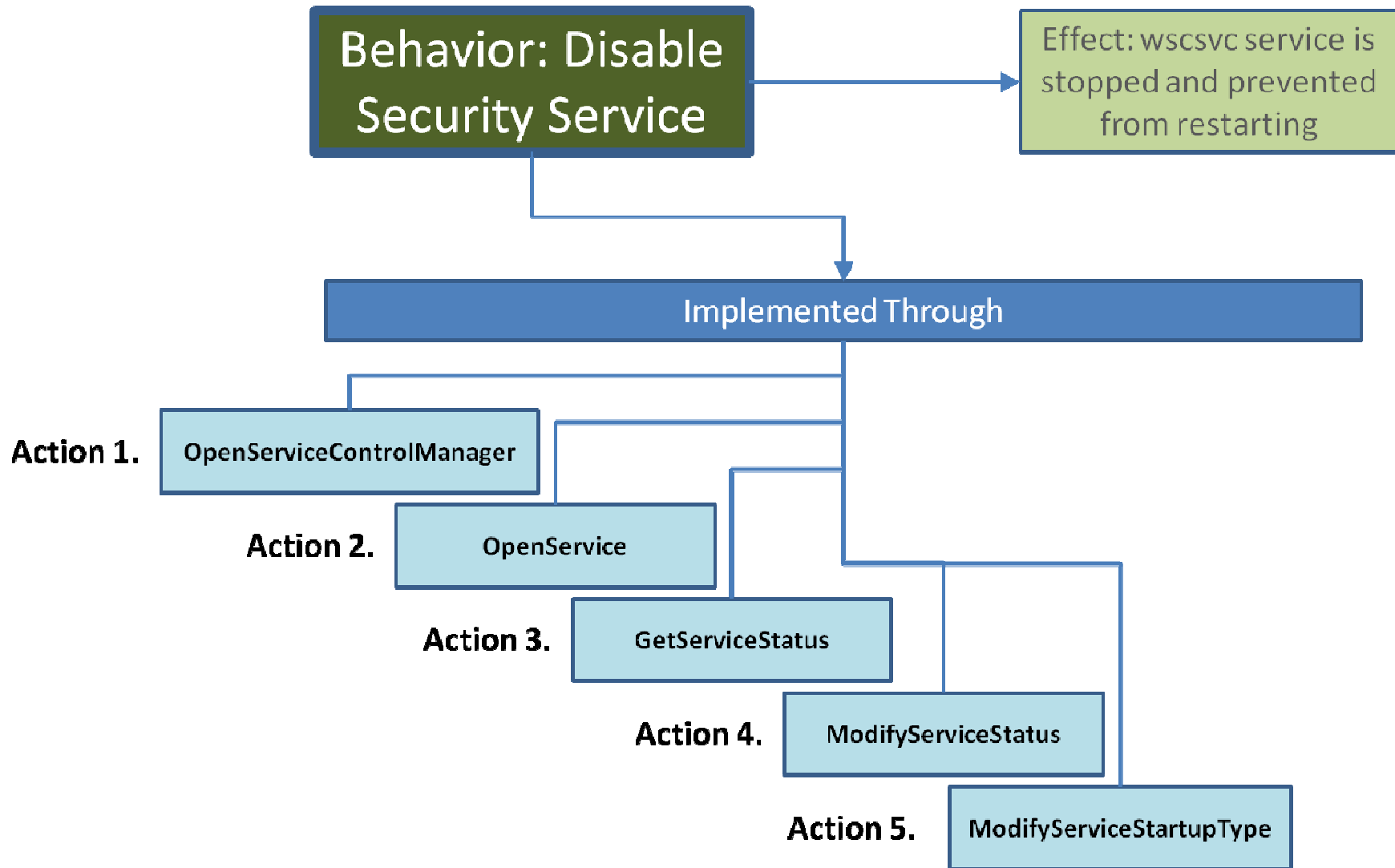


MAEC Behavior Model



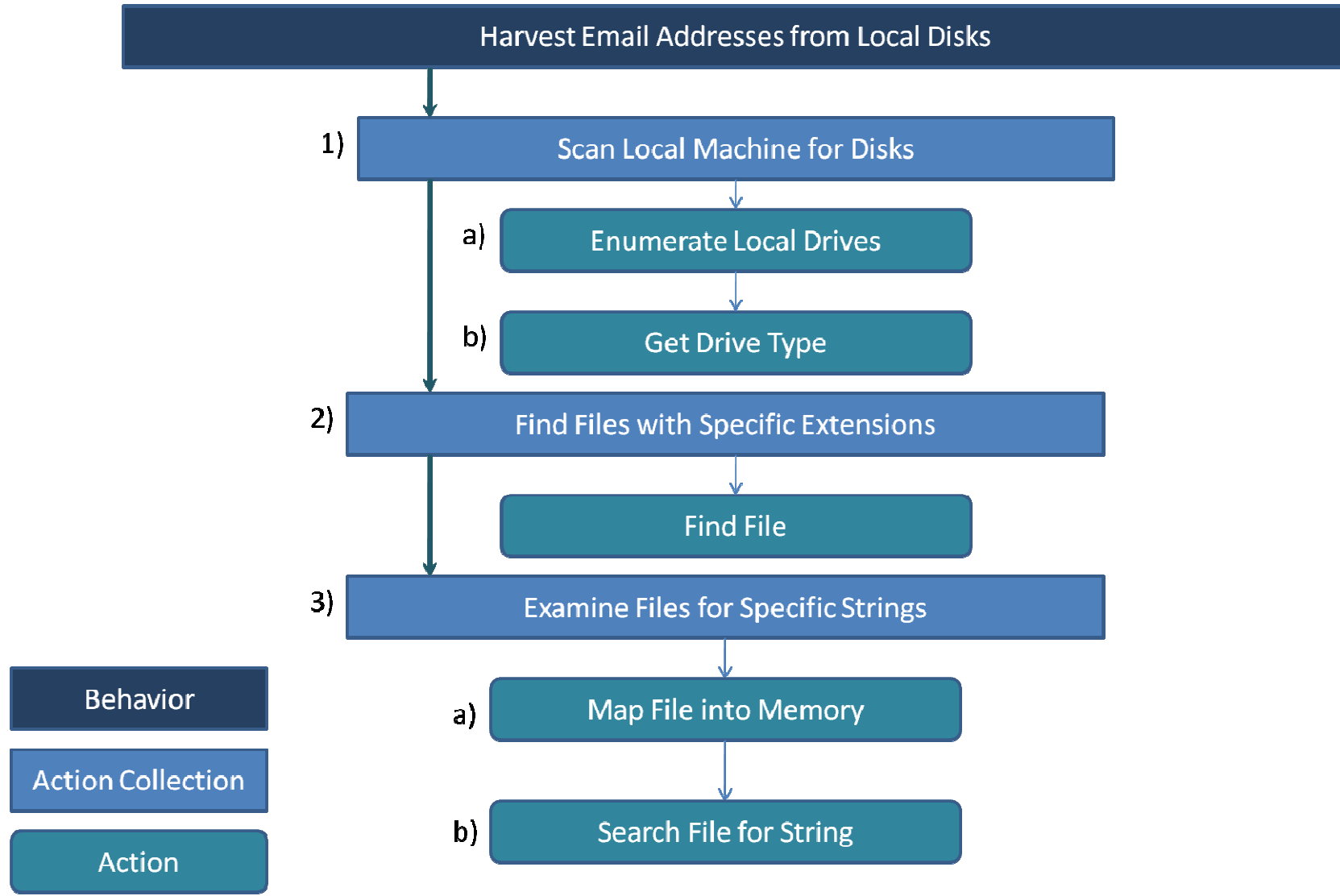


Basic Behavior Example



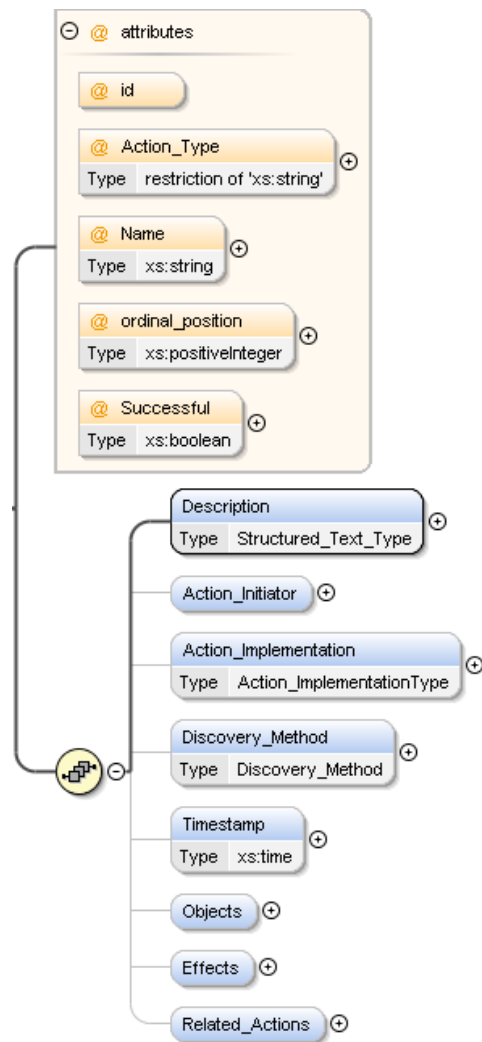


More Complex Behavior Example

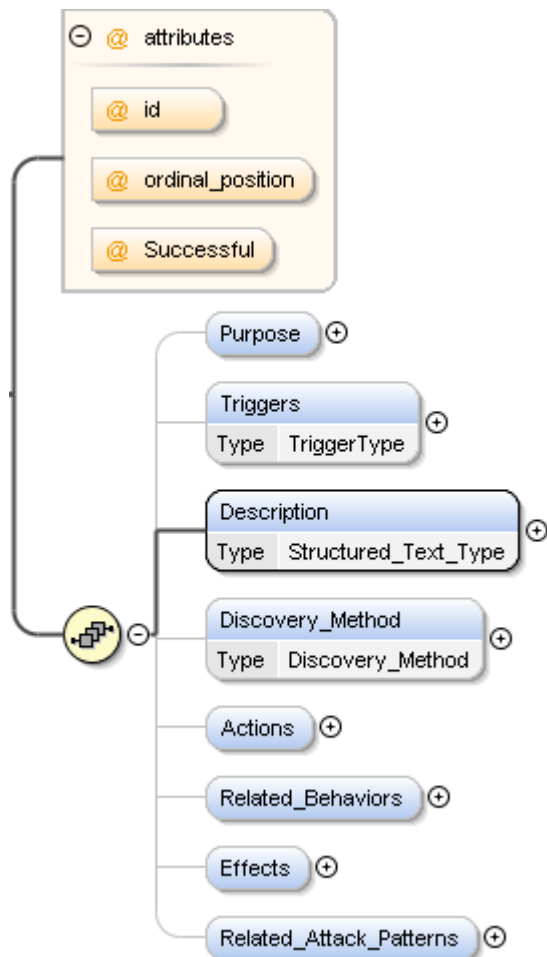


MAEC Schema Overview – Initial Release

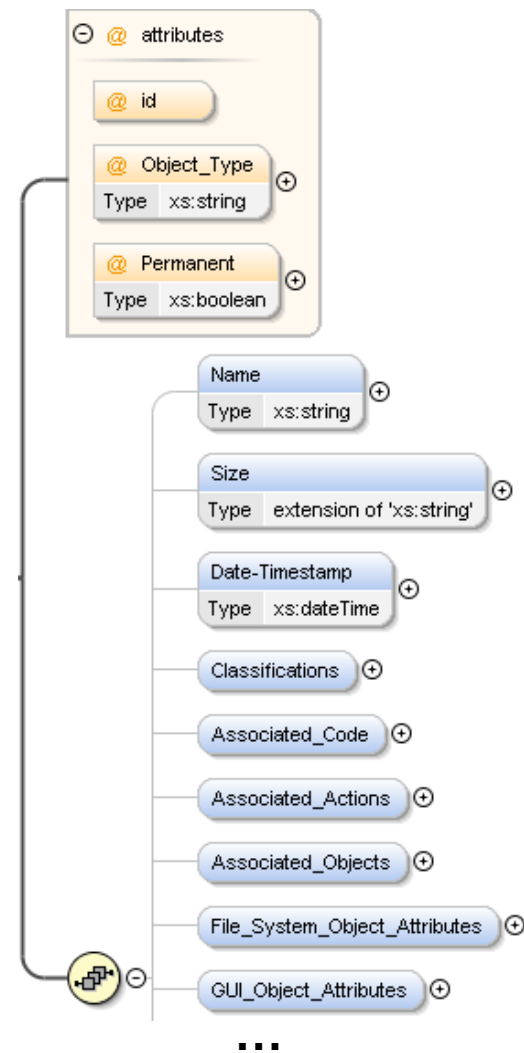
ActionType



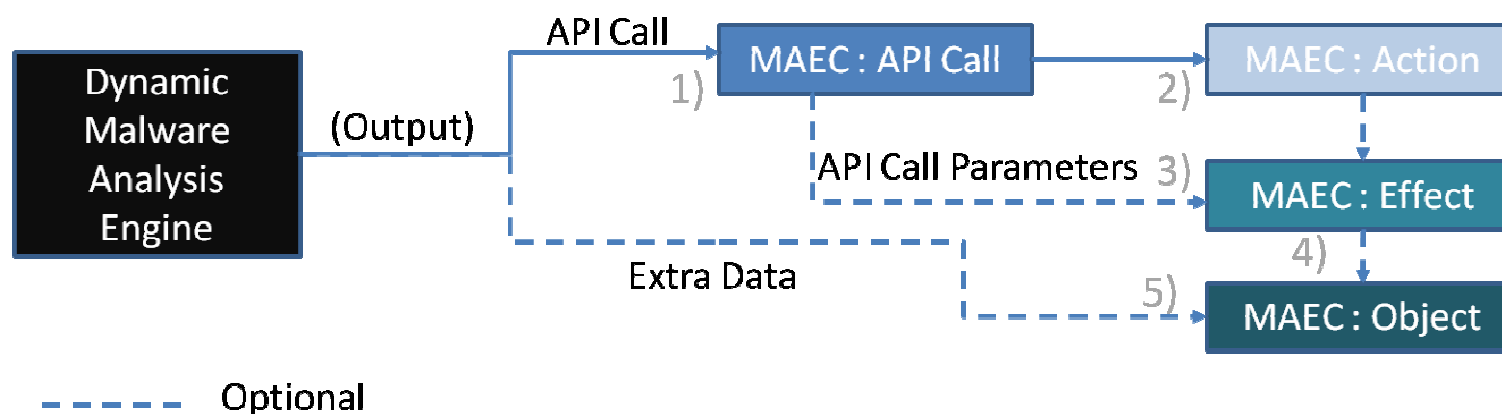
BehaviorType



ObjectType



Dynamic Malware Analysis <-> MAEC



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).

Test Case: CWSandbox Output -> MAEC

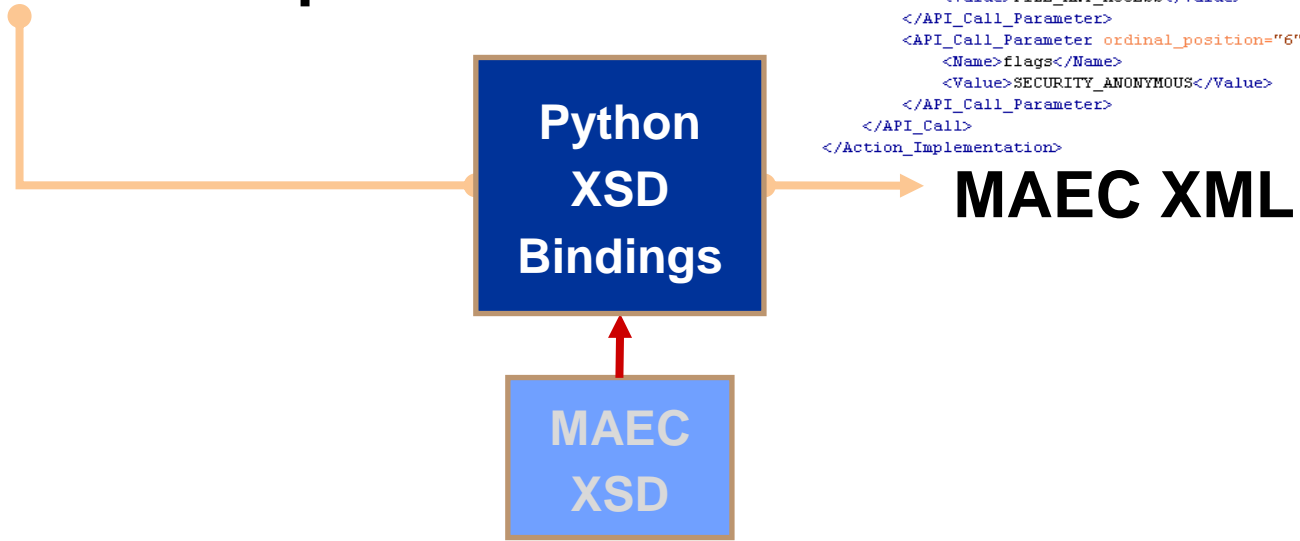
```

PID:1080,TID:1812,Caller:$00400000("KB823988.exe"),BEFORE,typFileSystem."FindFirstFile"
PID:1080,TID:1812,Caller:$00400000("KB823988.exe"),BEFORE,typFileSystem."SetFileAttrib
PID:1080,TID:1812,Caller:$00400000("KB823988.exe"),BEFORE,typFileSystem."DeleteFileW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegEnumKeyA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegEnumKeyA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegEnumValueW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegEnumValueW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExA"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegOpenKeyExW"
PID:1080,TID:1812,Caller:$77A80000("CRYPT32.dll"),AFTER,typRegistry."RegCreateKeyExW"
    
```

```

<Action Successful="true" id="10" Action_Type="copy" Name="copy_file">
  <Description/>
  <Action_Initiator type="Process">
    <Initiator_Name>KB823988.exe</Initiator_Name>
    <Process_ID>1080</Process_ID>
    <Thread_ID>1812</Thread_ID>
  </Action_Initiator>
  <Action_Implementation>
    <API_Call>
      <Name>CopyFileW</Name>
      <API_Call_Parameter ordinal_position="1">
        <Name>filetype</Name>
        <Value>file</Value>
      </API_Call_Parameter>
      <API_Call_Parameter ordinal_position="2">
        <Name>srcfile</Name>
        <Value>c:\\KB823988.exe</Value>
      </API_Call_Parameter>
      <API_Call_Parameter ordinal_position="3">
        <Name>dstfile</Name>
        <Value>C:\\WINDOWS\\system32\\ntos.exe</Value>
      </API_Call_Parameter>
      <API_Call_Parameter ordinal_position="4">
        <Name>creationdistribution</Name>
        <Value>CREATE_ALWAYS</Value>
      </API_Call_Parameter>
      <API_Call_Parameter ordinal_position="5">
        <Name>desiredaccess</Name>
        <Value>FILE_ANY_ACCESS</Value>
      </API_Call_Parameter>
      <API_Call_Parameter ordinal_position="6">
        <Name>flags</Name>
        <Value>SECURITY_ANONYMOUS</Value>
      </API_Call_Parameter>
    </API_Call>
  </Action_Implementation>
    
```

Raw CWSandbox Output





Collaboration and Outreach

- **Engaged with IEEE Industry Connections Security Group (ICSG) Malware Group**
 - MAEC team invited to be “guest” members
 - IEEE ICSG Malware Group Developed a Malware Metadata Exchange Schema
 - Oriented towards providing a mechanism for the sharing of sample data between AV product vendors
 - Current version:
<http://grouper.ieee.org/groups/malware/malwg/Schema1.1/>
 - MAEC imports portions of this schema, particularly with regards to sample prevalence and AV classification

MAEC Community: Discussion List

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

The screenshot shows a web browser window displaying the MAEC Discussion Archive. The browser's address bar shows the URL <http://maec.mitre.org/community/archive.html>. The page features the MAEC logo and the title "MAEC - Malware Attribute Enumeration and Characterization". Below the logo, there is a navigation menu with links for "About", "Community", "News & Events", and "Contact Us". The main content area is titled "Discussion Archive" and contains a search bar and a table of discussion topics. The table has columns for "Sub-Forums & Topics (26)", "Replies", "Last Post", and "Views".

Sub-Forums & Topics (26)	Replies	Last Post	Views
MAEC Updates by Kirillov, Ivan A.	0	Jun 18 by Kirillov, Ivan A.	1
schema thoughts - JP 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

- MITRE hosts a social networking collaboration environment: <https://handshake.mitre.org>
- Supplement to mailing list to facilitate collaborative schema development





Future Plans

- **Develop additional translators for dynamic analysis tools into MAEC XML**
- **Begin creation of process for cataloguing malware behaviors**
- **Expand and revise schema, particularly with regards to action attributes**
- **Collaborate with CAPEC & CWE teams in order to develop consensus approach on object/observable development**
- **Encourage and invite more participation in the development process**
 - MAEC Website: <http://maec.mitre.org> (contains MAEC Discussion list sign-up)
 - MAEC Handshake Group