OVAL Update

SACM Virtual Interim Meeting

03/09/2016

Agenda

- Status
- Background
- Logical Assessment Model
- OVAL Data Models and Processing Model
- Alignment with the SACM Vulnerability Assessment Scenario
- Next steps

Status

- Resolved IPR issues and submitted the OVAL data models in I-D format
  - draft-cokus-sacm-oval-common-model[1]
  - draft-haynes-sacm-oval-definitions-model[2]
  - draft-haynes-sacm-oval-variables-model[3]
  - draft-rothenberg-sacm-oval-system-characteristics-model[4]
  - draft-cokus-sacm-oval-results-model[5]
  - draft-rothenberg-sacm-oval-directives-model[6]
  - draft-haynes-sacm-oval-processing-model[7]

- Updated OVAL and SACM Information Model I-D[8]
  - Explains submission, intended use, and alignment with the SACM Vulnerability Assessment Scenario[9]

1. https://datatracker.ietf.org/doc/draft-cokus-sacm-oval-common-model/
2. https://datatracker.ietf.org/doc/draft-haynes-sacm-oval-definitions-model/
3. https://datatracker.ietf.org/doc/draft-haynes-sacm-oval-variables-model/
4. https://datatracker.ietf.org/doc/draft-rothenberg-sacm-oval-sys-char-model/
5. https://datatracker.ietf.org/doc/draft-cokus-sacm-oval-results-model/
6. https://datatracker.ietf.org/doc/draft-rothenberg-sacm-oval-directives-model/
7. https://datatracker.ietf.org/doc/draft-haynes-sacm-oval-processing-model/
8. https://datatracker.ietf.org/doc/draft-hansbury-sacm-oval-info-model-mapping/
9. https://datatracker.ietf.org/doc/draft-coffin-sacm-vuln-scenario/

Background

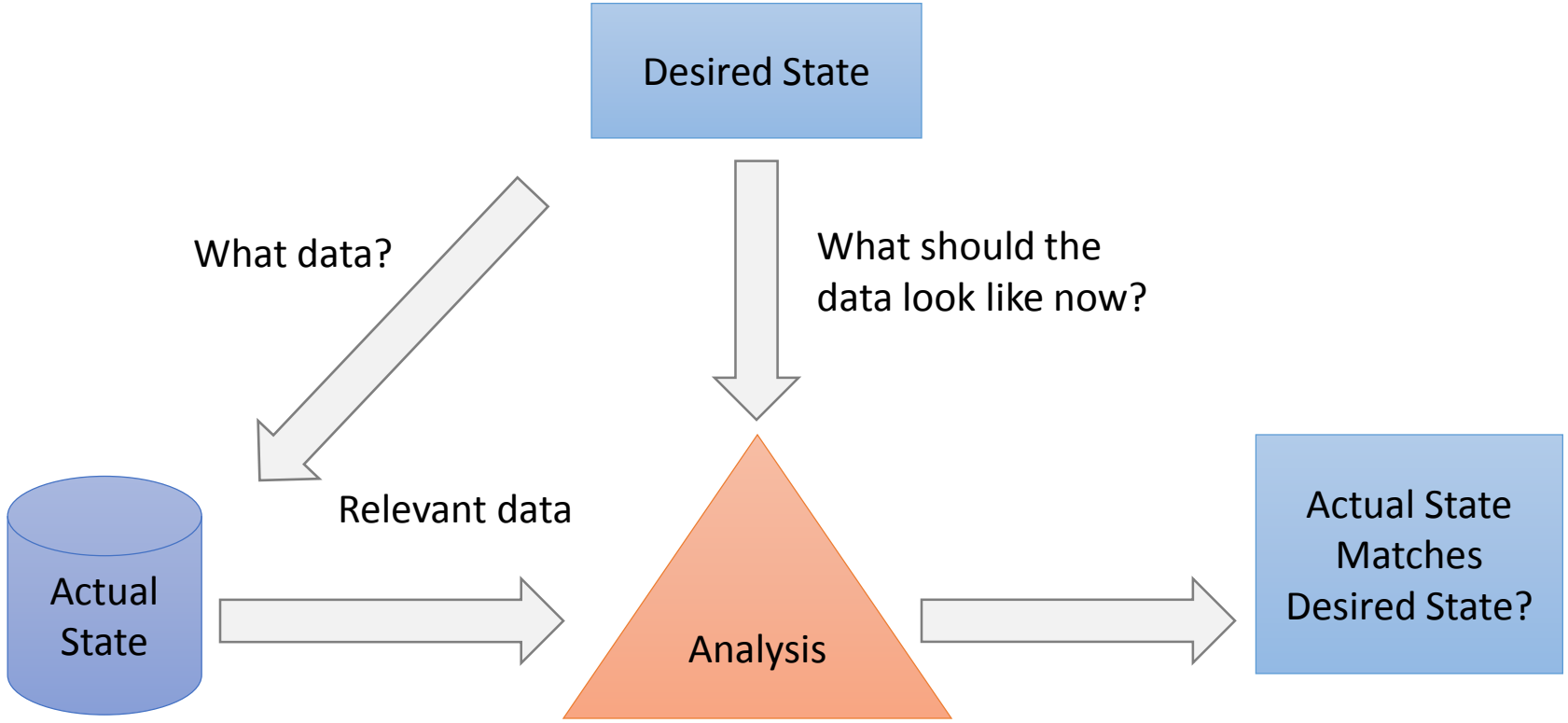
- XML-based language that encodes the details of the assessment of an endpoint
  - Founded in 2002 as a community-driven effort
  - Operated by the MITRE Corporation on behalf of DHS

- Widely adopted
  - Supported by 47 organizations, with 65 products and services, across 13 countries[1]
  - Primary checking language for the Security Content Automation Protocol (SCAP)[2]

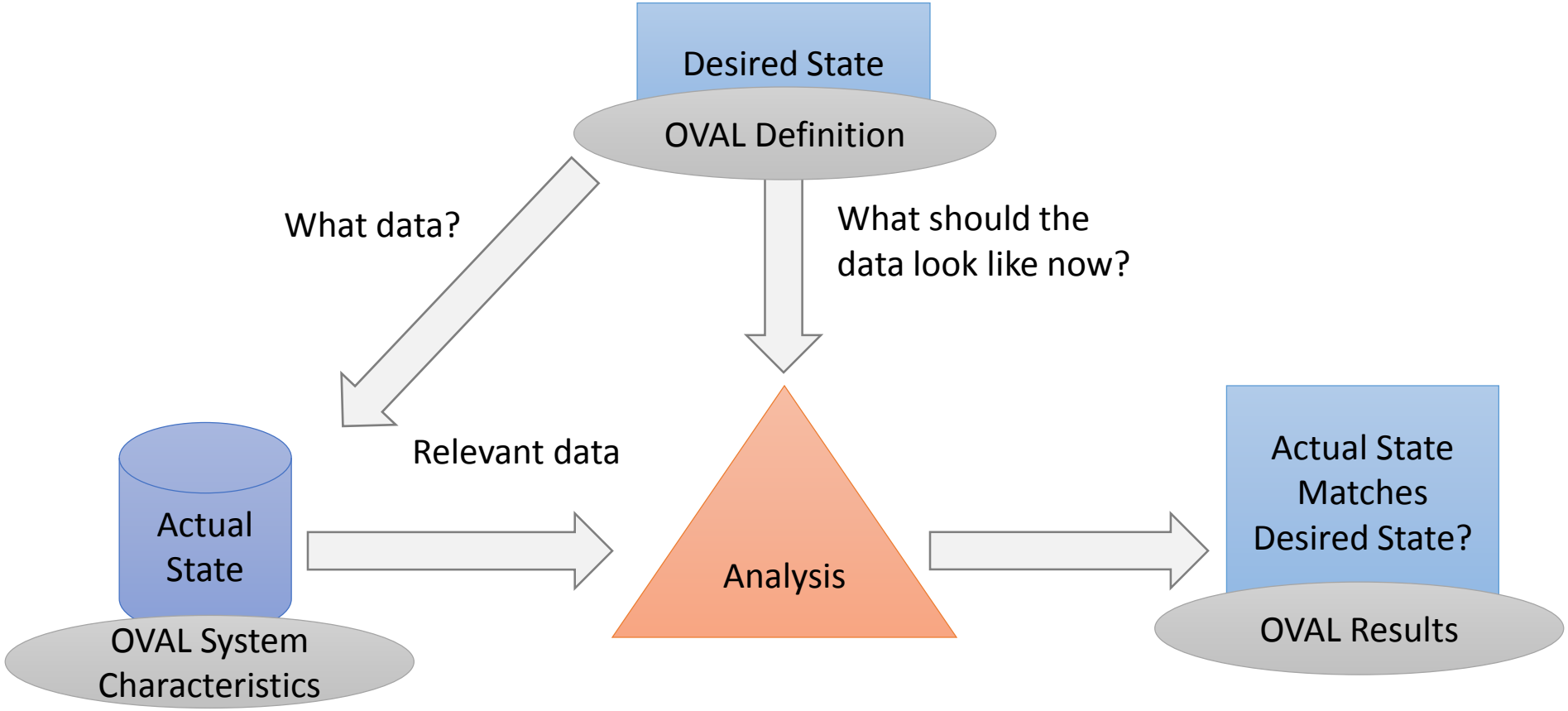
- Transitioned to industry
  - Transferred to CIS on behalf of the OVAL community to support existing products
  - Transferred to SACM as a potential starting point for the next generation standards
  - No expectation of compatibility between the versions developed by the OVAL community and SACM

1. https://oval.mitre.org/adoption/participants.html
2. http://scap.nist.gov/

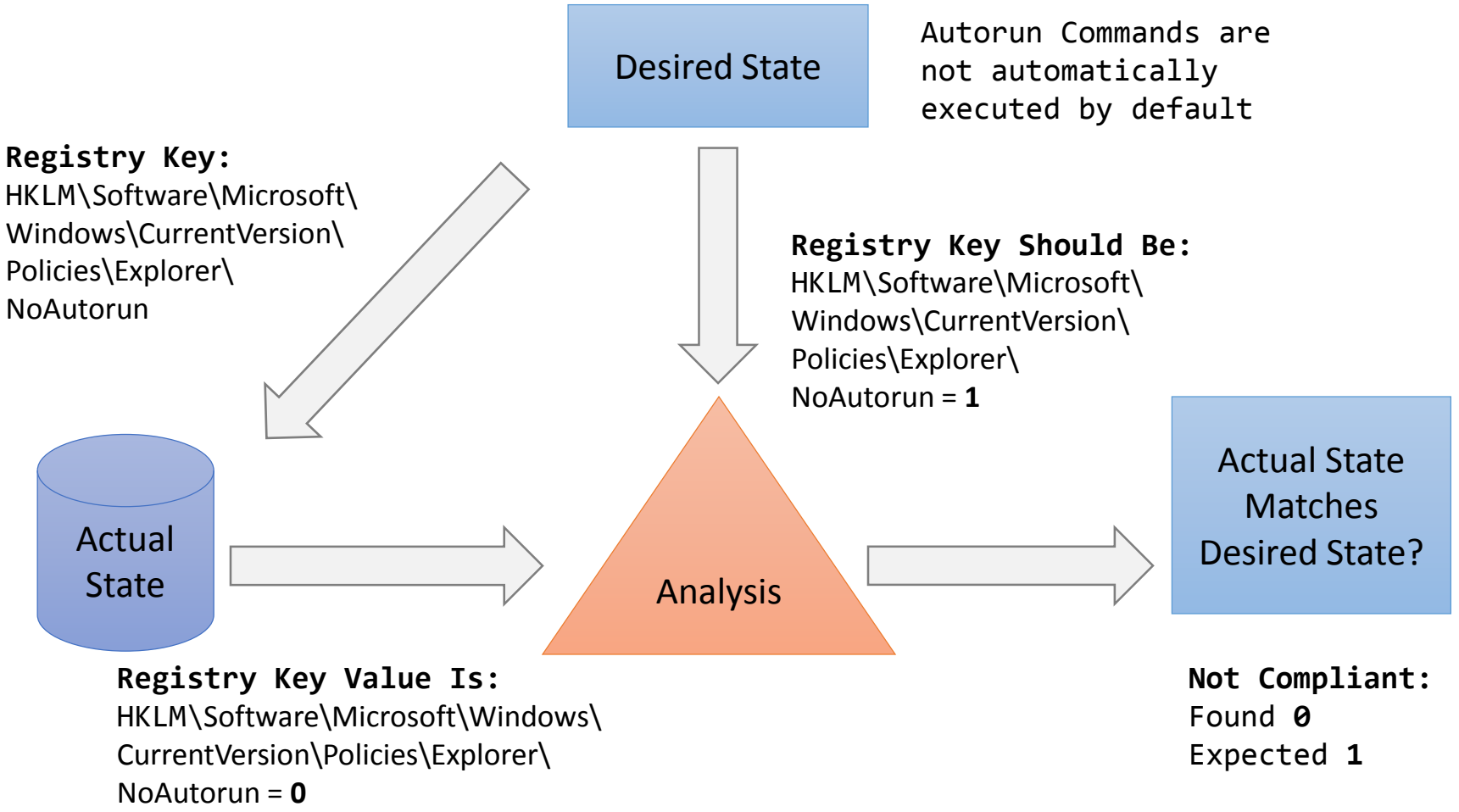
Logical Assessment Model



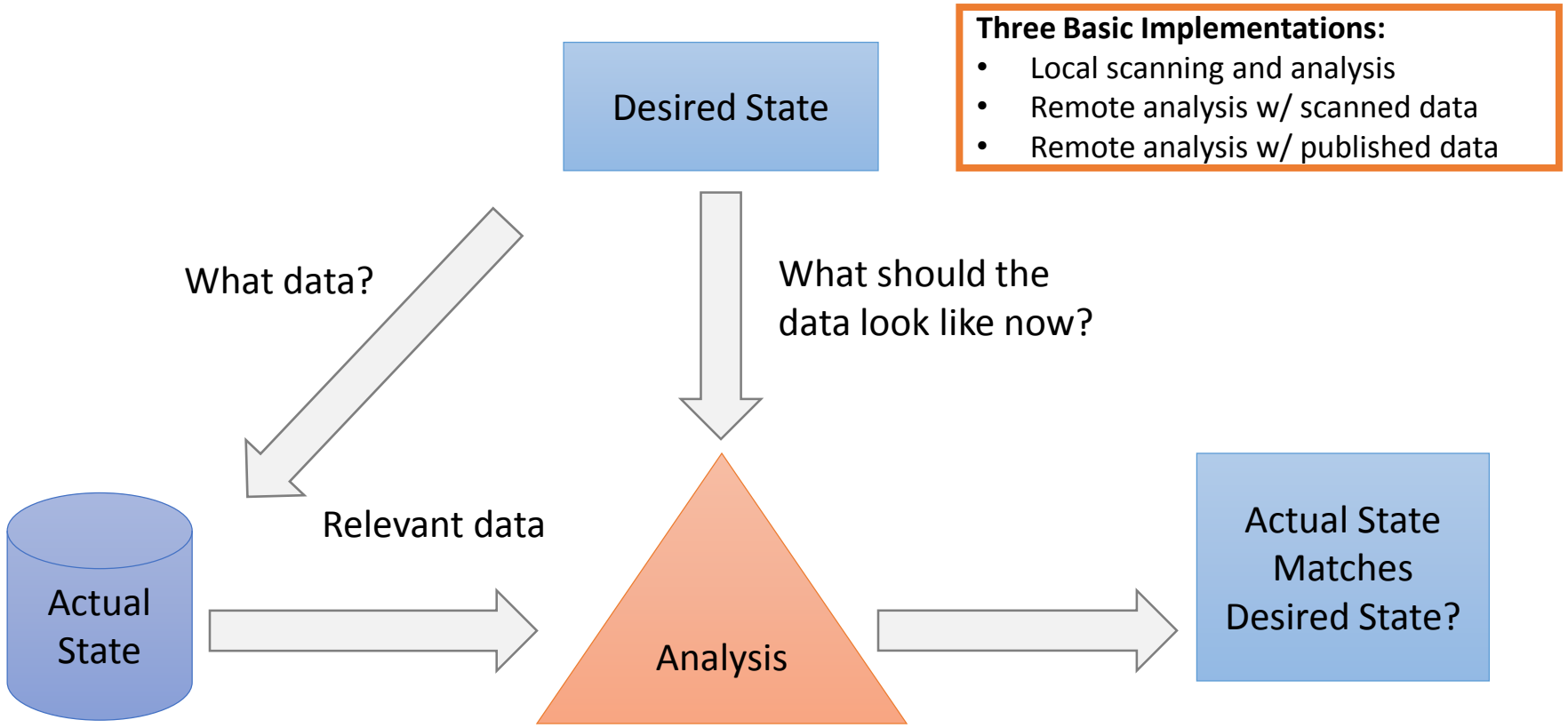
Logical Assessment Model



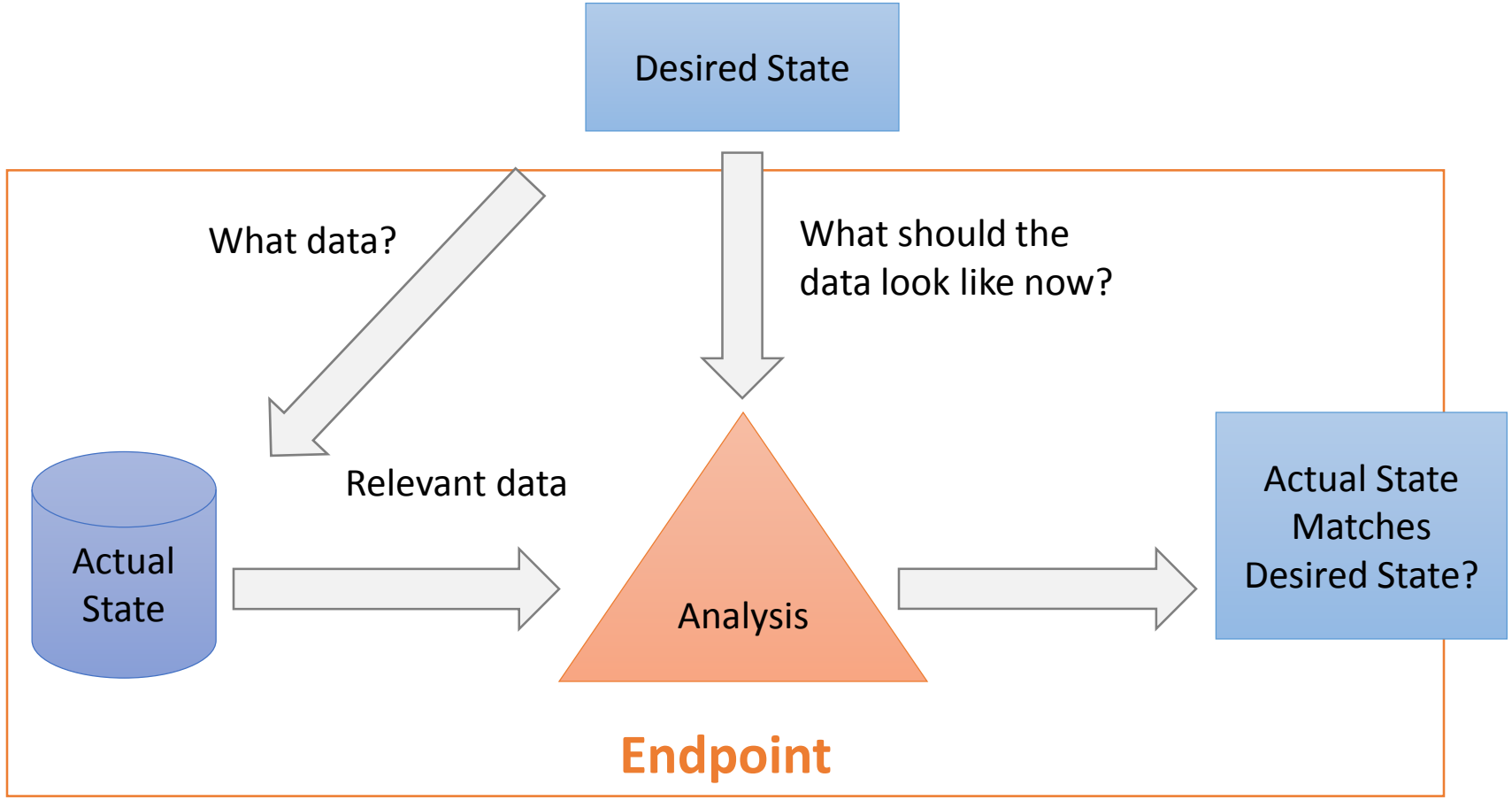
Logical Assessment Model



Logical Assessment Model

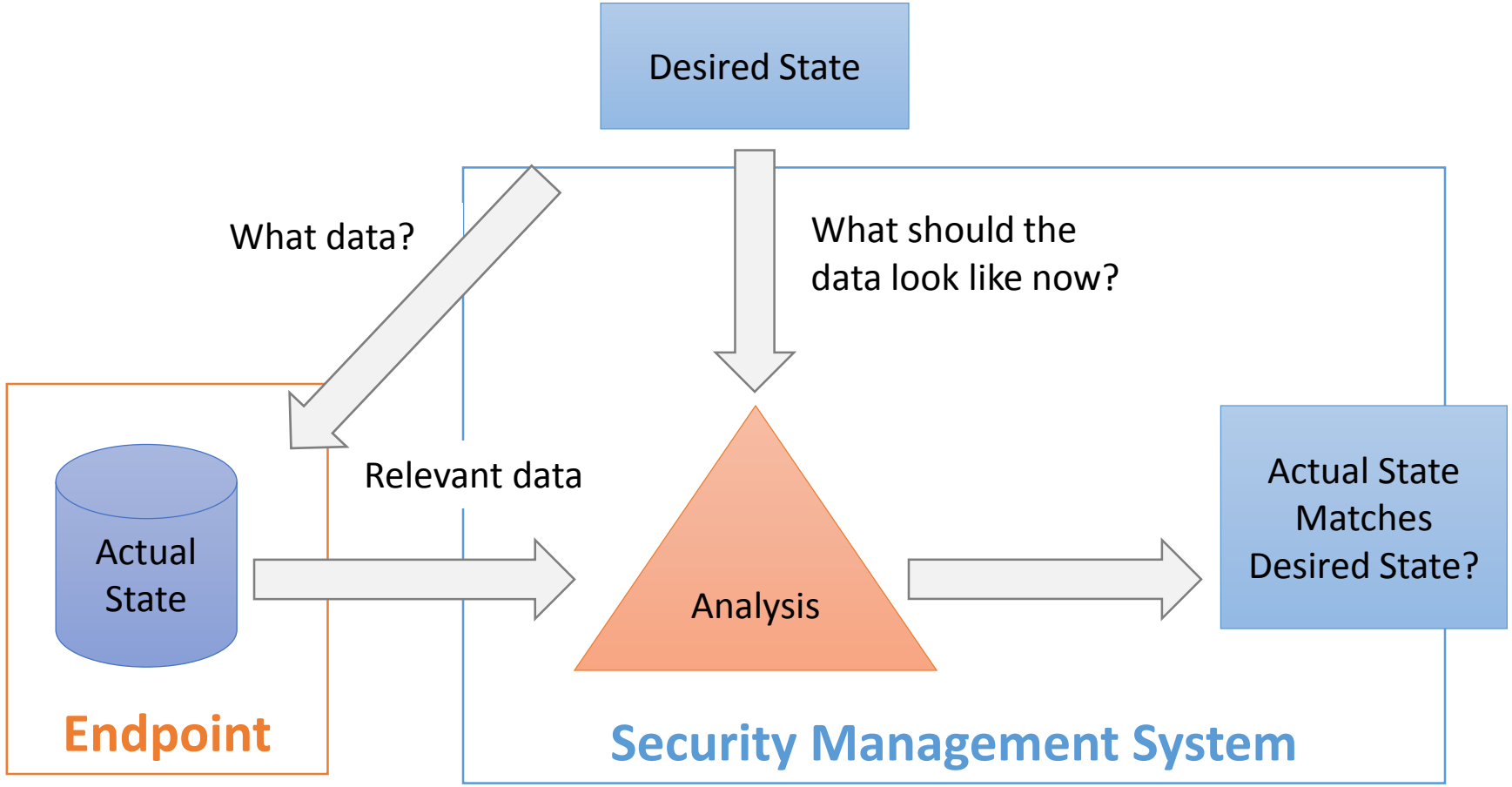


Assessment Model – Local Scanning



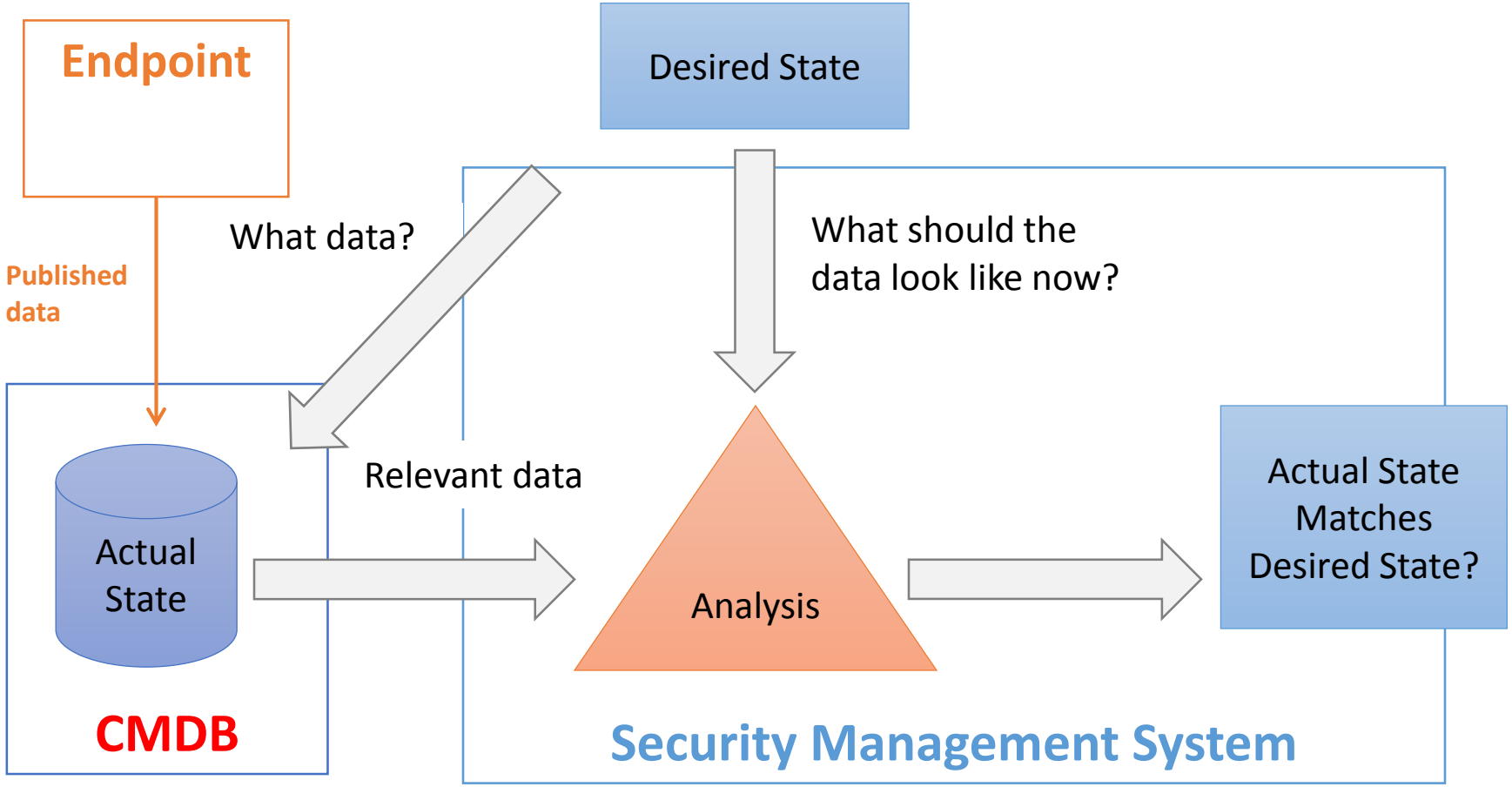
Many security vendors follow this implementation.

Assessment Model – Scanned Data



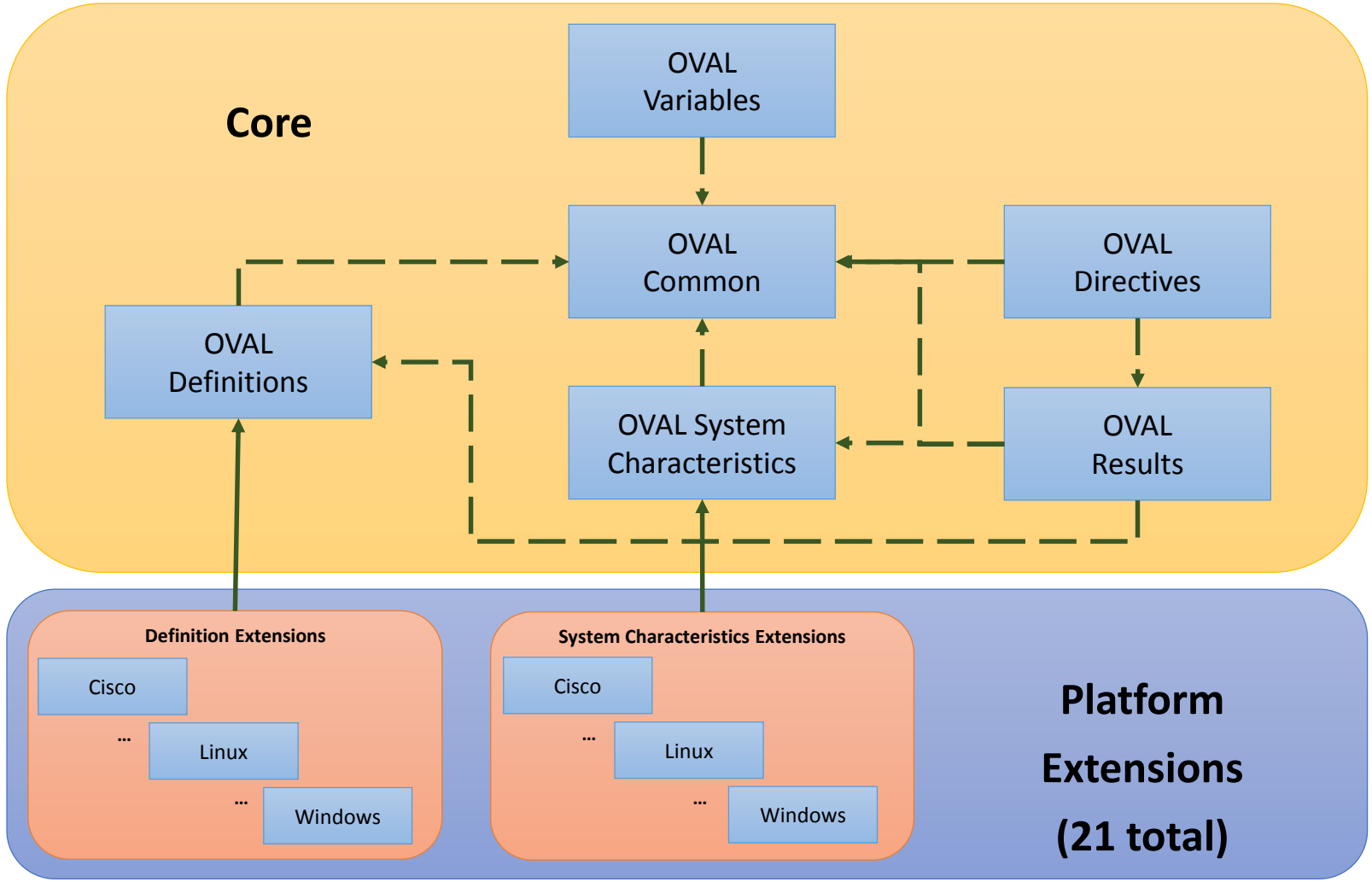
The original OVAL implementation.

Assessment Model – Published Data



The original OVAL implementation.

OVAL Data Model



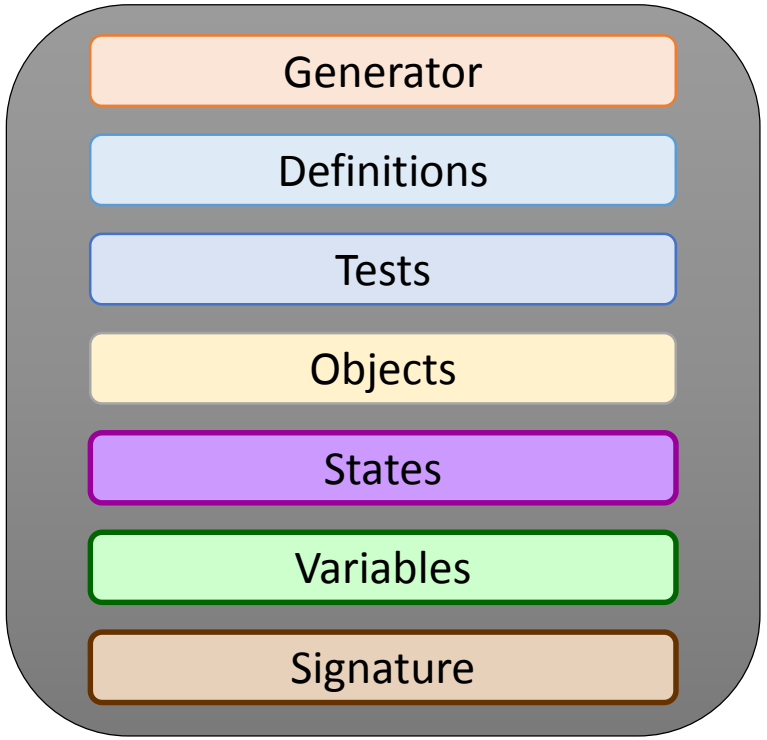
OVAL Common Model

- Defines constructs and enumerations that are reused throughout the OVAL Data Models

- Includes:
  - Generator
  - Message
  - Notes
  - Check Enumeration
  - Definition Classes
  - Data Type Enumeration
  - Operation Enumeration
  - Operator Enumeration
  - Existence Enumeration
  - Family Enumeration
  - OVAL Identifiers

OVAL Definitions Model

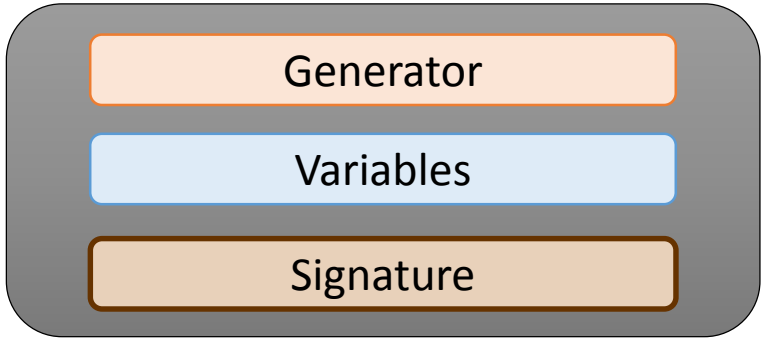
- Defines an extensible framework for making assertions about the desired state of an endpoint



```
<oval_definitions ...>
  <generator>...</generator>
  <definitions>
    <definition class="compliance" id="oval:gov.nist.usgcb.windowsseven:def:258" ...>
      <metadata>...</metadata>
      <criteria operator="AND">
        <extend_definition comment="Windows 7 is installed" definition_ref="oval:gov.nist.cpe.oval:def:1"/>
        <criterion comment="Default behavior for AutoRun = var" test_ref="oval:gov.nist.usgcb.windowsseven:tst:100055"/>
      </criteria>
    </definition>
    ...
  </definitions>
  <tests>
    <registry_test check="all" check_existence="at_least_one_exists" id="oval:gov.nist.usgcb.windowsseven:tst:100055"...>
      <object object_ref="oval:gov.nist.usgcb.windowsseven:obj:100055"/>
      <state state_ref="oval:gov.nist.usgcb.windowsseven:ste:100055"/>
    </registry_test>
    ...
  </tests>
  <objects>
    <registry_object id="oval:gov.nist.usgcb.windowsseven:obj:100055" ...>
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>Software\Microsoft\Windows\CurrentVersion\Policies\Explorer</key>
      <name>NoAutorun</name>
    </registry_object>
    ...
  </objects>
  <states>
    <registry_state id="oval:gov.nist.usgcb.windowsseven:ste:100055" ...>
      <type>reg_dword</type>
      <value datatype="int" operation="equals" var_ref="oval:gov.nist.usgcb.windowsseven:var:100055"/>
    </registry_state>
    ...
  </states>
  <variables>
    <external_variable datatype="int" id="oval:gov.nist.usgcb.windowsseven:var:100055" .../>
  </variables>
</oval_definitions>
```

OVAL Variables Model

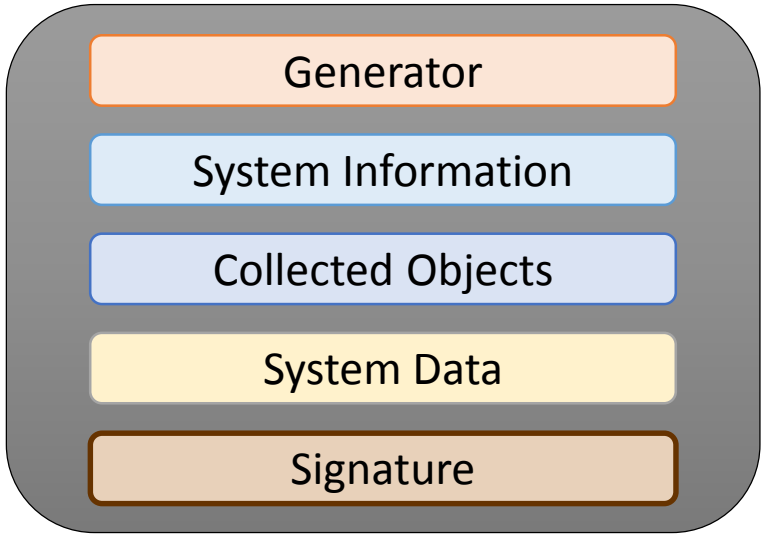
- Defines a framework for externally specifying OVAL Variables that can used by OVAL Definitions at run-time



```
<oval_variables ...>
  <generator>
    <oval:schema_version>5.11.1</oval:schema_version>
    <oval:timestamp>2015-10-28T23:06:29.903-04:00</oval:timestamp>
    ...
  </generator>
  <variables>
    <variable id="oval:gov.nist.usgcb.windowsseven:var:100055" datatype="int"...>
      <value>1</value>
    </variable>
  </variables>
</oval_variables>
```

OVAL System Characteristics Model

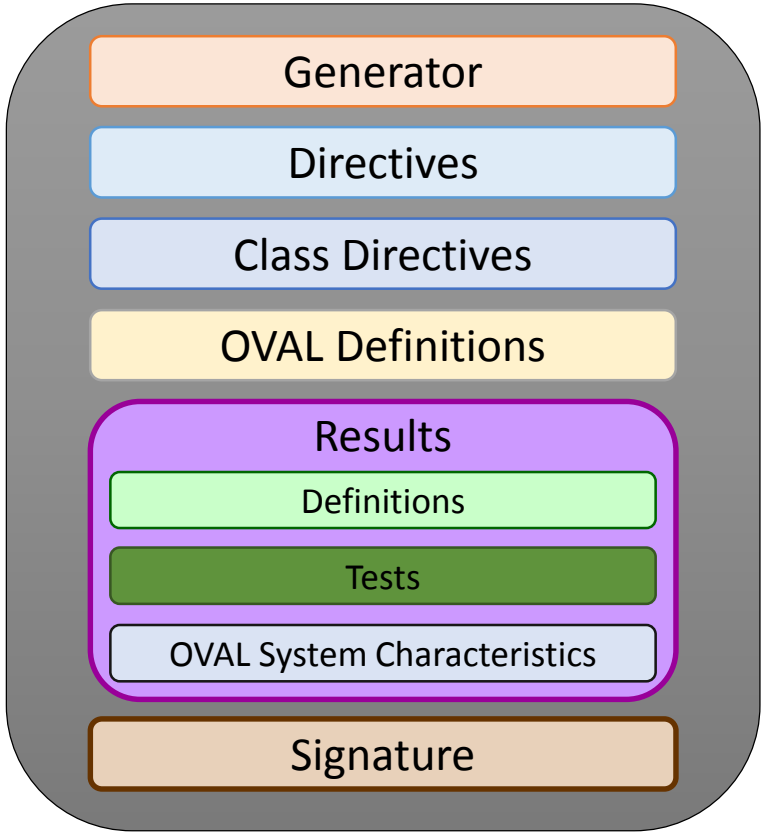
- Defines a framework for representing the actual state of an endpoint



```
<oval_system_characteristics ...>
  <generator>...</generator>
  <system_info>
    <os_name>Microsoft Windows 7 Professional</os_name>
    <os_version>6.1.7601 Service Pack 1</os_version>
    <architecture>AMD64</architecture>
    <primary_host_name>HOSTNAME.EXAMPLE.COM</primary_host_name>
    <interfaces>
      <interface>
        <interface_name>Intel(R) Centrino(R)...</interface_name>
        <ip_address>192.168.1.5</ip_address>
        <mac_address>AB-CD-EF-01-23-34</mac_address>
      </interface>
    </interfaces>
  </system_info>
  <collected_objects>
    <object flag="complete" id="oval:gov.nist.usgcb.windowsseven:obj:100055" ...>
      <reference item_ref="1"/>
    </object>
    ...
  </collected_objects>
  <system_data>
    <registry_item id="1" ...>
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key>Software\Microsoft\Windows\CurrentVersion\Policies\Explorer</key>
      <name>NoAutorun</name>
      <last_write_time datatype="int">130625756830667820</last_write_time>
      <type>reg_dword</type>
      <value datatype="int">1</value>
      <windows_view>64_bit</windows_view>
    </registry_item>
    ...
  </system_data>
</oval_system_characteristics>
```

OVAL Results Model

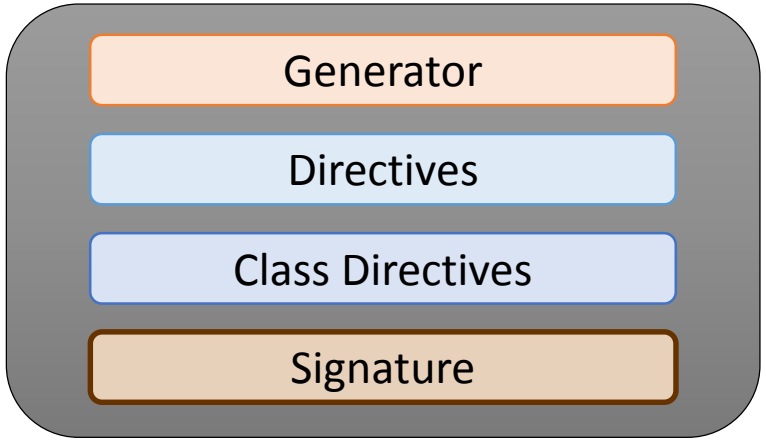
- Defines extensible framework for expressing the outcome of the assessment of the actual state and desired state of an endpoint



```
<oval_results ...>
  <generator>...</generator>
  <directives include_source_definitions="true">...</directives>
  <oval_definitions ...>...</oval_definitions>
  <results>
    <system>
      <definitions>
        <definition definition_id="oval:gov.nist.usgcb.windowsseven:def:258" result="error" ...>
          <criteria operator="AND" result="error">
            <extend_definition definition_ref="oval:gov.nist.cpe.oval:def:1" result="true" .../>
            <criterion result="error" test_ref="oval:gov.nist.usgcb.windowsseven:tst:100055" .../>
          </criteria>
        </definition>
        <definition definition_id="oval:gov.nist.cpe.oval:def:1" result="true" ...>
          <criteria operator="AND" result="true">
            <criterion result="true" test_ref="oval:org.mitre.oval:tst:999" .../>
            <criterion result="true" test_ref="oval:org.mitre.oval:tst:10792" .../>
          </criteria>
        </definition>
      </definitions>
      <tests>
        <test check="only one" check_existence="at_least_one_exists" result="true" state_operator="AND"
              test_id="oval:org.mitre.oval:tst:999" ...>
          <tested_item item_id="2" result="true"/>
        </test>
        <test check="at least one" check_existence="at_least_one_exists" result="true" state_operator="AND"
              test_id="oval:org.mitre.oval:tst:10792" ...>
          <tested_item item_id="3" result="true"/>
        </test>
        <test check="all" check_existence="at_least_one_exists" result="error" state_operator="AND"
              test_id="oval:gov.nist.usgcb.windowsseven:tst:100055" ...>
          <tested_item item_id="1" result="not evaluated"/>
        </test>
      </tests>
      <oval_system_characteristics ...>...</oval_system_characteristics>
    </system>
  </results>
</oval_results>
```

OVAL Directives Model

- Defines a framework for controlling the level of detail in an OVAL Results document



```
<oval_directives ...>
  <generator>...</generator>
  <directives include_source_definitions="false">
    <oval-res:definition_true content="thin" reported="true"/>
    <oval-res:definition_false content="thin" reported="true"/>
    <oval-res:definition_unknown content="thin" reported="true"/>
    <oval-res:definition_error content="thin" reported="true"/>
    <oval-res:definition_not_evaluated content="thin" reported="true"/>
    <oval-res:definition_not_applicable content="thin" reported="true"/>
  </directives>
</oval_directives>
```

OVAL Processing Model

- Producing OVAL Definitions
- Producing OVAL System Characteristics
- Producing OVAL Results

Producing OVAL Definitions

- Convert prose guidance into machine readable content that expresses the desired state of an endpoint
  - Security advisories, configuration policy, threat indicators, etc.
  - This is difficult

- Often a manual process working directly with XML
  - No fully featured OVAL editors
  - Organizations have developed scripts to generate content

Producing OVAL System Characteristics

- Generate a snapshot of the actual state of an endpoint
  - System information that accurately describes an endpoint
  - Collect the actual state data with or without OVAL Objects
  - Record the actual state data as OVAL Items

- Typically generated by tools

Producing OVAL Results

- Evaluate OVAL Definitions against OVAL System Characteristics
  - Definition Evaluation
  - Test Evaluation
  - Object Evaluation
  - State Evaluation
  - Variable Evaluation

- Typically generated by tools

Alignment with the SACM Vulnerability Assessment Scenario

- Endpoint identification and initial data collection
  - Guidance to drive the collection of endpoint identification and characterization data
  - Express endpoint data in a format that is consumable by other tools
- Endpoint applicability and secondary assessment
  - Evaluate endpoint identification and characterization data to determine vulnerability description data applicability and vulnerability status
- Assessment results
  - Express the results of an evaluation

Next steps

- Consider recommendations provided in the OVAL and SACM Information Model I-D

- Determine which data models we want to use to inform our work
  - Prioritize (Collection Guidance, Posture Attributes, Results, etc.)
  - Select data model implementation (e.g., JSON, XML, etc.)

- Develop highest priority data model leveraging OVAL concepts and lessons learned