# OVAL Results Tutorial


MITRE

# Agenda

- Process Model
- OVAL Results Tutorial
  - The Basics
    - OVAL Results document
  - Advanced Topics
    - Thin vs Full


MITRE

# OVAL Results

- XML encoding of the results of an analysis
  - which systems are vulnerable?
  - which systems are non-compliant?
  - which patches should be installed?

- Includes the details
  - why are you vulnerable?
  - why are you non-compliant?
  - why should a patch be installed?

MITRE

# The OVAL Process

1

**Security advisories**

Vendors and leading security organizations publish security advisories that warn of current threats and system vulnerabilities.

**Configuration policy**

Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

2

OVAL Definitions

**Definitions are generated**

Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

3

**Data collected from computers**

OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

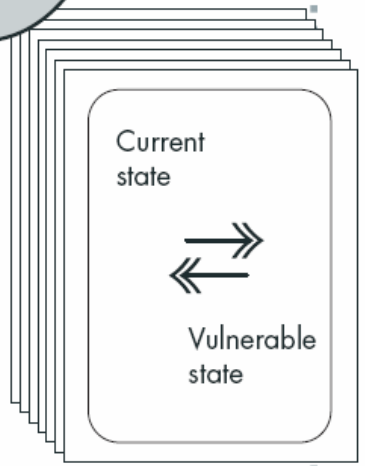
OVAL System Characteristics

4

OVAL Analysis

**Analysis**

The OVAL Definitions from Step 2, and the System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not.




5

**Analysis results**

Results of analysis are formatted as an OVAL Results document.

OVAL Results


MITRE

# Thin vs Full

- A value of 'thin' means only a minimal amount of information is provided.
  - Schematron rules

- A value of 'full' means that very detailed information is provided
  - allowing in-depth reports to be generated from the results.

MITRE

# Thin Results

```
...
<results>

  <system>
    <definitions>
      <definition definition_id="" version="1“ result="true">
      <definition definition_id="" version="1“ result="true">
      <definition definition_id="" version="1“ result="true">
      <definition definition_id="" version="1“ result="true">
    </definitions>
  </system>

  <system>
  ...
  </system>

  </results>
  ...
```

MITRE

# Full Results

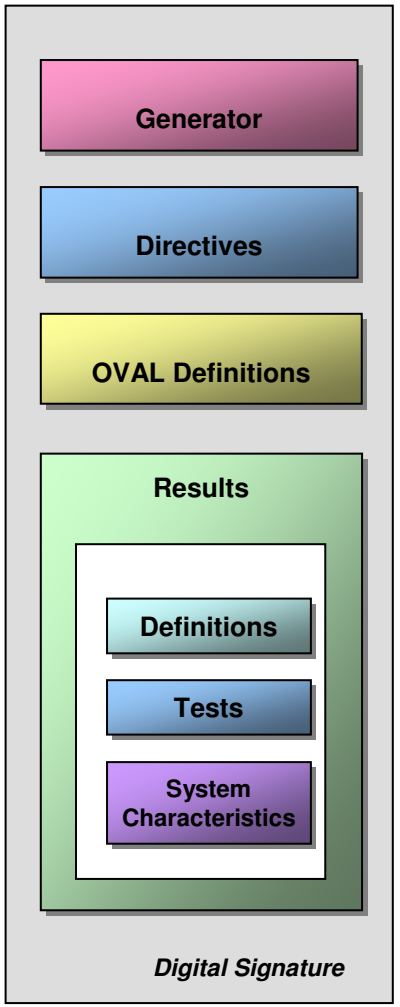
```
...
 <results>

   <system>
     <definitions>
       <definition definition_id="" version="1" result="true">
         <criteria operator="AND" result="false">
           <criterion test_ref="" version="1" result="true"/>
           <criterion test_ref="" version="1" result="true"/>
         </criteria>
       </definition>
     </definitions>
     <tests>
       <test test_id="" version="2" check="at least one" result="true">
         <tested_item item_id="1" result="true"/>
         <tested_item item_id="1" result="true"/>
         <tested_variable variable_id="">C:\WINDOWS\</tested_variable>
       </test>
     </tests>
     <oval_system_characteristics>
   </system>

 </results>
 ...
```

# Advanced Topics


MITRE

# An OVAL Results File

- Generator
- Directives
- OVAL Definitions
- Results
- Digital Signature



# Generator Section

- Information about how the OVAL Document was created
  - product name
  - product version
  - schema version
  - timestamp
- Not about the content, but about the document!

```
<generator>
      <oval:product_name>OVAL Definition
Interpreter</oval:product_name>
      <oval:product_version>4.2</oval:product_version>
      <oval:schema_version>5.0</oval:schema_version>
      <oval:timestamp>2006-10-12T18:13:45</oval:timestamp>
</generator>
```

MITRE

# Directives Section

- Reports on the contents of the results document

```
<directives>
    <definition_true reported="true“ content="full"/>
    <definition_false reported=“false"/>
    <definition_unknown reported="true" content=“thin"/>
    <definition_error reported=“false"/>
    <definition_not_evaluated reported="true" content=“thin" />
    <definition_not_applicable reported="true" content=“thin" />
</directives>
```

MITRE

# OVAL Definitions Section

- An exact copy of the definitions evaluated
- Optional
- When used along with full results allows for a complete snapshot of the evaluation results in one document.

MITRE

# Results Section

- Evaluation results for a set of definitions
- Any number of system results
- Each system has
  - Definitions section
  - Tests section
  - System characteristics section

MITRE

# Result Values

- Possible result attribute values
  - True
  - False
  - Unknown
  - Error
  - Not evaluated
  - Not applicable

MITRE

# Signing OVAL Documents

- Defined by the XML-Signature Syntax and Processing W3C Recommendation

- Enveloped Signature - The signature is over the XML content that contains the signature as an element.