OVAL System Characteristics Tutorial

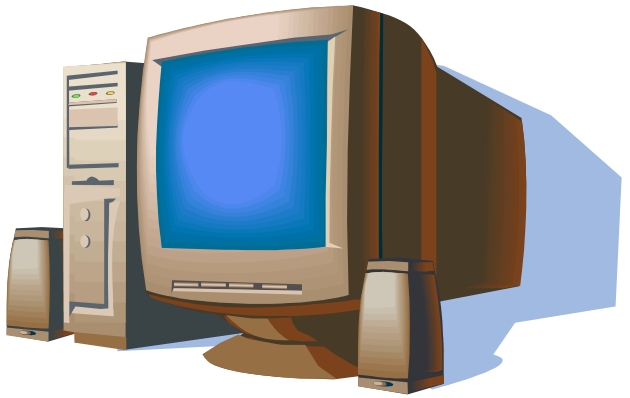
MITRE

Agenda

- Overview
- OVAL SC Tutorial
  - The Basics
    - SC structure
  - Advanced Topics
    - Incomplete Collection
    - Missing Objects

OVAL System Characteristics

- XML encoding of the details of a system
  - file versions
  - running processes
  - patches installed
  - etc.
- provides a snapshot of the system
  - save for auditing purposes
  - use for analysis



MITRE

Use Cases

- database
- historical snapshot
- drive OVAL evaluation
  - past and present
- what if scenarios

MITRE

File is Complete

- assumption is that file is complete
  - if object doesn't exist on system, then it needs to be recorded in SC file that it doesn't exist
    - can't just be left out

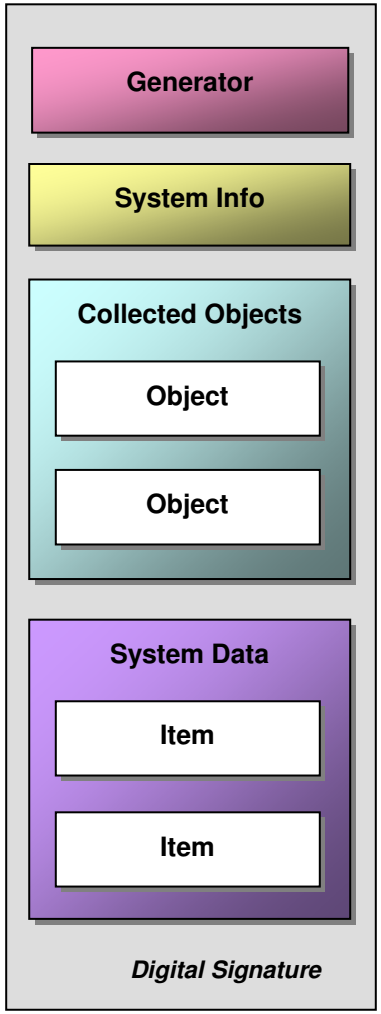
MITRE

Advanced Topics

MITRE

An OVAL SC File

- Generator
- System Info
- Collected Objects
- System Data
- 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>5.3</oval:product_version>
      <oval:schema_version>5.3</oval:schema_version>
      <oval:timestamp>2006-10-12T18:13:45</oval:timestamp>
</generator>
```

MITRE

System Info Section

- Identifies the system from which the set of data was collected.
  - Primary host name
  - Operating System name & version
  - Interfaces

```
<system_info>
   <os_name>Microsoft Windows XP Professional Service Pack 2</os_name>
   <os_version>5.1.2600</os_version>
   <architecture>INTEL32</architecture>
   <primary_host_name>MyHostName.example.com</primary_host_name>
   <interfaces>
     <interface>
       <interface_name>Broadcom NetXtreme ...</interface_name>
       <ip_address>192.68.0.10</ip_address>
       <mac_address>00-11-22-AA-BB-33</mac_address>
     </interface>
   </interfaces>
 </system_info>
```

MITRE

Collected Objects Section

- Provides a mapping from the objects specified by an OVAL Definition to the set of items collected on a host.

```
<collected_objects>
  ...
  <object flag="complete" id="oval:org.mitre.oval:obj:281" version="1">
    <reference item_ref="2"/>
  </object>
  <object flag="complete" id="oval:org.mitre.oval:obj:38" version="1">
    <variable_value variable_id="oval:org.mitre.oval:var:200">C:\Program
    Files</variable_value>
    <reference item_ref="3"/>
  </object>
  ...
</collected_objects>
```

MITRE

Flag Attribute

- Holds information about the attempt to collect the system data specified by an object.

- Possible values:
  - Error
  - Complete
  - Incomplete
  - Does not exist
  - Not collected
  - Not applicable

MITRE

System Data Section

- The set of items found on the host system.
  - Actual data (reg keys, file attrs, permissions, etc.)

```
<system_data>
    ...
    <file_item id="3" xmlns="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#windows">
      <path>C:\Program Files\Common Files\Microsoft Shared\WMI</path>
      <filename>WmiScriptUtils.dll</filename>
      <owner>Administrators</owner>
      <size datatype="int">54272</size>
      <a_time datatype="int">1183042181</a_time>
      <c_time datatype="int">1165044708</c_time>
      <m_time datatype="int">1165044708</m_time>
      <ms_checksum>60432</ms_checksum>
      <version datatype="version">8.0.50727.762</version>
      <type>FILE_TYPE_DISK</type>
      <development_class>SP</development_class>
      <company>Microsoft Corporation</company>
      <internal_name>WMIScriptUtils.DLL</internal_name>
      <language status="not collected"/>
      <original_filename>WMIScriptUtils.DLL</original_filename>
      <product_name>Microsoft® Visual Studio® 2005</product_name>
      <product_version>8.0.50727.762</product_version>
    </file_item>
    ...
 </system_data>
```

MITRE

Item Status Attribute

- Holds information about the attempt to collect a specific item on the host.

- Possible values:
  - Error
  - Exists
  - Does not exist
  - Not collected

MITRE

Incomplete Collection

- Can still get accurate results ... sometimes

```
<collected_objects>
    <object id="“ flag=“incomplete">
      <reference item_ref="1"/>
      <reference item_ref=“2"/>
      <reference item_ref=“3"/>
    </object>
</collected_objects>
```

MITRE

Missing <collected_objects>

- Still a useable SC file
  - need to search the entire file for matching items

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.