HS SEDI
Homeland Security Systems Engineering and Development Institute


Matthew Hansbury
September 27th, 2010

Homeland Security

# Overview

- **What & Why?**
- **OVAL Language**
  - Overall Assessment Process
  - Language details
  - Example
  - OVAL Interpreter
- **OVAL Repository**
- **Advanced Topics**
- **Resources**

# What is OVAL?

An international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

- **Open Vulnerability and Assessment Language**
  - A community-developed open standard
  - Began in December 2002
  - Enables automated assessment and compliance checking
- **OVAL Language**
  - XML-based framework for making logical assertions about a system
    - Vulnerable, Compliant, Installed application, Patched
  - OVAL Interpreter
    - An open source reference implementation
- **OVAL Repository**
  - Collection of community contributed OVAL Definitions
  - “promote open and publicly available security content”
- **OVAL Adoption**
  - Both educate vendors and receive constructive technical feedback

# Why OVAL?

- **Transparency & Interoperability**
  - Allows users to know exactly what their tool is doing
  - Allows users to compare and mix-and-match tools
  - Allows vendors to focus on core competency

- **Variety of use cases**
  - Security advisory distribution
  - Vulnerability assessment
  - Malware and threat indicator sharing
  - Configuration management
  - Audit and centralized audit validation
  - Security Information Management Systems (SIMS)
  - System inventory
  - Patch management

# MITRE's Role in OVAL

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **MITRE is a not-for-profit corporation, chartered to work solely in the public interest.**
  - MITRE operates Federally Funded Research and Development Centers (FFRDCs).
  - Non-compete charter fosters "trusted moderator" status.
  - Work in the public interest.
  - Government sponsored.

- **OVAL Moderator**
  - Help drive consensus between government customers and greater community with technical solutions and changes.
  - Promote the **growth and adoption** of OVAL.
  - **Listen** to the community and guide the development of OVAL.
  - **Facilitate** the OVAL Board.
  - **Moderate** the OVAL Repository.
  - **Balance different perspectives** to arrive at the consensus solution that is best for OVAL and the public interest.

# OVAL Language: Schemas

## OVAL Definitions Schema

- Framework for logical assertions about a system

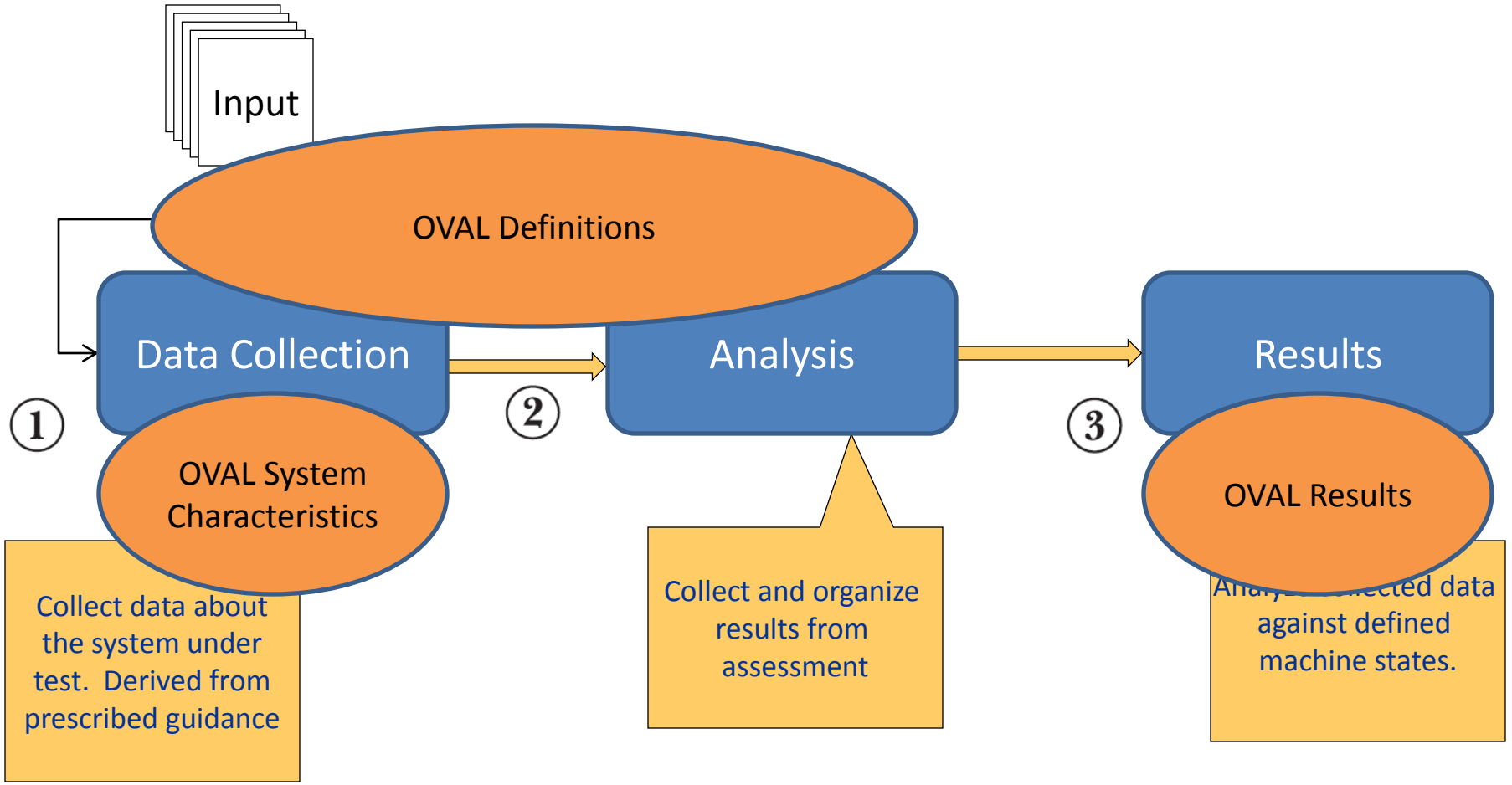
## OVAL System Characteristics Schema

- Encoding of the details of a system (database of system info)

## OVAL Results Schema

- Encoding of the detailed results of an analysis

# Assessment Process



# OVAL Language

- **Standardizes the three main steps of the assessment process**
  - **Representing** configuration information of systems for testing
    - Characteristics of the system (**OVAL System Characteristics**)
  - **Analyzing** the system for the presence of a specified machine state
    - Defining how to check for a state (**OVAL Definitions**)
  - **Reporting** the results of the assessment
    - Results (**OVAL Results**)

- **More than just compliance, can describe many states:**
  - Vulnerable
  - Compliant
  - Installed application
  - Patched

# 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.

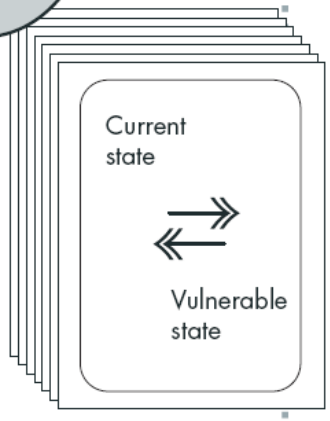
OVAL System Characteristics

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.



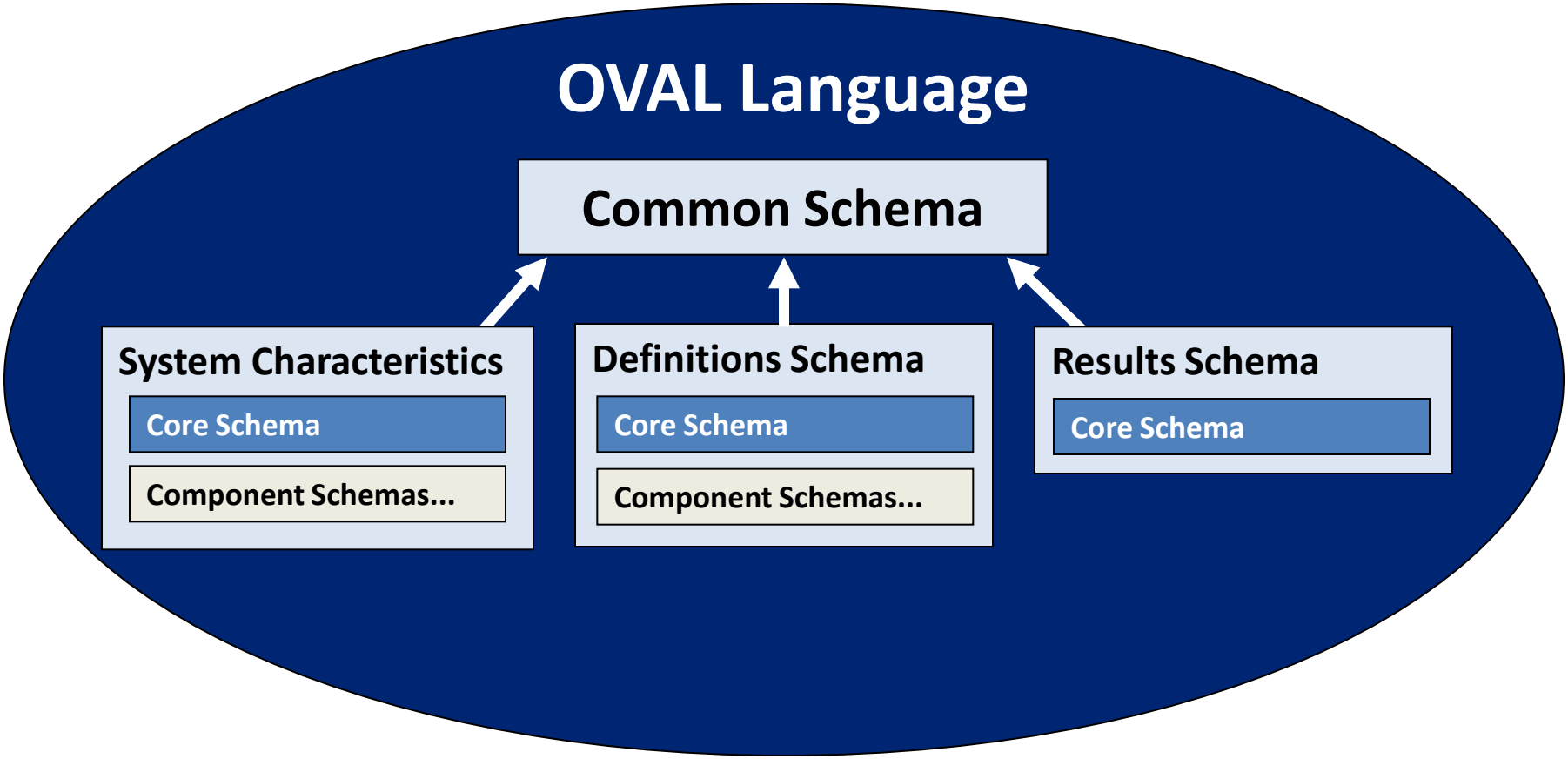

5

**Analysis results**

Results of analysis are formatted as an OVAL Results document.

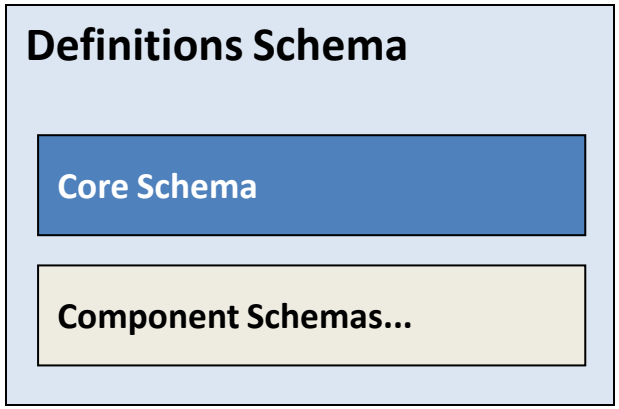
OVAL Results

# Core Schemas Relationships

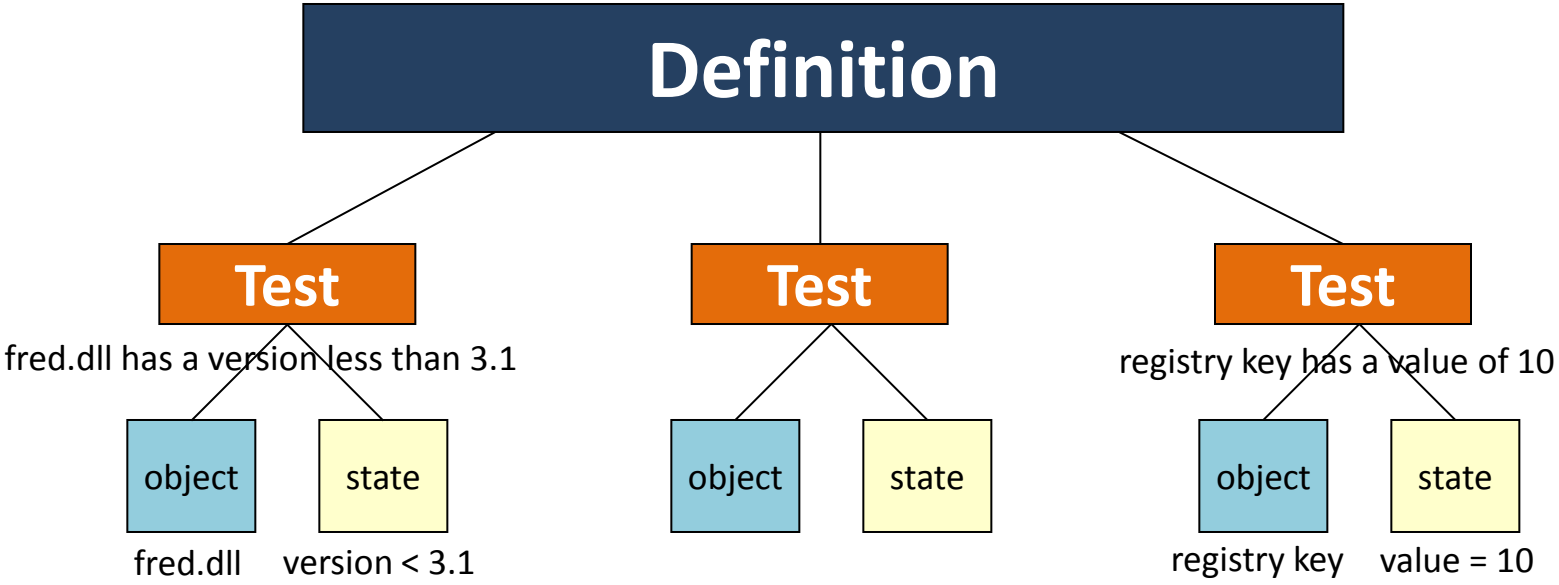


# Component Schemas

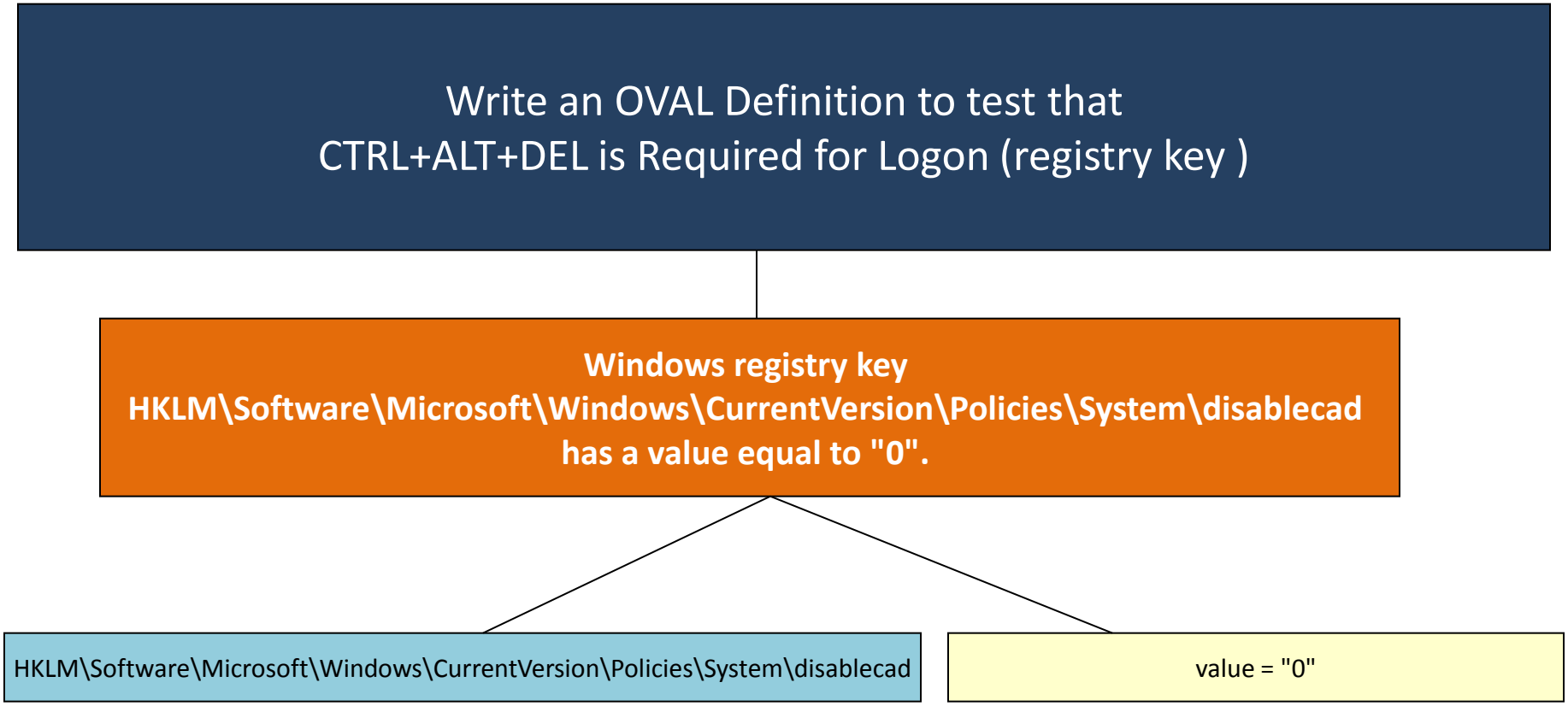
- **Number of Definition Component Schemas: 16**
  - Types of Schemas
    - Linux
    - Unix
    - Apple MacOS
    - Microsoft Windows
    - Sun Solaris
    - Microsoft Sharepoint
    - …
  - Where do these schemas come from?
    - OVAL community drives schema development



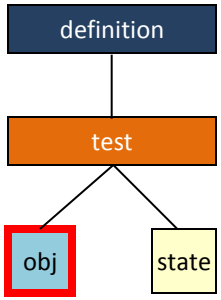
# Structure of an OVAL Definition



# CTRL+ALT+DEL - OVAL Definition

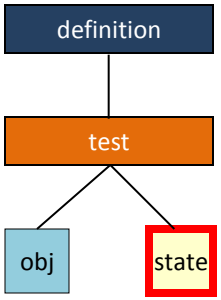


# CTRL+ALT+DEL - Registry Object



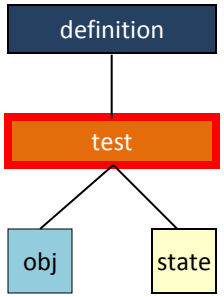

```
<registry_object id="oval:com.example:obj:1">
  <hive>HKEY_LOCAL_MACHINE</hive>
  <key>Software\Microsoft\Windows\CurrentVersion\Policies\System</key>
  <name>disablecad</name>
</registry_object>
```

# CTRL+ALT+DEL - Registry State




```
<registry_state id="oval:com.example:ste:1">
  <value datatype="int" operation="equals">0</value>
</registry_state>
```

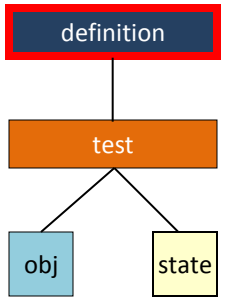
# CTRL+ALT+DEL - Registry Test




```
<registry_test id="oval:com.example:tst:1" check="all">
    <object object_ref="oval:com.example:obj:1"/>
    <state state_ref="oval:com.example:ste:1"/>
</registry_test>
```

# CTRL+ALT+DEL - OVAL Definition

```
<definition id="oval:com.example:def:1">
  <metadata>
    <title>CTRL+ALT+DEL Required for Logon</title>
    <description>
       This definition is used to introduce the OVAL
       Language to individuals interested in writing
       OVAL Content.
    </description>
  </metadata>
  <criteria>
    <criterion test_ref="oval:com.example:tst:1"
               comment="The registry key is set to require CTRL+ALT+DEL for Logon"/>
  </criteria>
</definition>
```



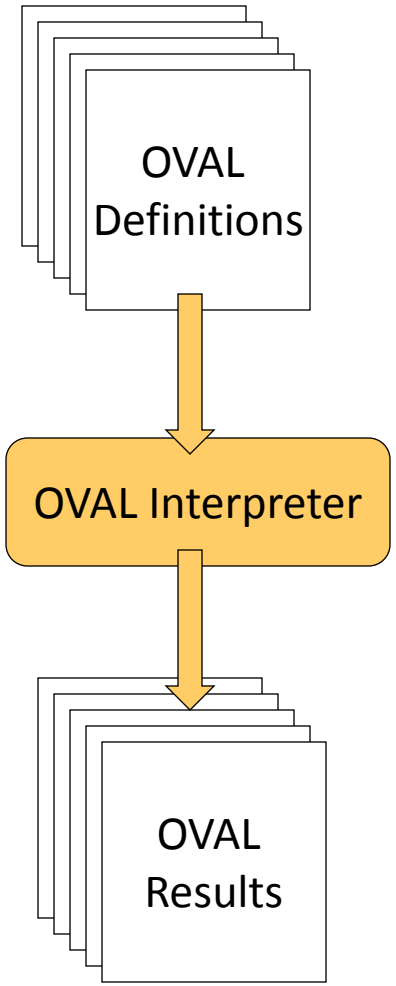
```
<oval_definitions …>
 <generator>…</generator>
 <definitions>
  <definition id="oval:org.mitre.oval.tutorial:def:1" version="1" class="miscellaneous">
   <metadata>
    <title>CTRL+ALT+DEL Required for Logon</title>
    <affected family="windows"/>
    <description>This definition is used to introduce the OVAL Language.</description>
   </metadata>
   <criteria>
    <criterion test_ref="oval:org.mitre.oval.tutorial:tst:1" comment="The registry key is set to require CTRL+ALT+DEL for Logon"/>
   </criteria>
  </definition>
 </definitions>
 <tests>
  <registry_test id="oval:org.mitre.oval.tutorial:tst:1" version="1" check= "all" comment="The registry key is set to require CTRL+ALT+DEL
      for Logon"  xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <object object_ref="oval:org.mitre.oval.tutorial:obj:1"/>
   <state state_ref="oval:org.mitre.oval.tutorial:ste:1"/>
  </registry_test>
 </tests>
 <objects>
  <registry_object id="oval:org.mitre.oval.tutorial:obj:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>Software\Microsoft\Windows\CurrentVersion\Policies\System</key>
   <name>disablecad </name>
  </registry_object>
 </objects>
 <states>
  <registry_state id="oval:org.mitre.oval.tutorial:ste:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
   <value datatype="int" operation="equals">0</value>
  </registry_state>
 </states>
</oval_definitions>
```

# OVAL Interpreter

Freely available **reference implementation** that demonstrates usability and drives the development of the OVAL Language

- Validates & tests content
- A reference for developers
- Supports OVAL Adoption
  - Leveraged by the NIST SCAP and OVAL Validation Programs
- Version 5.8.1 released on September 15th, 2010

https://oval.mitre.org/language/interpreter



# OVAL Repository

The central meeting place for the community to discuss, analyze, store, and disseminate OVAL Definitions.

- **Active community contributing OVAL Definitions for the latest vulnerabilities.**
  - https://oval.mitre.org/repository/
- **Coverage for a diverse set of applications and operating systems**
  - Microsoft, Mozilla, Solaris, Adobe, Apple
  - **10,000** Definition Milestone – September 16, 2010

Other Public Repositories of OVAL content

debian NIST Novell redhat

# Advanced Topics

- **Variables**
  - Variables define values to be obtained at run time
  - Three types of variables
    - constant_variable
    - external_variable
    - local_variable
  - Used to pass XCCDF variables into OVAL
- **Extended Definitions**
  - Existing definitions may be extended.
  - Simplifies writing definitions
- **Pattern Matching**
  - Allows use of Regular Expressions for matching
- **Behaviors**
  - Allow more detailed definition of an Object
  - Guides data collectors

# ITSAC Resources

- **Come to the Automation Specifications track OVAL session**
  - Further explore the OVAL Language
  - Tuesday from 1:30pm – 2:15pm
- **Come to the OVAL Workshop**
  - Help shape the future direction
  - Wednesday from 2:15pm – 3:00pm
- **MITRE Booth**
  - Talk to MITRE representatives regarding OVAL and other Standards

# Get Involved!



- **Website**
  - https://oval.mitre.org/
- **Join the OVAL mailing lists**
  - **OVAL-Announce** – General news and announcements about OVAL
  - **OVAL Developer's Forum** – Public forum for discussing the OVAL Language, addressing OVAL implementation issues, and for assisting other developers with OVAL.
  - **OVAL Repository Forum** – Public forum for discussing OVAL Repository content.
  - https://oval.mitre.org/community/registration.html
- **Participate in the OVAL Adoption Program**
  - List your product and help shape the effort
  - https://oval.mitre.org/adoption/