Languages:
XCCDF, OVAL, & Interactive

Jon Baker

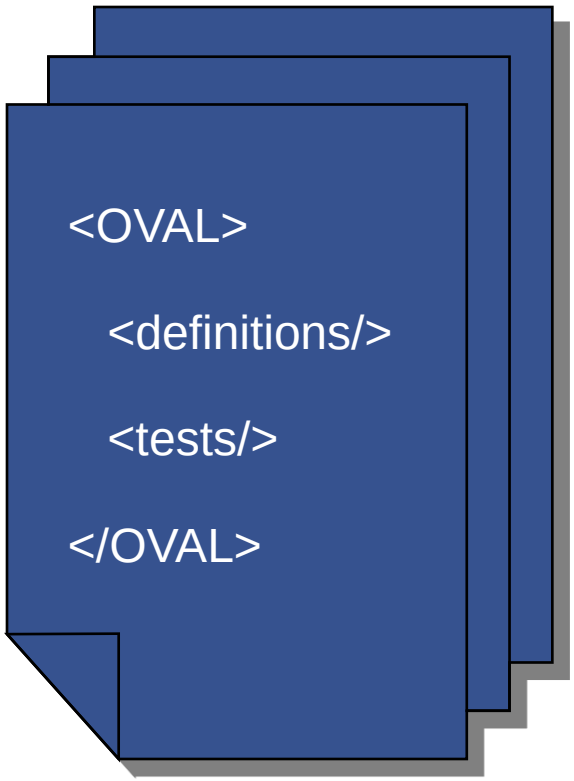
September 22, 2008

Why Languages?

- Use a standardized format to ensure guidance is easily consumed by a broad audience.
  - assessment tools
  - reporting
  - system administrators

Benefits

- machine readable document
  - less errors due to human translation
- immediate response
  - through automation
- interoperability
  - vendor neutral languages
- open to the user



Introduction to OVAL

"Open Vulnerability and Assessment Language"

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.

- XML language framework for assertions
- Can describe many different machine states
  - Vulnerable
  - Compliant
  - Installed application

OVAL Language

- Standardizes the three main steps of the assessment process
  - **Representing** configuration information of systems for testing
    - characteristics of the system
  - **Analyzing** the system for the presence of a specified machine state
    - defining how to check for a state
  - **Reporting** the results of the assessment
    - results

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

http://oval.mitre.org/language

OVAL Language: Core Schemas

OVAL Definitions Schema

- Framework for logical assertions about a system

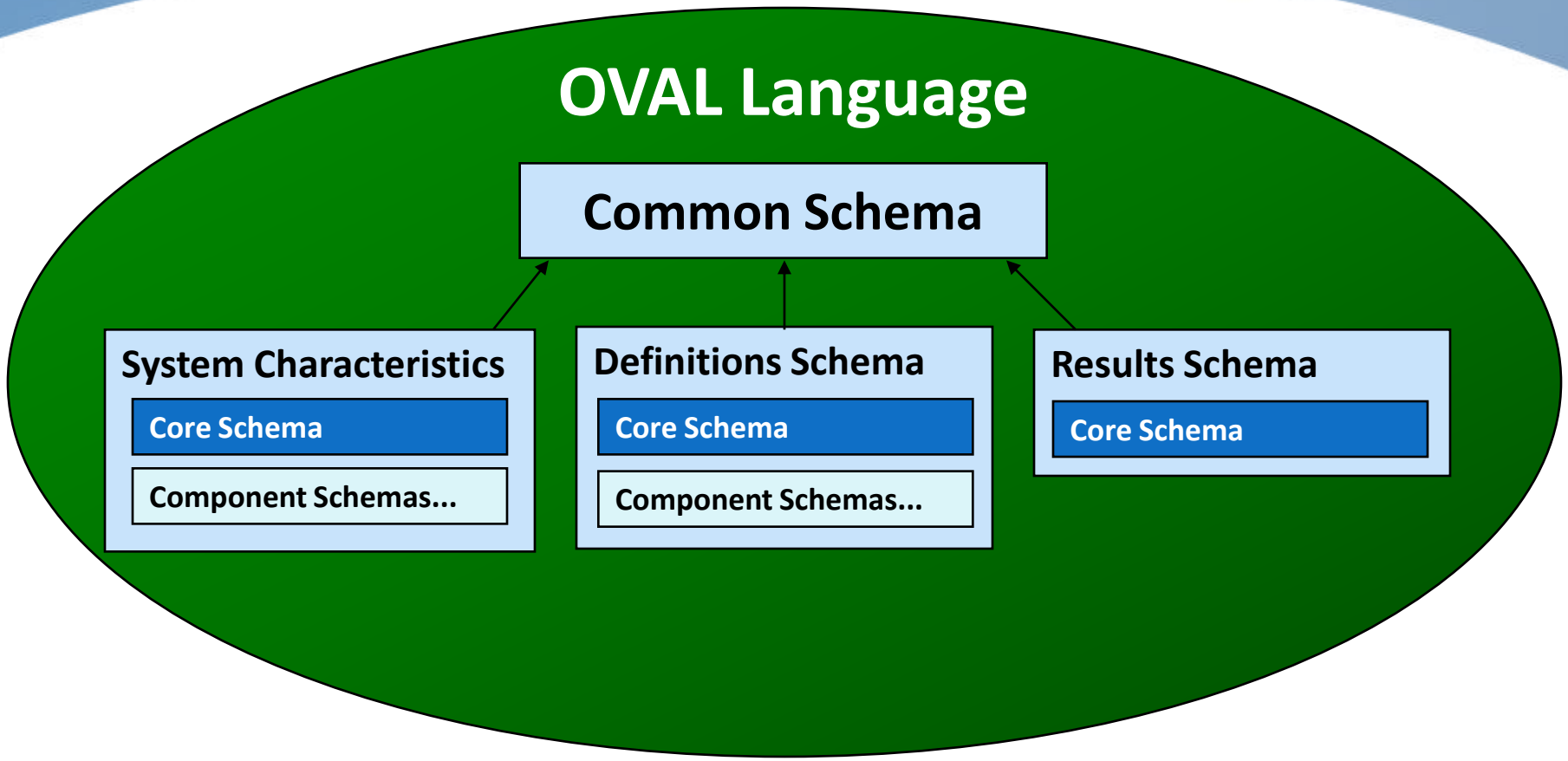
OVAL System Characteristics Schema

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

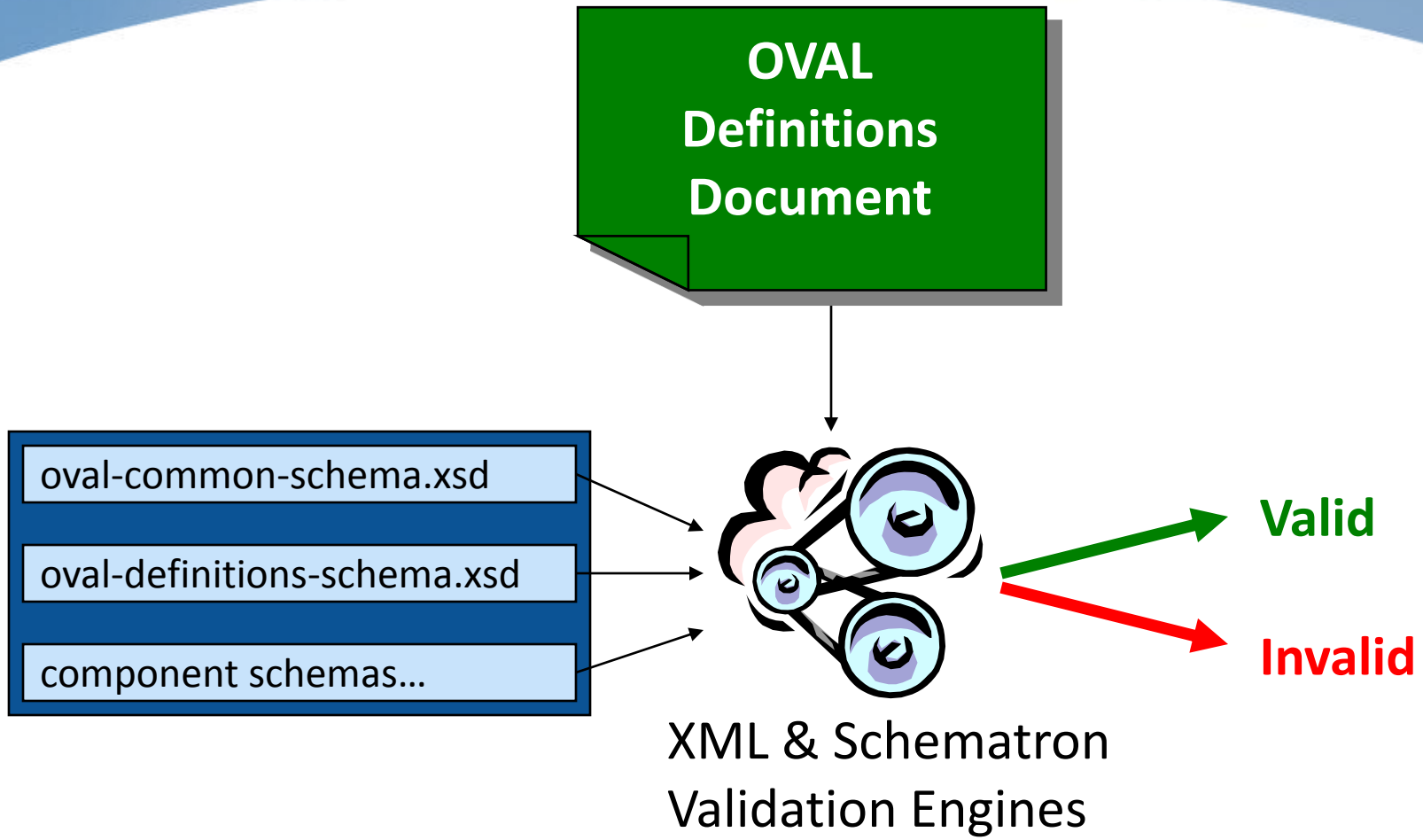
OVAL Results Schema

- Encoding of the detailed results of an analysis

Core Schemas Relationships



OVAL Document Validation Process



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.

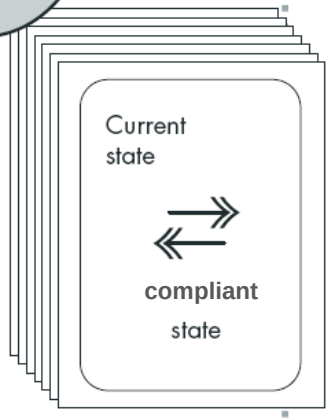
OVAL System Characteristics

OVAL Analysis

4

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.



OVAL Results

5

Analysis results

Results of analysis are formatted as an OVAL Results document.

MITRE

Demo: OVAL Process

Assessing your local system

OVAL Interpreter

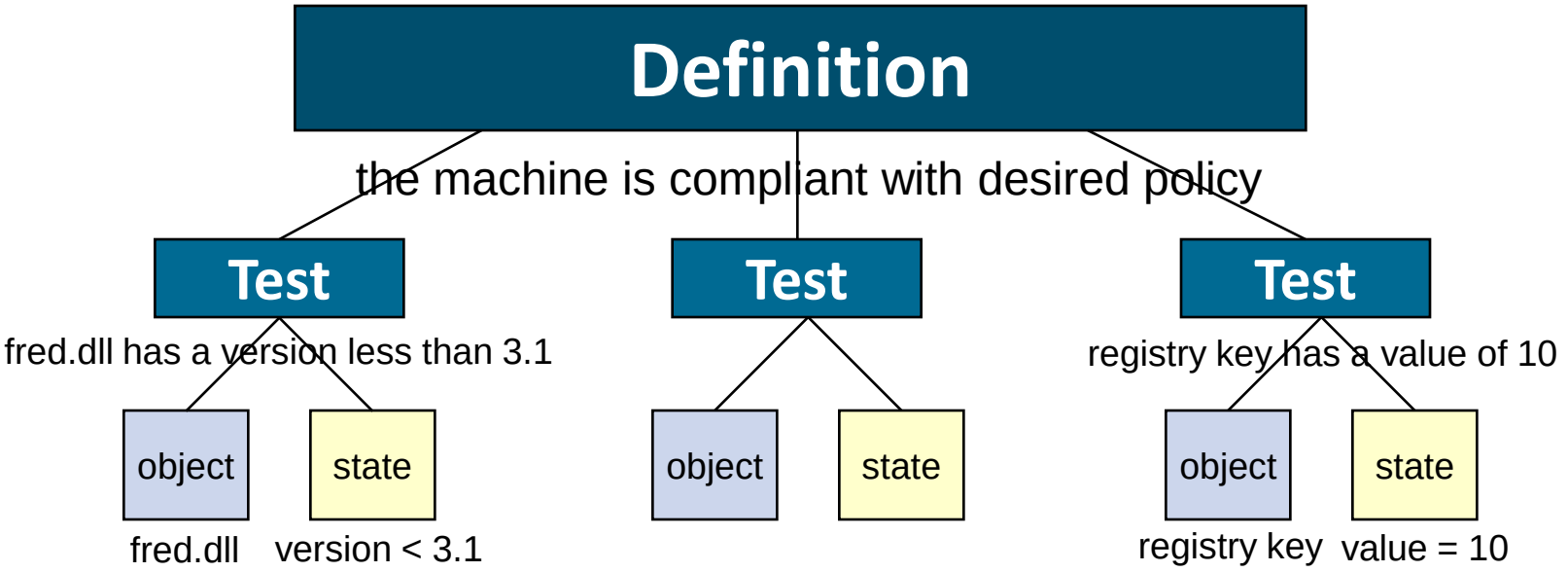
- Freely available reference implementation

- Demonstrates usability of the OVAL Language
- Helps drive the development of the OVAL Language
- Test new content
- Reference for developers
- Reduces the cost of OVAL adoption

http://oval.mitre.org/language/download/interpreter

OVAL Definition Tutorial

Structure of an OVAL Definition



CTRL+ALT+DEL - OVAL Definition

Write an OVAL Definition to test that
CTRL+ALT+DEL is Required for Logon (registry key)
'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\disablecad'
has a value equal to “0".

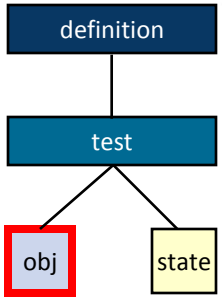
Windows registry key
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\disablecad
has a value equal to “0".

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\disablecad

value = “0"

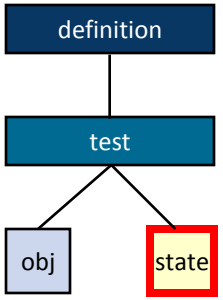
MITRE

CTRL+ALT+DEL - Registry Object



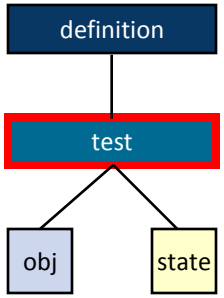

```
<registry_object id="oval:com.example:obj:1">
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>Software\Microsoft\Windows\CurrentVersion\Policies\System</key>
   <name>disablecad</name>
</registry_object>
```

CTRL+ALT+DEL - Registry State




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

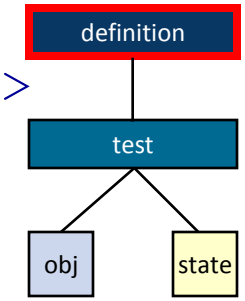
CTRL+ALT+DEL - Registry Test




```
<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

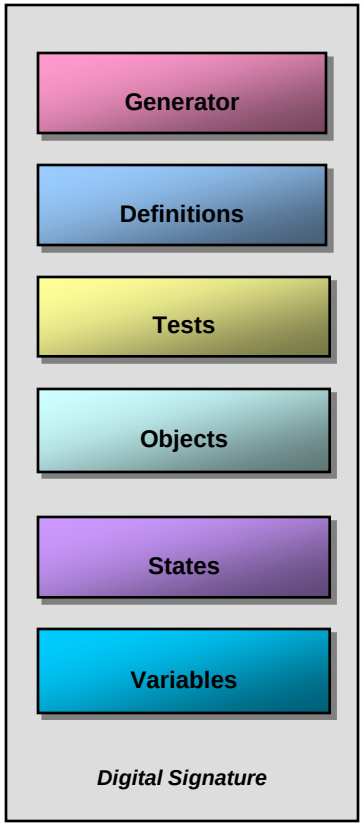
```
<definition id="oval:com.example:def:1">
  <metadata>
    <title>CTRL+ALT+DEL Required for Logon</title>
    <description>
      This definition is used to introduce the
      OVAL Language to individuals interested
      in writing OVAL Content.
    </description>
  </metadata>
  <criteria>
    <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 Definition File Overview

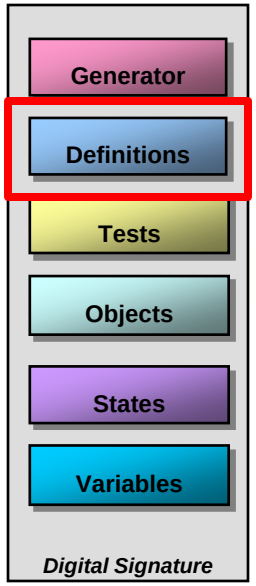
- Generator
- Definitions
- Tests
- Objects
- States
- Variables
- Digital Signature



Definitions Section

- A container for a set of Definitions
- Definitions give meaning to a set of reusable components
- Each definition has two major parts
  - Metadata – What is this definition about?
  - Criteria – Logical combination of tests and other definitions

- Definitions may be reused by other definitions
  - <extend_definition ...>
  - Easier/Faster to create new definitions
    - Leverage existing proven definitions in new definitions



Tests, Objects, and States Sections

Tests

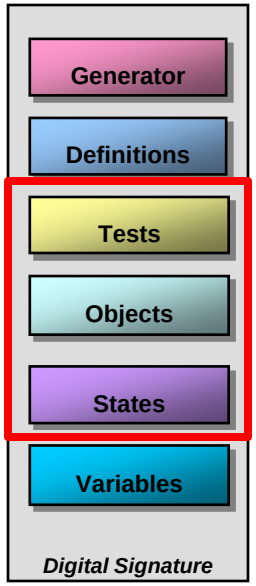
- Check a set of items on a system for an expected state
- Each test references an object and a state
  - Includes check attributes to guide evaluation

Objects

- Define a **set** of items on a system to examine

States

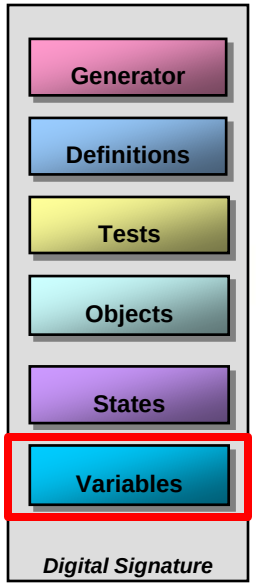
- Define the expected “state” of an item on a system



Variables Section

- A container for a set of variables
- Variables define values to be obtained at run time
  - Variables represent an array of values
- Variables can be used in numerous ways

Variables enable compliance check reuse across organizations with differing needs.



- Three types of variables
  - **constant_variable:** a constant value to be separated and reused
  - **external_variable:** parameters supplied during definition evaluation
  - **local_variable:** values constructed from other variables and local system settings

Introduction to the Interactive Schema

MITRE

What is the Interactive Schema?

- XML based framework for expressing compliance questionnaires
  - Developed as an XCCDF checking system
- Supports questions and follow up questions
- Defines logical constructs to allow lengthy questionnaires to be evaluated and produce a single result

http://nvd.nist.gov/interactive.cfm

Interactive Schema Data Model

generator

- Information about the origin of the document

questionnaire

- Descriptive metadata about the Questionnaire
- Logical combination of a set of Actions
  - Actions can leverage existing Questionnaires

test _action

- Associate a set of actions with a Question
  - Ask the question then based on the response ask another question or determine a result

question

- Numerous types of questions (Boolean, Choice, etc.)

results

- Detailed result information for a Questionnaire

MITRE

Interactive Schema Example

A Questionnaire for the following recommendation:

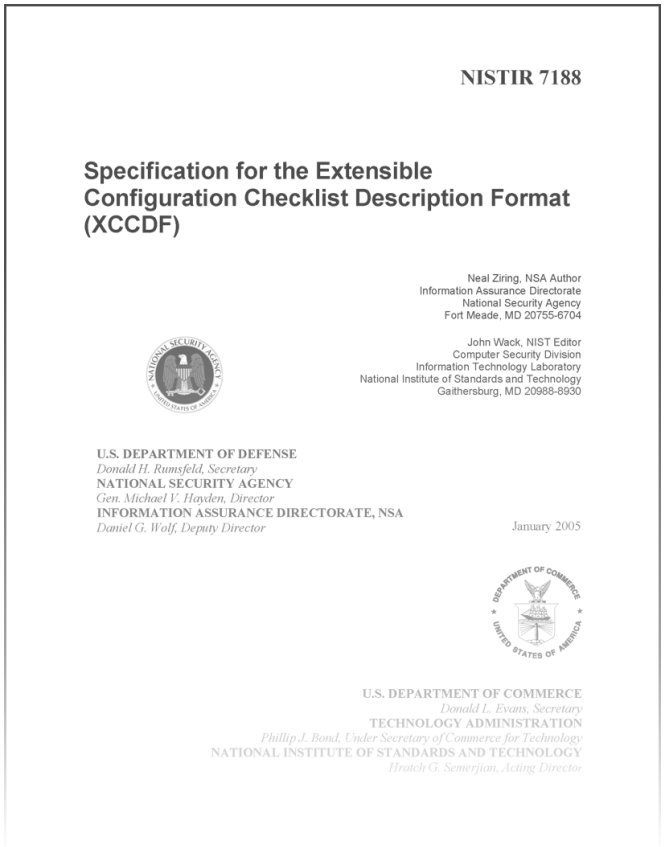
"Apply the security guidance for Windows XP found at the Center for Internet Security site."

```
<interactive xmlns="http://www.mitre.org/interactive/0.2" >
  <generator>... </generator>
  <questionnaire priority="HIGH" id="inter:org.mitre.example:questionnaire:1">
    <title>Apply CIS Windows XP Guidance Questionnaire</title>
    <actions priority="HIGH" operation="AND">
      <test_action_ref priority="HIGH">inter:org.mitre.example:testaction:1</test_action_ref>
    </actions>
  </questionnaire>
  <!-- The test action references a question and defines the action to be taken for each response to the question. -->
  <boolean_question_test_action id="inter:org.mitre.example:testaction:1" question_ref="inter:org.mitre.example:question:1">
    <title>Question 1 with follow up question.</title>
    <when_true>
      <test_action_ref priority="HIGH">inter:org.mitre.example:testaction:2</test_action_ref>
    </when_true>
    <when_false>
      <result>FAIL</result>
    </when_false>
  </boolean_question_test_action>
  <boolean_question_test_action id="inter:org.mitre.example:testaction:2" question_ref="inter:org.mitre.example:question:2">
    <notes></notes>
    <when_true>
      <result>PASS</result>
    </when_true>
    <when_false>
      <result>FAIL</result>
    </when_false>
  </boolean_question_test_action>
  <!-- The set of questions to be asked.-->
  <boolean_question id="inter:org.mitre.example:question:1" model="MODEL_YES_NO">
    <question_text>Has the CIS Windows XP Guidance been applied?</question_text>
  </boolean_question>
  <boolean_question id="inter:org.mitre.example:question:2" model="MODEL_YES_NO">
    <question_text>Did you confirm that you were applying the most recent version?</question_text>
  </boolean_question>
</interactive>
```

Introduction to XCCDF

What is XCCDF

- **The eXtensible Configuration Checklist Description Format**
- **An XML specification for expressing security benchmarks and recording assessment results.**
- **Designed for three purposes:**
  - driving system security checking tools
  - generating human-readable documents and reports
  - scoring and tracking compliance



NISTIR 7188

Specification for the Extensible Configuration Checklist Description Format (XCCDF)

Neal Ziring, NSA Author
Information Assurance Directorate
National Security Agency
Fort Meade, MD 20755-6704

John Wack, NIST Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20988-8930

U.S. DEPARTMENT OF DEFENSE
Donald H. Rumsfeld, Secretary
NATIONAL SECURITY AGENCY
Gen. Michael V. Hayden, Director
INFORMATION ASSURANCE DIRECTORATE, NSA
Daniel G. Wolf, Deputy Director

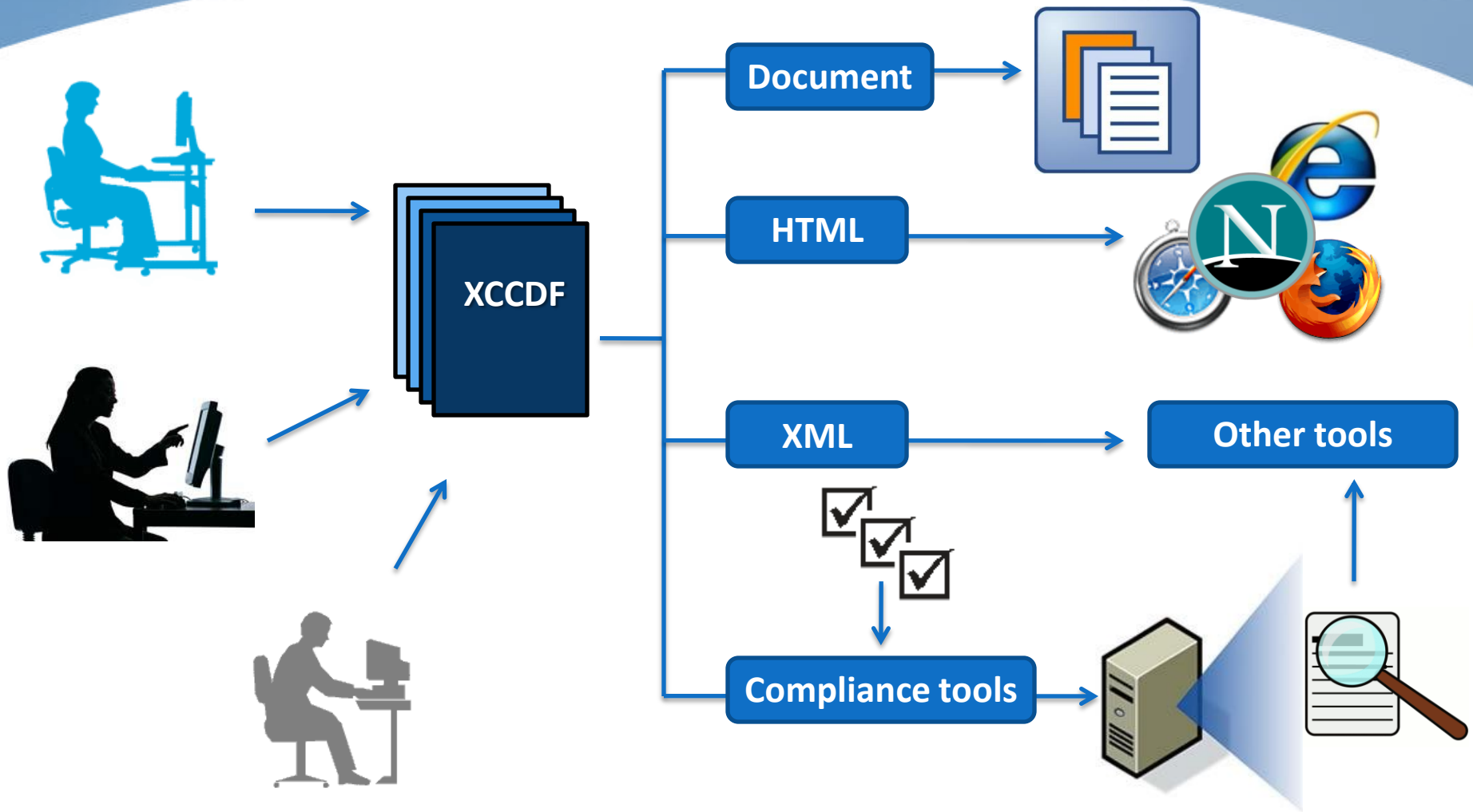
January 2005

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary of Commerce for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Hratch G. Semerjian, Acting Director

http://nvd.nist.gov/xccdf.cfm

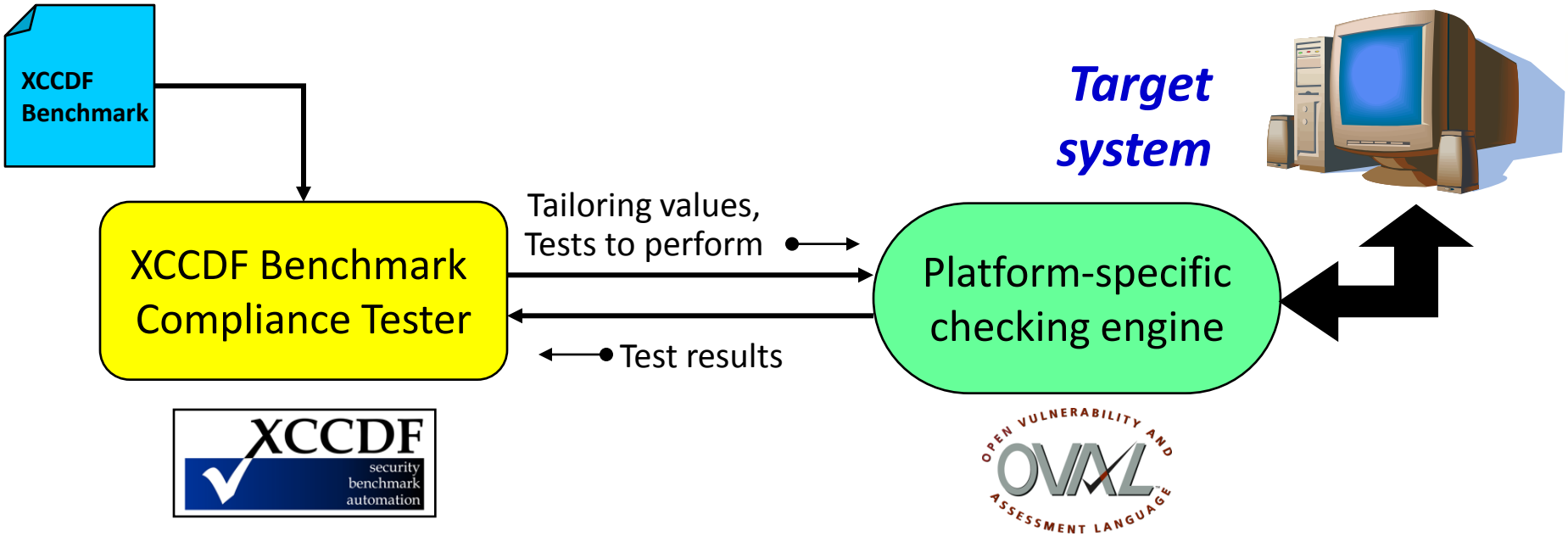
MITRE

XCCDF Use Cases

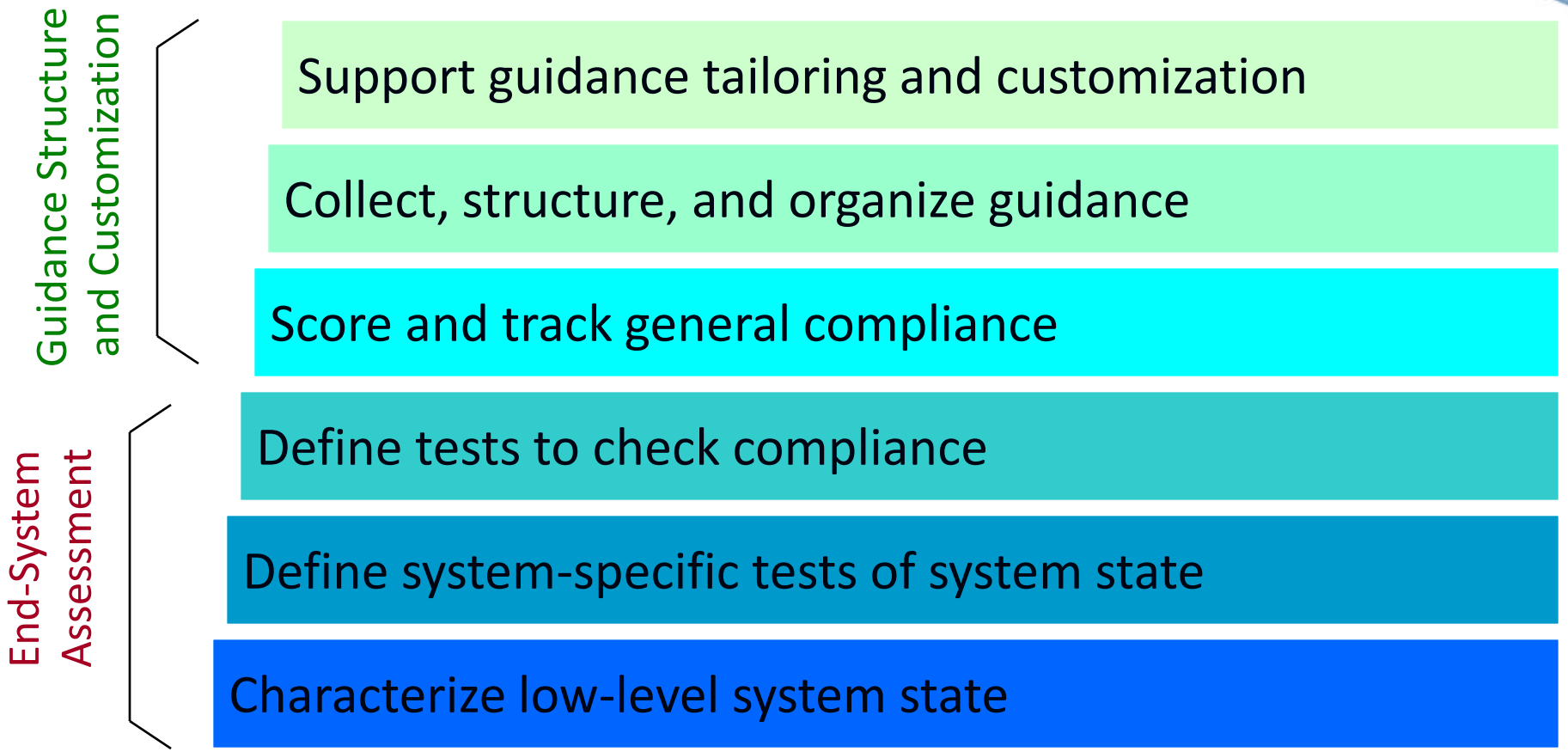


XCCDF and Checking Engines

- XCCDF does ***not*** specify platform-specific system rule checking logic.
- The `Rule/check` element contains information for driving a platform-specific checking engine.



XCCDF and OVAL Interaction

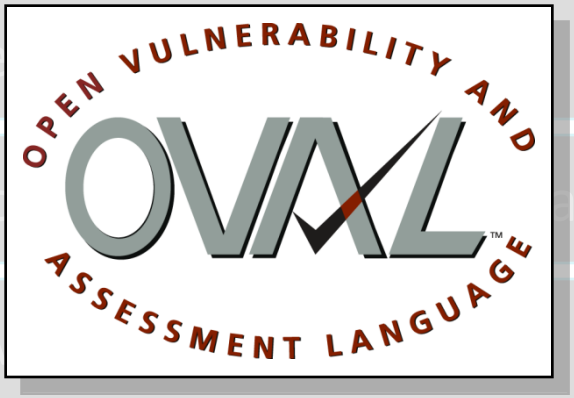


35

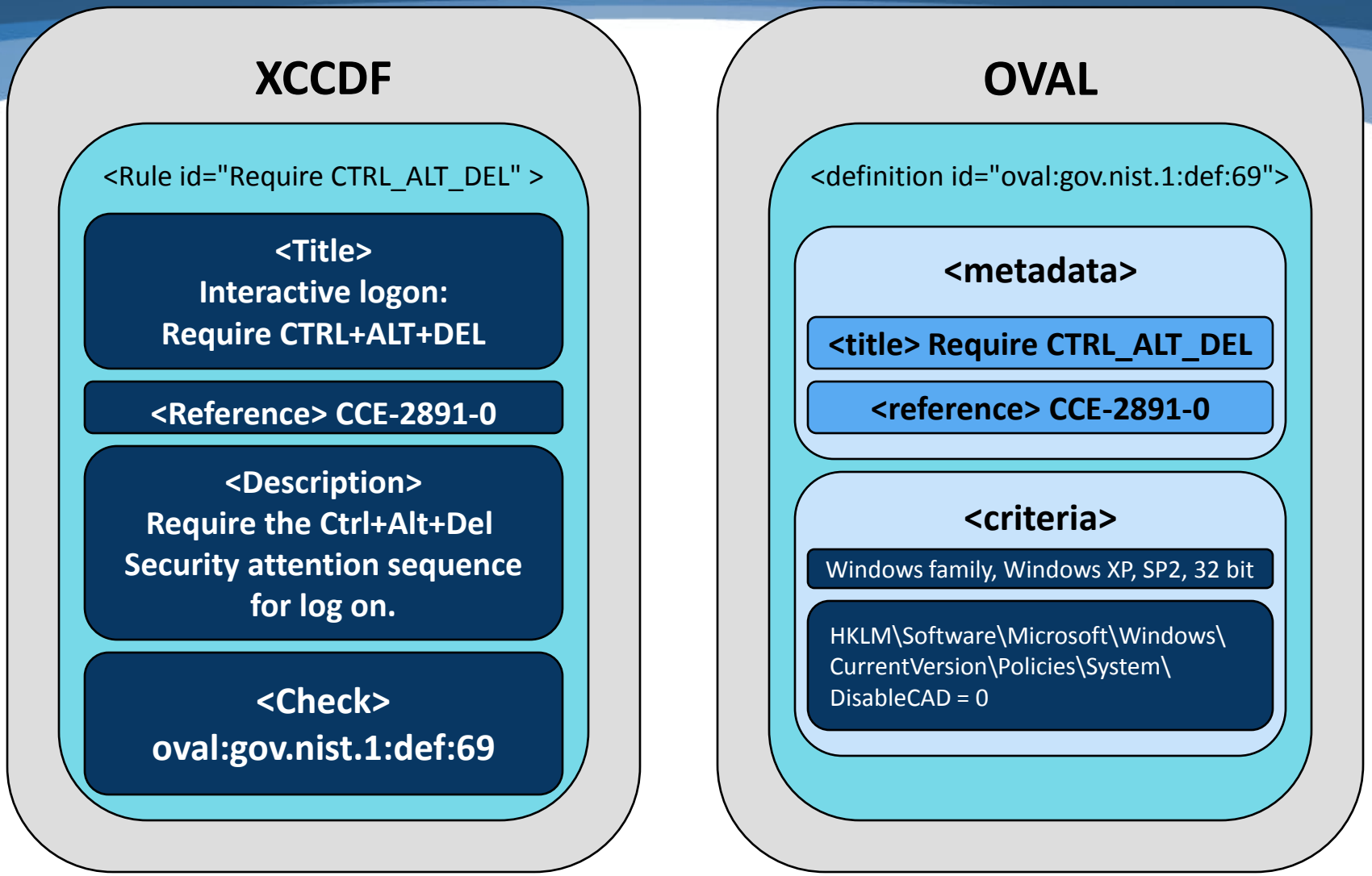
XCCDF and OVAL Interaction

Guidance Structure and Customization

End-System Assessment



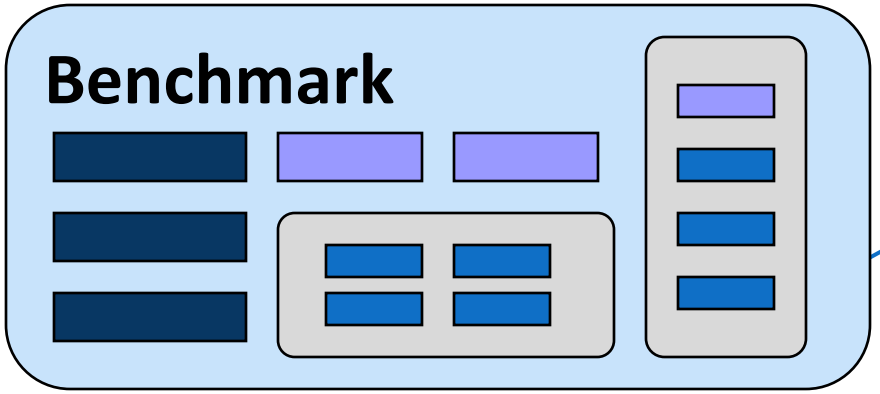
XCCDF & OVAL Illustrated



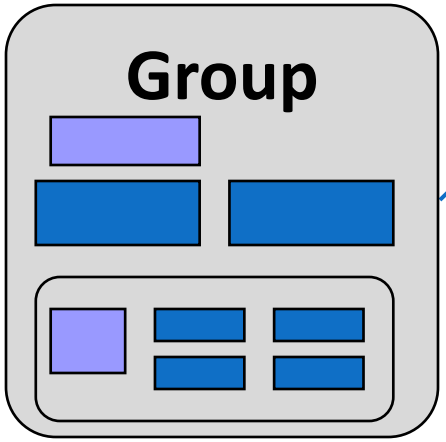
MITRE

XCCDF Data Model

XCCDF defines the following key object types:



The complete document; corresponds to recommendation tracker's application



A set of related recommendations and values; can be nested

Rule

As in the recommendation tracker

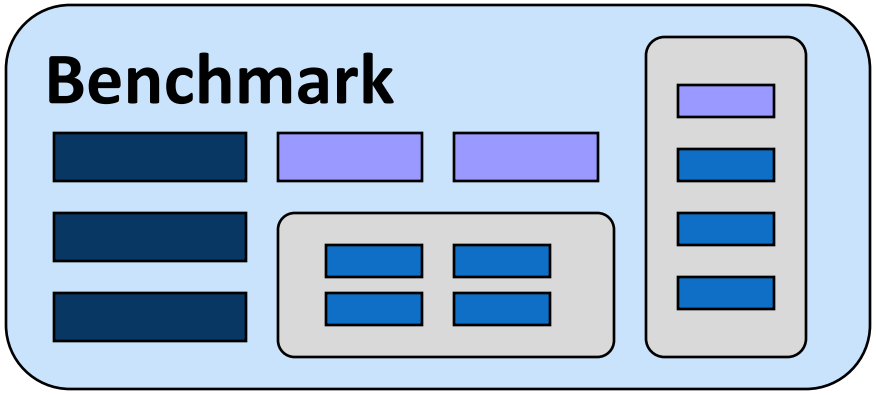
Value

Profile

Support tailoring, guidance for multiple roles, rule reuse

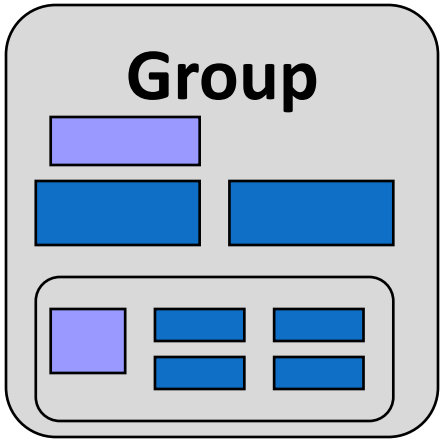
XCCDF Benchmark

```
<Benchmark id="Windows-XP">
   <title>Guidance for Securing Microsoft Windows XP</title>
   <platform idref="cpe:/o:microsoft:windows_xp"/>
   <Profile id="XP-Pro">...</Profile>
   <Group id="Chapter1">
      <Group id="PasswordPolicy">
         <Value>
         <Rule>
      </Group>
      <Group id="AuditPolicy">
          <Rule>
      </Group>
   </Group>
   <Group id="Chapter2">
   </Group>
</Benchmark>
```



XCCDF Group

```
<Group id="account_policies_group">
    <Group id="password_policies">
       <title>Password Policies</title>
       <description>In addition to educating users regarding the
       selection and use of good passwords, it is also important
       to set password parameters so that passwords are
       sufficiently strong...</description>
       <value>...</value>
       <rule>...</rule>
       <rule>...</rule>
    </Group>
</Group>
<Group id="file_permissions_group">
   ...
</Group>
```



XCCDF Rule

```
<Rule id="maximum_password_age" >
    <title>Maximum Password Age</title>
    <description>Set the "Maximum password age" password parameter to 90
   days.</description>
    <reference href="http://cce.mitre.org">CCE-2920-7</reference>
    <rationale>The "Maximum password age" password parameter is set to
        force users to change passwords at regular, defined, intervals…
    </rationale>
    <fixtext>1 - Launch the Local Security Policy editor: Start ->
        All Programs -> Administrative Tools -> Local Security Policy…
    </fixtext>
    <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-export value-id="maximum_password_age_var"
                    export-name="oval:gov.nist.fdcc.xp:var:90"/>
      <check-content-ref href="BDC-XP-oval.xml"
                         name="oval:gov.nist.fdcc.xp:def:17"/>
    </check>
</Rule>
```

Rule

XCCDF Profile

```
<Profile id="federal_desktop_core_configuration">
    <title>Federal Desktop Core Configuration</title>
    <description>This profile represents guidance outlined in
   Federal Desktop Core Configuration settings for Desktop
   systems.</description>
    <!--Password Policy Settings-->
    <select idref="maximum_password_age" selected="true"/>
    <select idref="minimum_password_length" selected="true"/>
    <refine-value idref="maximum_password_age_var"
        selector="5184000_seconds"/>
    <refine-value idref="minimum_password_length_var"
        selector="12_characters"/>
</Profile>
```

Profile

Summary

Standard languages allow for automated exchange of information between different sources.

- saves time
- reduces error
- interoperability