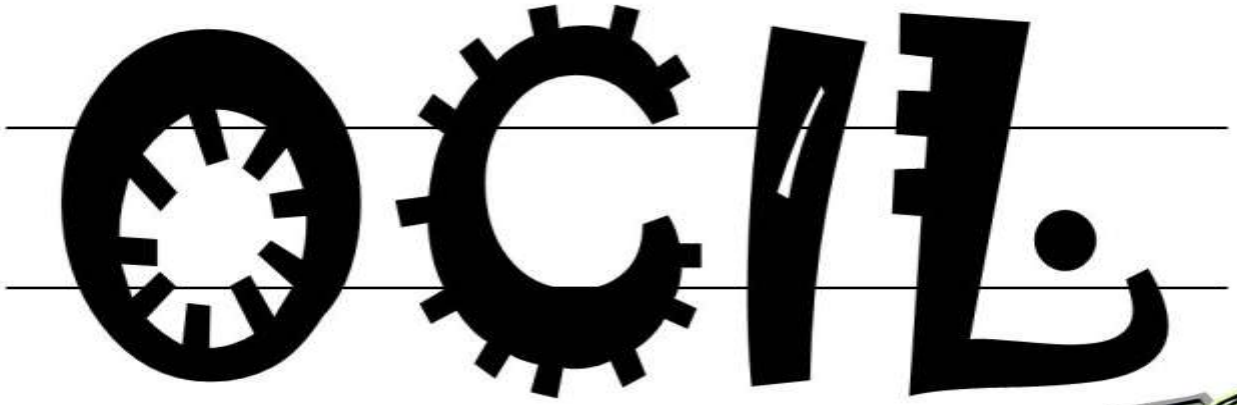


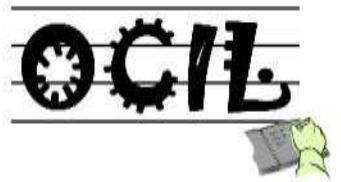
Open Checklist Interactive Language

ITSAC September 28, 2010

Maria Casipe

MITRE

Overview



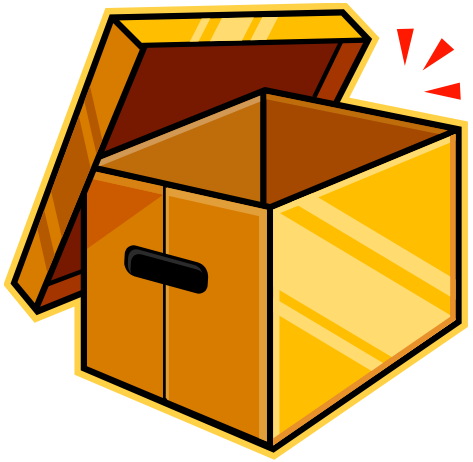
- **Part I**
  - **Introduction**
  - **SCAP Use Case**
- **Part 2**
  - **Core Objects**
  - **Basic Features**
  - **Advanced Features**
- **Part 3**
  - **Demo of Reference Implementation**
  - **Recent Activities**
  - **Community Resources**

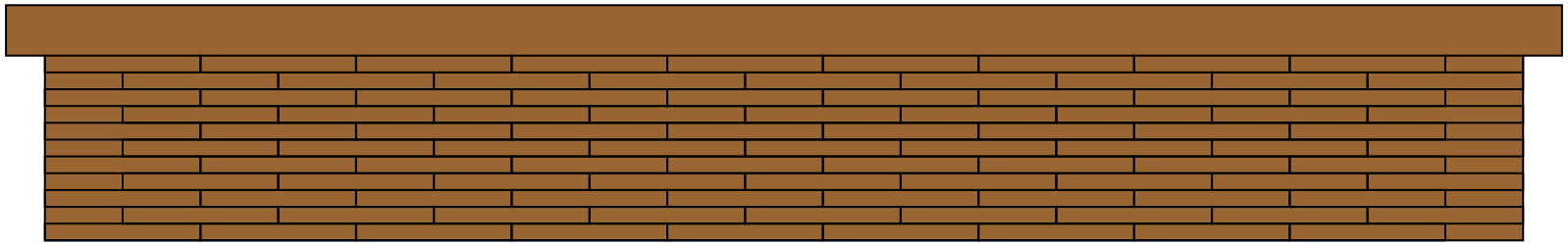
OCIL in a Nutshell

BUILD

EVALUATE

STORE





QUESTIONNAIRE FRAMEWORK

SCAP 1.0 Languages

- **XCCDF**
  - **eXtensible Configuration Checklist Description Format**
  - **A specification for writing security checklists, benchmarks, and other related documents.**

- **OVAL**
  - **Open Vulnerability and Assessment Language**
  - **A specification language for machine-readable rules to check a state of the system.**

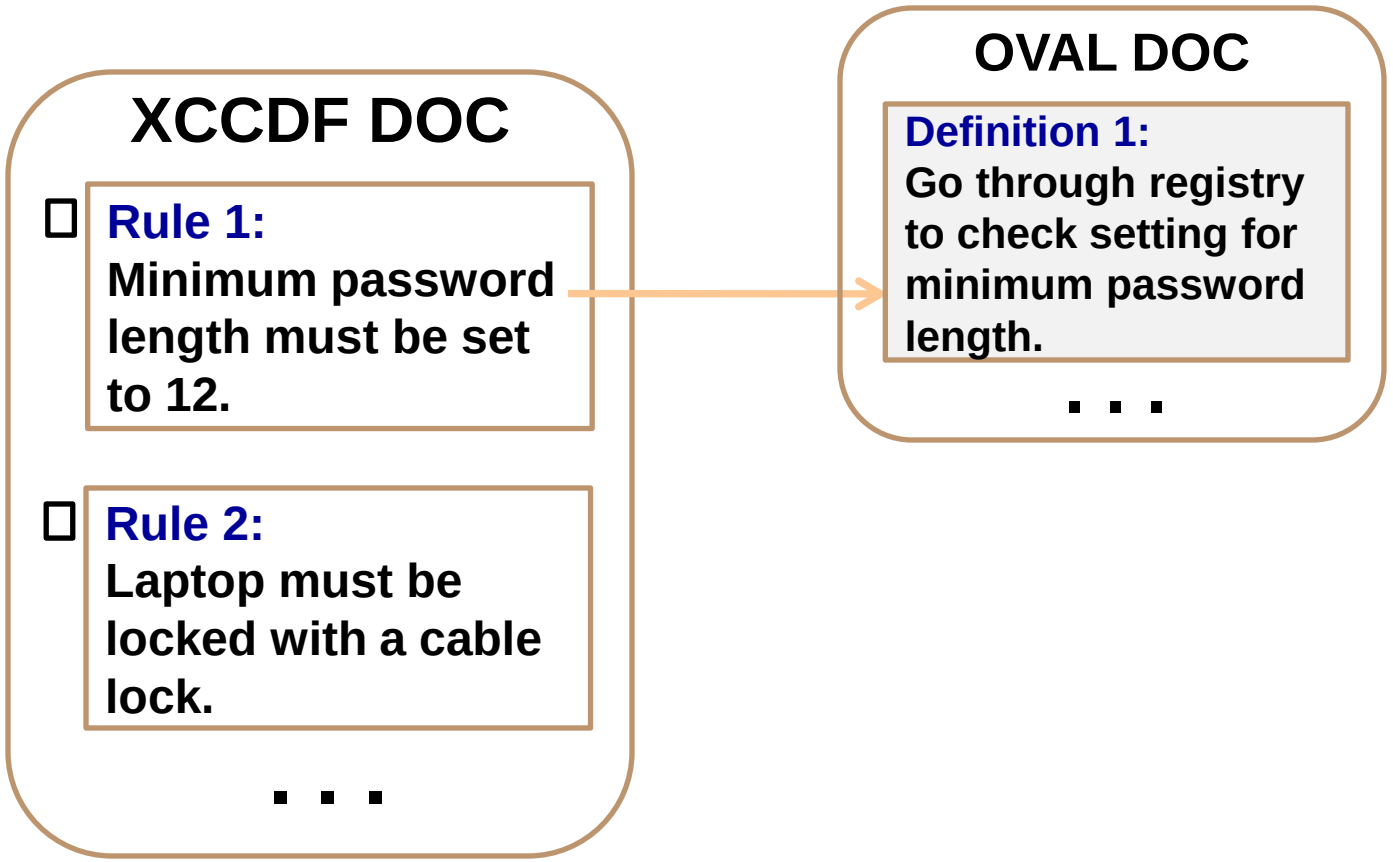
SCAP 1.0: XCCDF

XCCDF DOC

- **Rule 1:**
  Minimum password length must be set to 12.
- **Rule 2:**
  Laptop must be locked with a cable lock.

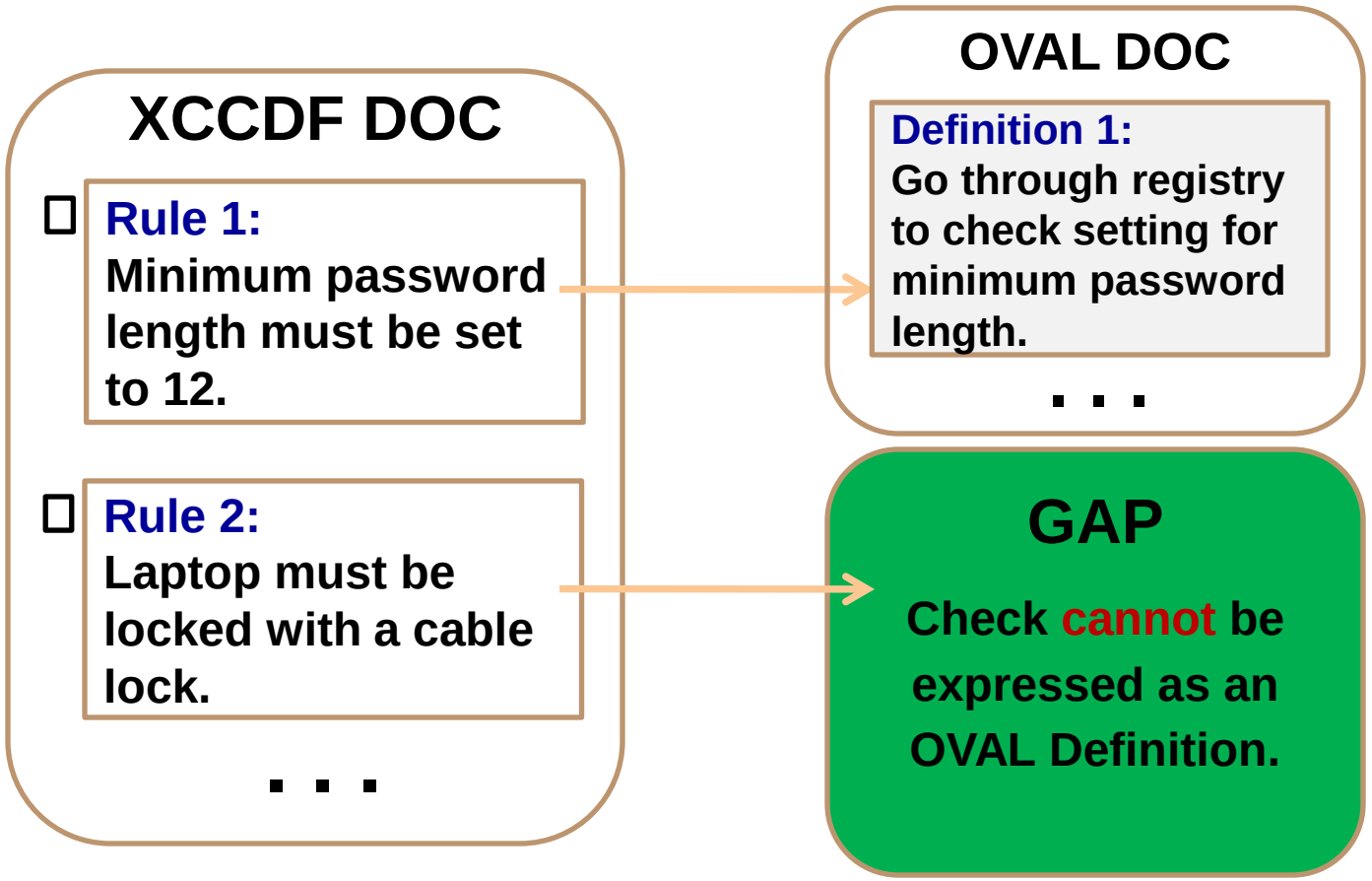
. . .

SCAP 1.0: XCCDF and OVAL



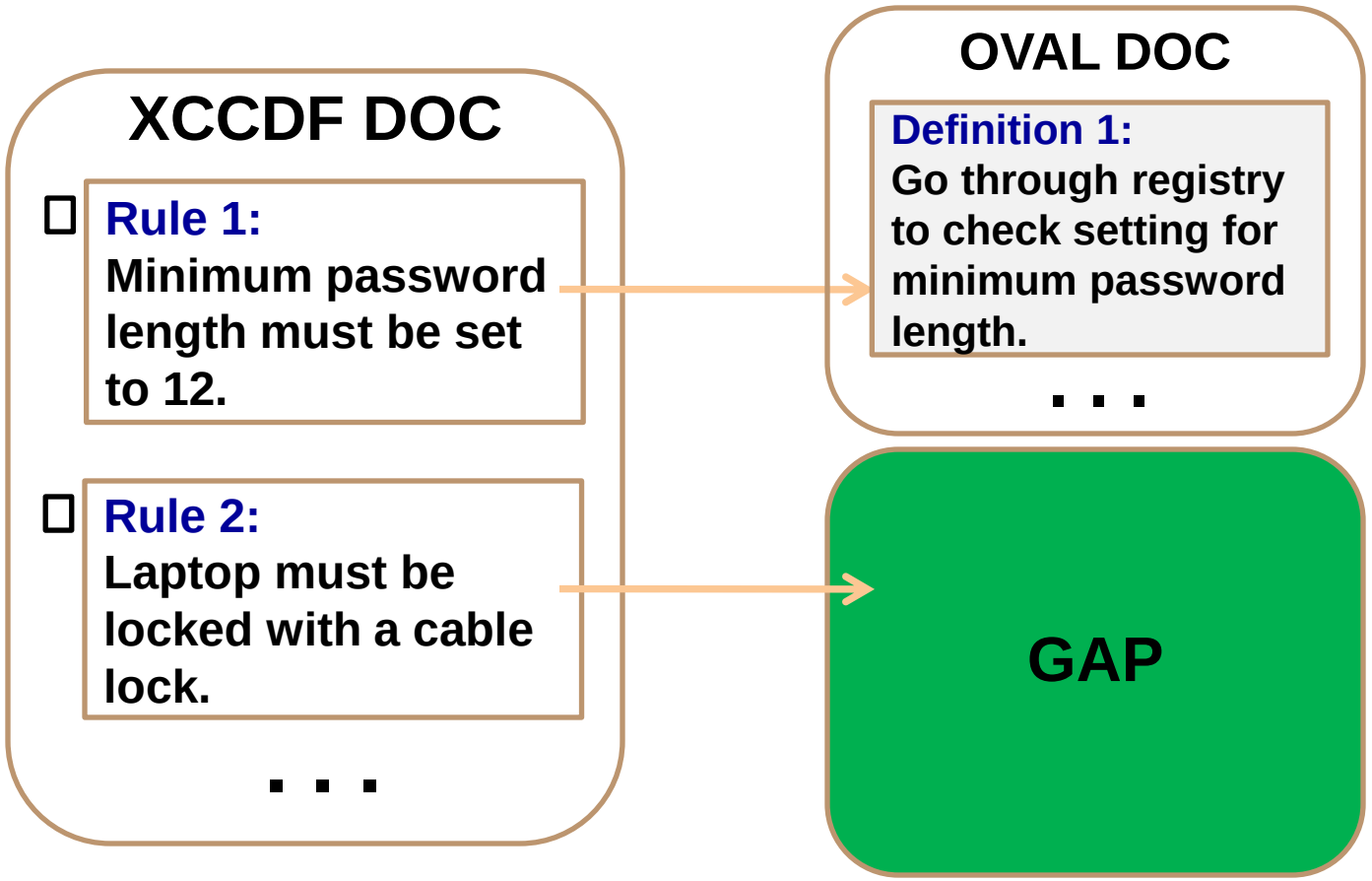
OVAL can be used to express automated checks.

SCAP 1.0: XCCDF and OVAL

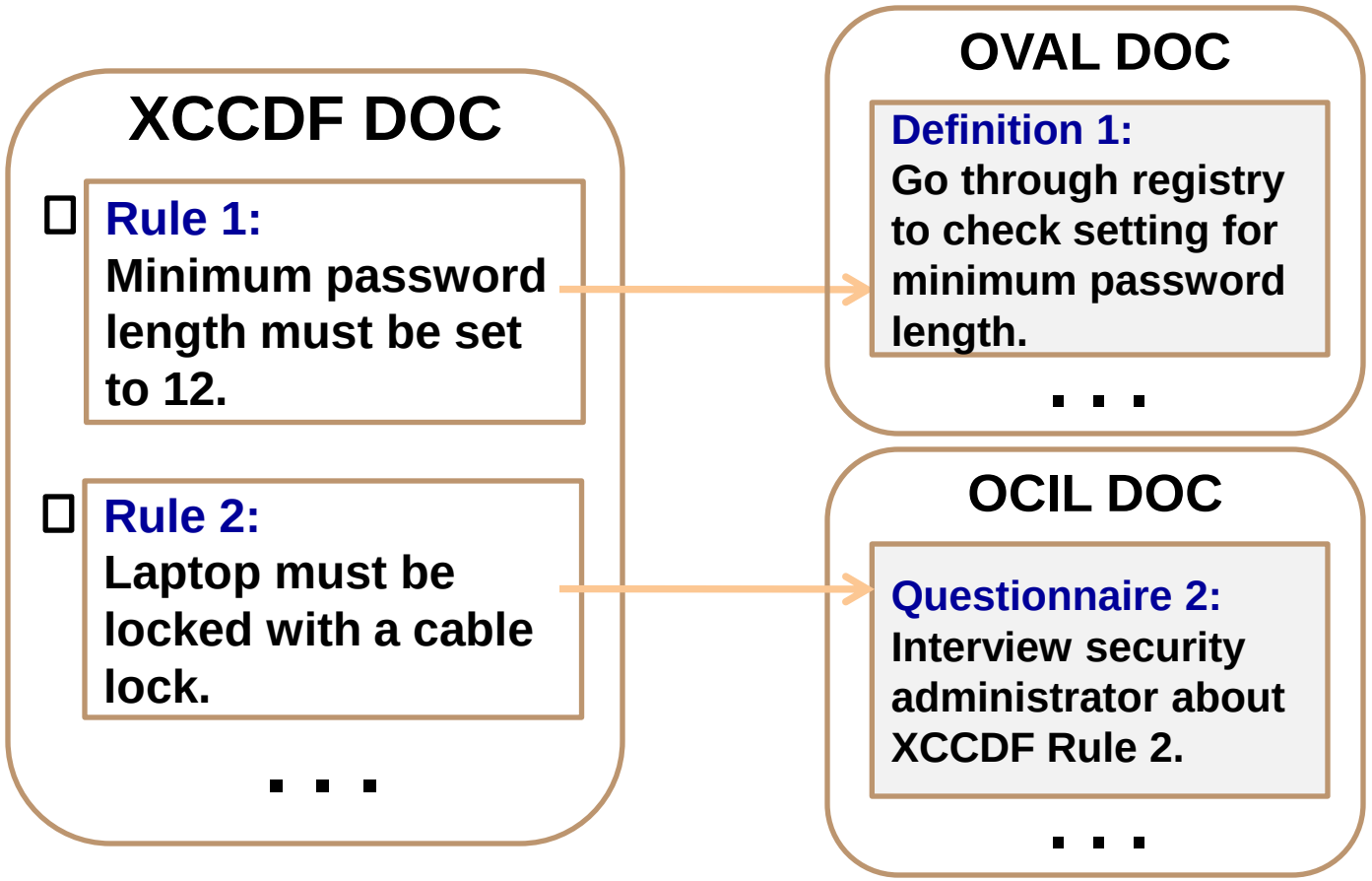


***OVAL** can be used to express **automated** checks.**

Can we use OCIL?

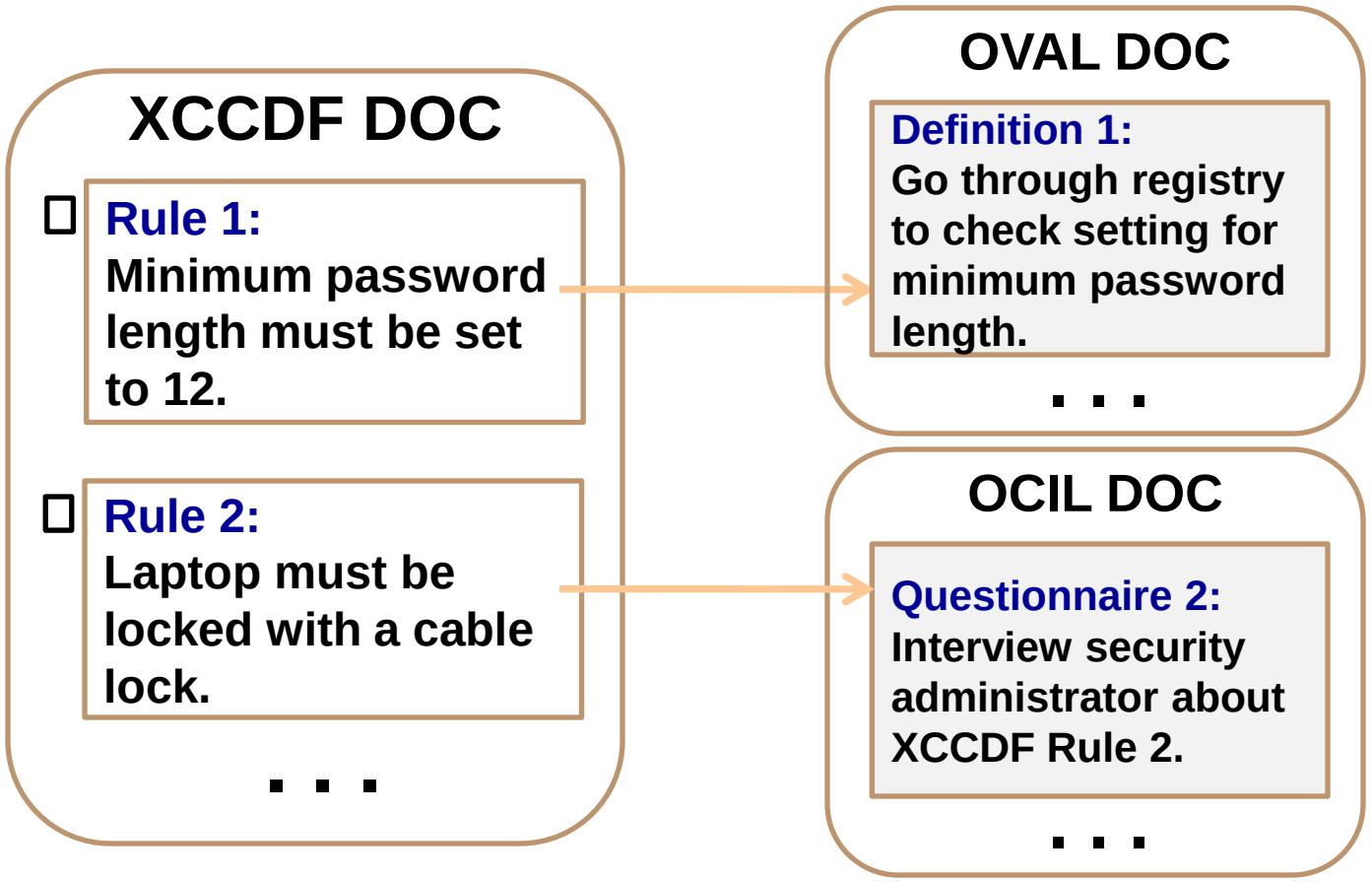


Can we use OCIL? YES



***OCIL** can be used to express **manual** security checks.**

SCAP 1.1: XCCDF, OVAL, and OCIL



OVAL can be used to express automated checks.

OCIL can be used to express manual security checks.

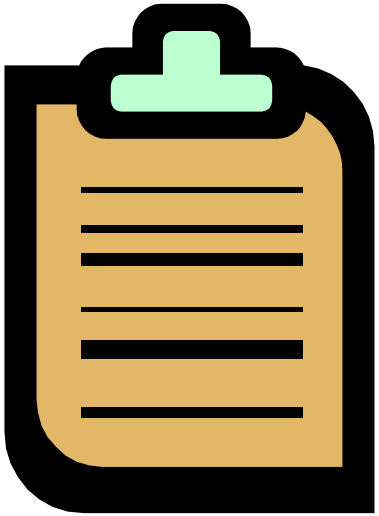
MITRE

Benefits of Using OCIL

- **Provides a common language for manual security checks**
  - **Consistency in check evaluation**
  - **Interoperability between tools**
  - **Ability to share documents between authors**

- **Enables the ability to audit evaluation results and inspect user responses**

Core OCIL Objects



Questionnaire
- Unique Id
- Description
- Set of Actions

Test Action
- Unique Id
- Reference to a Question
- When Clauses

Question
- Unique Id
- Text

OCIL Question Types

1. What type of computer is it?
   a) Laptop
   b) Desktop
   c) Workstation
   d) Server
   e) Not Listed

   ----------> choice_question

2. Who is responsible for the computer? *Answer must be in the following format: last name, first name (e.g. Doe, Jane).*

   ----------> string_question

3. What is the computer's barcode number?

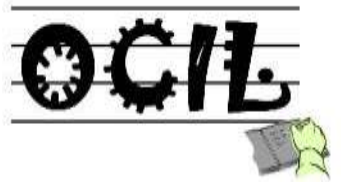
   ----------> numeric_question

4. Is the laptop secured with a cable lock?

   ----------> boolean_question

MITRE

OCIL Question Test Action Types



- Boolean Question Test Action
- Choice Question Test Action
- Numeric Question Test Action
- String Question Test Action

A Question Test Action Type provides evaluation instructions for a particular Question Type.

Example 1:
Questionnaire with A Single Question

Questionnaire 1
ocil:mitre.org:questionnaire:1
Questionnaire for Laptop Security
actions: ocil:mitre.org:testaction:4

Test Action 4
ocil:mitre.org:testaction:4
ocil:mitre.org:question:4
when true/yes: PASS
when false/no: FAIL

Boolean Test Action

Question 4
ocil:mitre.org:question:4
Is the laptop secured with a cable lock?

Boolean Question

Yes or No ?

Example 2: Questionnaire with Multiple Questions

Questionnaire 1
ocil:mitre.org:questionnaire:1
Questionnaire for Laptop Security
actions: ocil:mitre.org:testaction:3

Test Action 3
ocil:mitre.org:testaction:3
ocil:mitre.org:question:3
when choice is b:
ocil:mitre.org.testaction:4
when choice is a, c, d:
NOT APPLICABLE

Choice
Test Action

Question 3
ocil:mitre.org:question:3
Select the option that best describes the system:
a) Desktop
b) Laptop
c) Workstation
d) Not Listed

Choice
Question

Test Action 4
ocil:mitre.org:testaction:4
ocil:mitre.org:question:4
when true/yes: PASS
when false/no: FAIL

Question 4
ocil:mitre.org:question:4
Is the laptop secured with a cable lock?

Example 3: Questionnaire with Multiple Paths

Questionnaire 1
ocil:mitre.org:questionnaire:1
Questionnaire for Laptop Security
actions: ocil:mitre.org:testaction:3

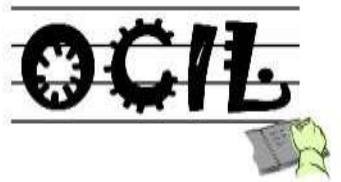
Test Action 3
ocil:mitre.org:testaction:3
ocil:mitre.org:question:3
when choice is a:
ocil:mitre.org.testaction:5
when choice is b:
ocil:mitre.org.testaction:4
when choice is c:
ocil:mitre.org.testaction:7
when choice is d:
ocil:mitre.org.testaction:8

Question 3
ocil:mitre.org:question:3
Select the option that best describes the system:
a) Desktop
b) Laptop
c) Workstation
d) Not Listed

Multiple Paths

?

Example 4:
Questionnaire with Multiple Branches



Questionnaire 1

ocil:mitre.org:questionnaire:1

Questionnaire for Laptop Security

actions:

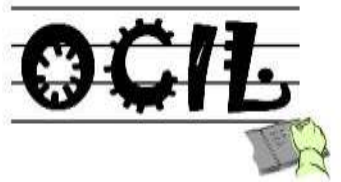
- **ocil:mitre.org:testaction:1**
- **ocil:mitre.org:testaction:2**
- **ocil:mitre.org:testaction:3**
- **ocil:mitre.org:testaction:4**
- **ocil:mitre.org:testaction:5**

Multiple Branches

Logical Operations

AND / OR / NOT

Example 5:
Child Questionnaires



Questionnaire 1

ocil:mitre.org:questionnaire:1

Questionnaire for Laptop Security

actions:

- **ocil:mitre.org:testaction:1**
- **ocil:mitre.org:testaction:2**
- **ocil:mitre.org:questionnaire:2**
- **ocil:mitre.org:questionnaire:3**

OR

Test Action 1

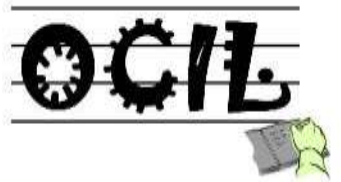
ocil:mitre.org:testaction:2

ocil:mitre.org:question:1

when true/yes: PASS

when false/no: ocil:mitre.org:questionnaire:2

Advance Features

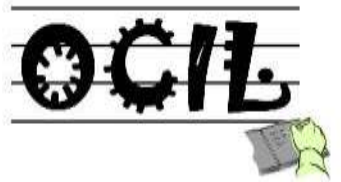


- Including Metadata
- Controlling Evaluation
- Including Artifacts
- Adding Instructions
- Setting Variables
- Recording Evaluation

Summary of Features

- **BASICS:**
  - **Building Simple Questionnaires (e.g. A Single Path)**
  - **Building Complex Questionnaires**
    - **Multiple Paths**
    - **Multiple Branches**
    - **Logical Operations**
    - **Child Questionnaires**
- **ADVANCE:**
  - **Including Metadata**
  - **Controlling Evaluation**
  - **Including Artifacts**
  - **Adding Instructions**
  - **Setting Variables**
  - **Recording Evaluation**

OCIL Reference Implementation



- **Standalone Java Application that demonstrates the features of OCIL**

- **Available at Sourceforge.net**

Activities since OCIL 2.0

- **Inclusion of OCIL 2.0 into the next revision of SCAP (v1.1)**
  - **Update schema, specification, documents, and reference implementation**
  - **Develop SCAP Validation Test Suite for OCIL**
- **OCIL as a NIST IR**

Resources

- **OCIL Specification and Files**

  http://scap.nist.gov/specifications/ocil/

- **OCIL Interpreter**

  http://sourceforge.net/projects/interactive/

- **OCIL Feedback**

  ocil-feedback-list@lists.mitre.org

- **OCIL Developer**

  ocil-developer-list@lists.mitre.org

- **OCIL Developer List Archive**

  http://n2.nabble.com/OCIL-Open-Checklist-Interactive-Language-f3231744.html

Questions