OVAL Compatibility

Andrew Buttner

July 12th, 2006

Goals of OVAL Compatibility

- create a set of guidelines
  - ensure capability incorporates OVAL in a pre-defined and standard way
- develop consistency
  - regarding implementation of OVAL
- tool interoperability
  - importing and exporting data

Program Overview

- three phases
  - declaration
  - implementation
  - evaluation

Types of Compatibility

- compatible with different schema types
  - system characteristics
  - definition
  - results
- based on action
  - producer
  - consumer

Examples

- Definition Producer
  - a vendor that writes OVAL Definitions based on a security advisory
- Definition Consumer
  - a tool that imports OVAL Definitions and evaluates systems based on these definitions

Examples (cont.)

- System Characteristics Producer
  - a tool that generates a system characteristic file based on a machine to be evaluated
- System Characteristics Consumer
  - a tool that imports system characteristic files used to describe the details of a system

Examples (cont.)

- Results Producer
  - a tool that can export the results of an evaluation in the OVAL Results format
- Results Consumer
  - a tool that imports OVAL Results files and displays the results to the user

OVAL Supporter

- those that don't fit compatibility program but still support OVAL
  - a language that includes OVAL Definitions

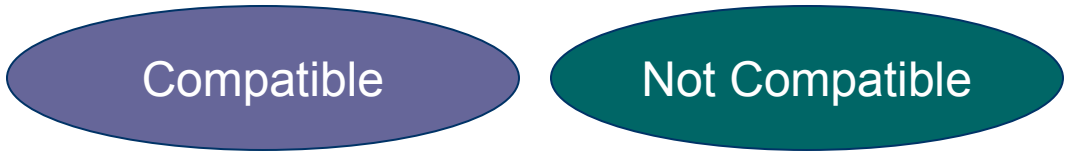
Compatibility Use Cases

- edge use cases
  - Where do we draw the line?
  - Who is compatible and who isn't compatible?

This will help us further define the OVAL Compatibility program.

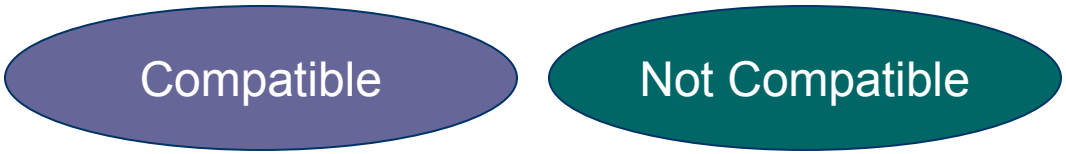
Finder Service

- A pay-for-service is stood up to reference the difference external repositories and provide a single place for a user to go in order to find OVAL Definitions.



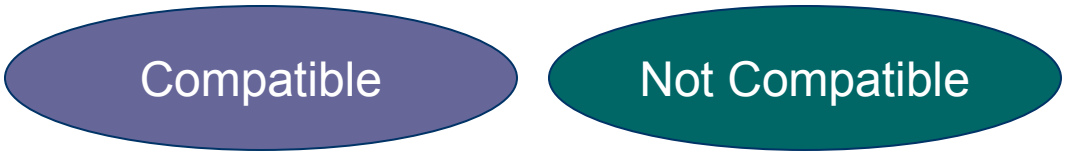
External Repository Provider

- An individual provides new content for an external repository.



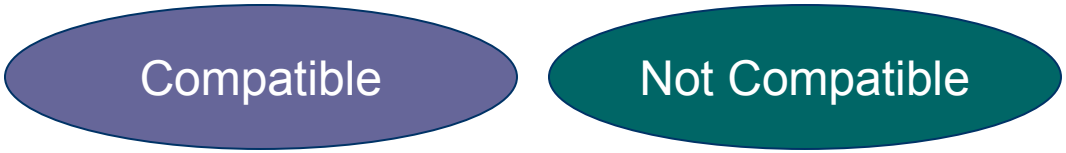
Content Reviewer

- An individual goes through OVAL and adds workarounds to vulnerability definitions.
  - How is this different then someone who writes buggy new content?



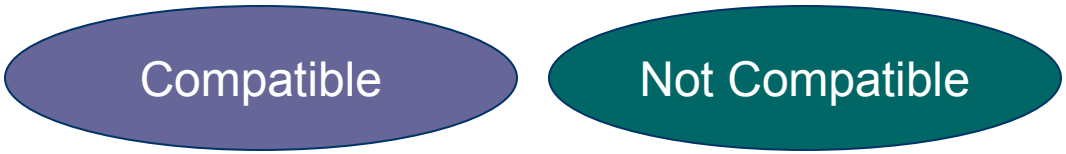
Schema Provider

- An organization submits an AIX schema to OVAL.



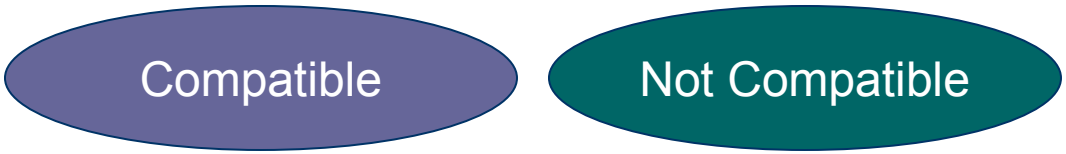
OVAL Component

- A tool integrates a vuln scanner to add to its feature set, it chooses an OVAL compatible scanner.



Depth vs Breadth

- A repository that has 1,000 defs (out of 10,000) vs one that has 10 defs (out of 10)
  - Are both compatible?



Correctness Testing

- the last step in compatibility program
- used to verify that a capability is adhering to the compatibility guidelines
- Walk the line between too strict (no one passes) and too lenient (test loses meaning)

Basic Setup

- Testbed
  - roughly 10 systems networked together
- Test Suites
- Tools evaluate testbed using test suites
  - results of evaluation are compared

Improvements

- Is this working?
- Is this worth it?

- How can we make testing more effective without putting too much burden on the capability or MITRE?