OVAL Remediation Proposal

HP LiveNet Security and Compliance Team

Optimize the business outcome of IT

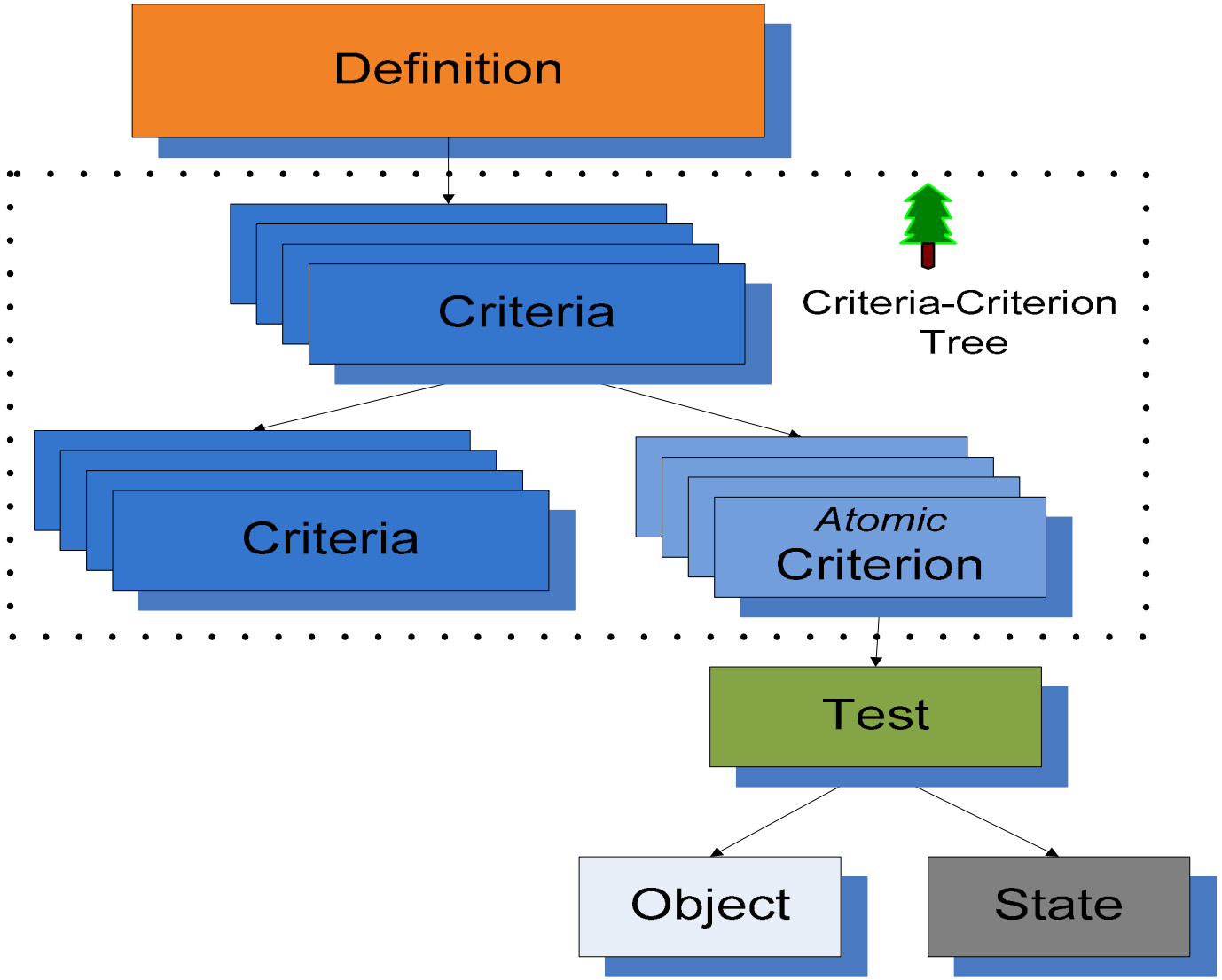
Motivation

- Current OVAL
  - Efficient audit description language
  - Lacks actionability
- User requirement
  - Audit current system
  - Remediate based on non-compliance

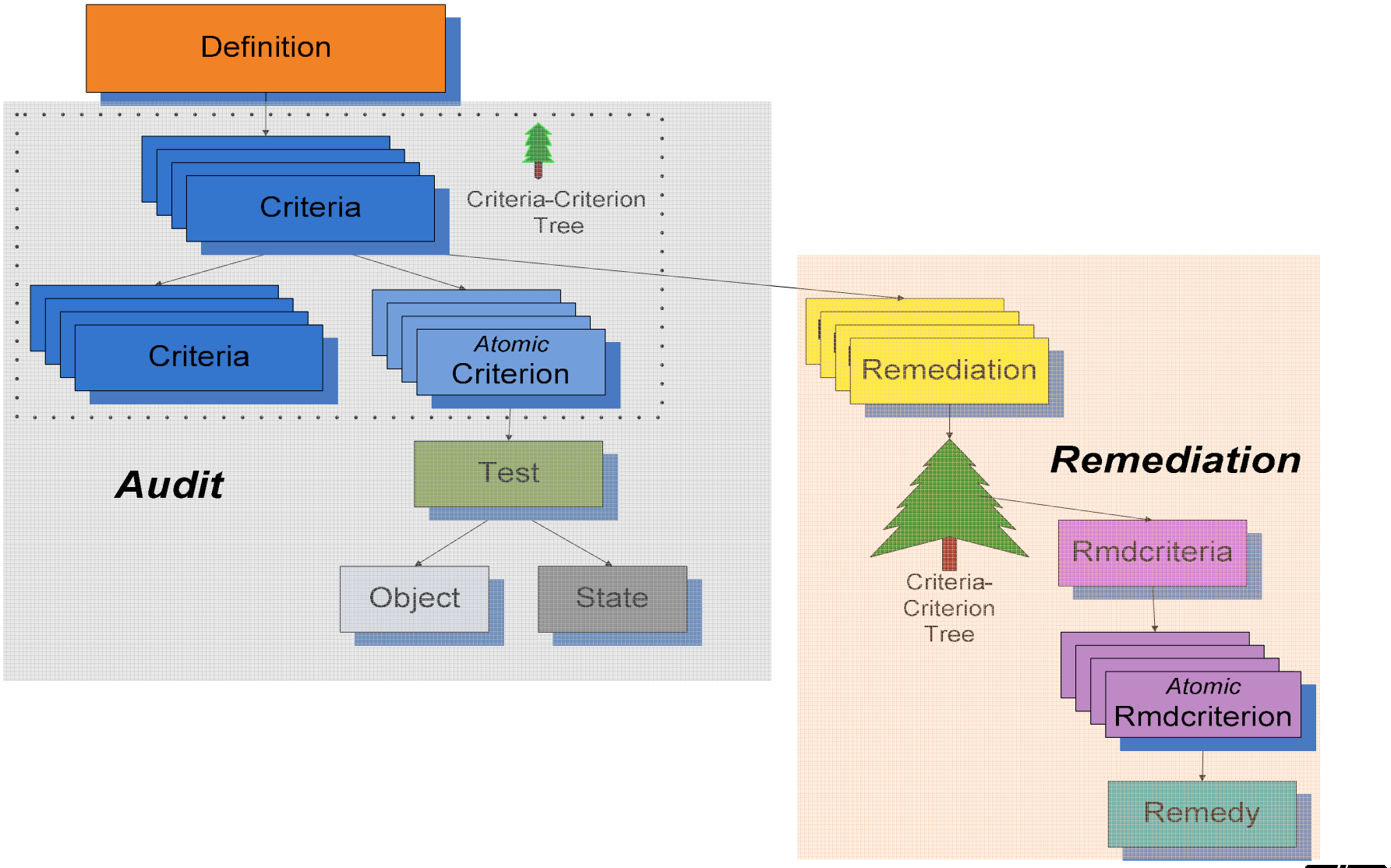
Design principles

- Backward-compatibility
  - Keep current OVAL audit schema intact
- Ease of understanding
  - Syntax of remediation schema is similar to current audit schema
- Extendibility
  - New types of remediation methods are easily supported

Current OVAL structure (w/o remediation)



OVAL structure (with remediation)



OVAL Remediation Structure Elements

- <remediation>
  - Border tag for remediation blocks
- <rmdcriteria>
  - Container for <rmdcriterion> elements
- <rmdcriterion>
  - Define an atomic remediation action
- <remedies>
  - Container for <remedy> elements
- <remedy>
  - Abstract element meant to be extended by individual remedies found in component schemas
  - Causes a change in user environment
  - Atomic in nature

Example OVAL Criteria w/o remediation

```
<definition> …
  <metadata> …….. </metadata>
  <criteria operator="AND“ comment="Win2K,SP4">
    <extend_definition comment="Win2k SP4 or later is installed"
definition_ref="oval:org.mitre.oval:def:229"/>
    <criterion comment="mqrt.dll version is less than 5.0.0.805“
   test_ref="oval:org.mitre.oval:tst:6814"/>
 </criteria>
<definition>
```

Example OVAL Criteria with remediation

```
<definition> …
  <metadata> …….. </metadata>
  <criteria operator="AND“ comment="Win2K,SP4">
    <extend_definition comment="Win2K SP4 or later is installed"
definition_ref="oval:org.mitre.oval:def:229"/>
    <criterion comment="mqrt.dll version is less than 5.0.0.805“
  test_ref="oval:org.mitre.oval:tst:6814"/>
    <remediation> <!-----Remediation border tag-->
      <rmdcriteria order_number=”1”> <!----Remediation
  operations-->
        <rmdcriterion remedy_ref="oval:hplivenet:rmd:0001"
  order_id="1“ comment="install patch for Win2K SP4 based
  on MS07-065"/> <!---- An atomic remediation operation-->
      </rmdcriteria>
    </remediation> <!----Remediation border tag-->
  </criteria>
<definition>
```

Example remedy nodes

```
<patch_remedy id="oval:hplivenet:rmd:0001" version="0"> <!---- An actual
   atomic remediation operation-->
  <description> MS07-065, patch for Win2K SP4 </description>
  <reference source="Microsoft Security Bulletin"
ref_url="http://www.microsoft.com/technet/security/bulletin/ms07-
   065.mspx"/>
  <kb_id>KB937894</kb_id>
  <install_flags>/q:a /r:n</install_flags>
  <need_reboot>true</need_reboot>
  <location type=”http” comment="Microsoft download center">
   <directory>http://download.microsoft.com/download/3/a/e/3ae9546e-
   621b-4429-aca3-ec55377d5f94</directory>
   <name>Windows2000-KB937894-x86-ENU.EXE</name>
  </location>
  <verification
   type="md5">973039d7e42e893b449aa27a4de59904</verification>
  <signature provider="The MITRE Corporation"></signature>
</patch_remedy>
```