
ThreatGuard
Standardized Remediation
Robert L. Hollis
(Director of Product Development)

Why did we do this, why now?

- Vulnerability Definitions
  - Not recommended, too many options
- Inventory Definitions
  - Not applicable
- Patch Definitions
  - Moot
- Compliance Definitions
  - SCAP
  - Gold Disk
  - Automatability

Solving the ‘what’ problem.

- With OVAL <_state>, taking action is easy
  - Introduce <_fix>
- Use OVAL <_object> to know what to change.
- Use OVAL <_tst> to know when to change it.
  - Reference the OVAL file objects from a Remediation content file


ThreatGuard
fdcc-winxp-oval

<!-- EXAMPLE 1 -->

Very similar structure of an OVAL test object.

```
<passwordpolicy_test id="oval:gov.nist.fdcc.xp:tst:12“
  version="1“
  comment="Password history enforcement is enabled and profile
    defined number of passwords are remembered“
  check_existence="at_least_one_exists“
  check="remediate-all">
  <hint>Password history enforcement is enabled and profile defined
number of passwords are remembered</hint>
  <object object_ref="oval:gov.nist.fdcc.xp:obj:8" />
  <fix fix_ref="oval:com.threatguard.xp:fix:1" />
</passwordpolicy_test>
```

Replace the state with a fix reference.

<!-- EXAMPLE 1 -->

```
<passwordpolicy_fix id="oval:com.threatguard.xp:fix:1"
  version="1" test_comment="Password history enforcement is enabled
and profile defined number of passwords are remembered">
  <password_hist_len
   variable_context="true" operation="equals“
   datatype="int">
    <options>
      <option context=“fdcc">24</option>
      <option context="default">24</option>
    </options>
  </password_hist_len>
  <reference state_ref="oval:gov.nist.fdcc.xp:ste:24" />
</passwordpolicy_fix>
```

Operation is an FYI from the state.

Context allow system to apply different values relative to external variables.

Original state is referenced as an FYI.

<!-- EXAMPLE 2 -->

```
<registry_test id="oval:gov.nist.fdcc.xp:tst:2" version="1"
comment="Registry key
HKEY_LOCAL_MACHINE\System\Currentcontrolset\Control\Lsa\Limitblank
passworduse=1" check_existence="at_least_one_exists"
check="remediate-all">
  <hint>Registry key
HKEY_LOCAL_MACHINE\System\Currentcontrolset\Control\Lsa\Limitblank
passworduse=1</hint>
  <object object_ref="oval:gov.nist.fdcc.xp:obj:1" />
  <fix fix_ref="oval:com.threatguard.xp:fix:123" />
</registry_test>
```

<!-- EXAMPLE 2 -->

```
<registry_fix id="oval:com.threatguard.xp:fix:123" version="1"
test_comment="Registry key
HKEY_LOCAL_MACHINE\System\Currentcontrolset\Control\Lsa\Limitblankp
asswordуse=1">
  <value variable_context="true" operation="equals“
   datatype="REG_DWORD">
    <options>
      <option context=“fdcc">1</option>
      <option context="default">1</option>
    </options>
  </value>
  <reference state_ref="oval:gov.nist.fdcc.xp:ste:120" />
</registry_fix>
```

Registry values *must* include the datatype.

<!-- EXAMPLE 3 -->

```
<fileeffectiverights_test id="oval:gov.nist.fdcc.xp:tst:193"
  version="1“
  comment="The Administrators group is granted full access
    to the file arp.exe" check_existence="at_least_one_exists"
    check="remediate-all">
    <hint>The Administrators group is granted full access
     to the file arp.exe</hint>
    <object object_ref="oval:gov.nist.fdcc.xp:obj:83" />
    <fix fix_ref="oval:com.threatguard.xp:fix:241" />
</fileeffectiverights_test>
```

<!-- EXAMPLE 3 -->

```
<fileeffectiverights_fix id="oval:com.threatguard.xp:fix:241“
  version="1" comment="specified account is granted full control"
  test_comment="The Administrators group is granted full access
    to the file arp.exe">
  <standard_delete set_to="1" operation="equals“
    datatype="boolean">
    <options>
      <option context="default">1</option>
    </options>
  </standard_delete>
  <standard_read_control set_to="1" operation="equals“
    datatype="boolean">
    <options>
      <option context="default">1</option>
    </options>
  </standard_read_control>
  <reference state_ref="oval:gov.nist.fdcc.xp:ste:51" />
</fileeffectiverights_fix>
```

Every right specified in OVAL gets explicitly set here.

Challenges

- OVAL has no priority in criteria.
  - Tests can evaluate true for multiple reasons
  - Interpreter can retest between fixes
  - Interpreter does not know which fix to apply first
- Content Automation
  - Datatype Specification (Windows Registry)
  - Ranges

    0 < desired_value < 5
  - Open-ended criteria

    desired_value != 0


ThreatGuard
TM
Deviations

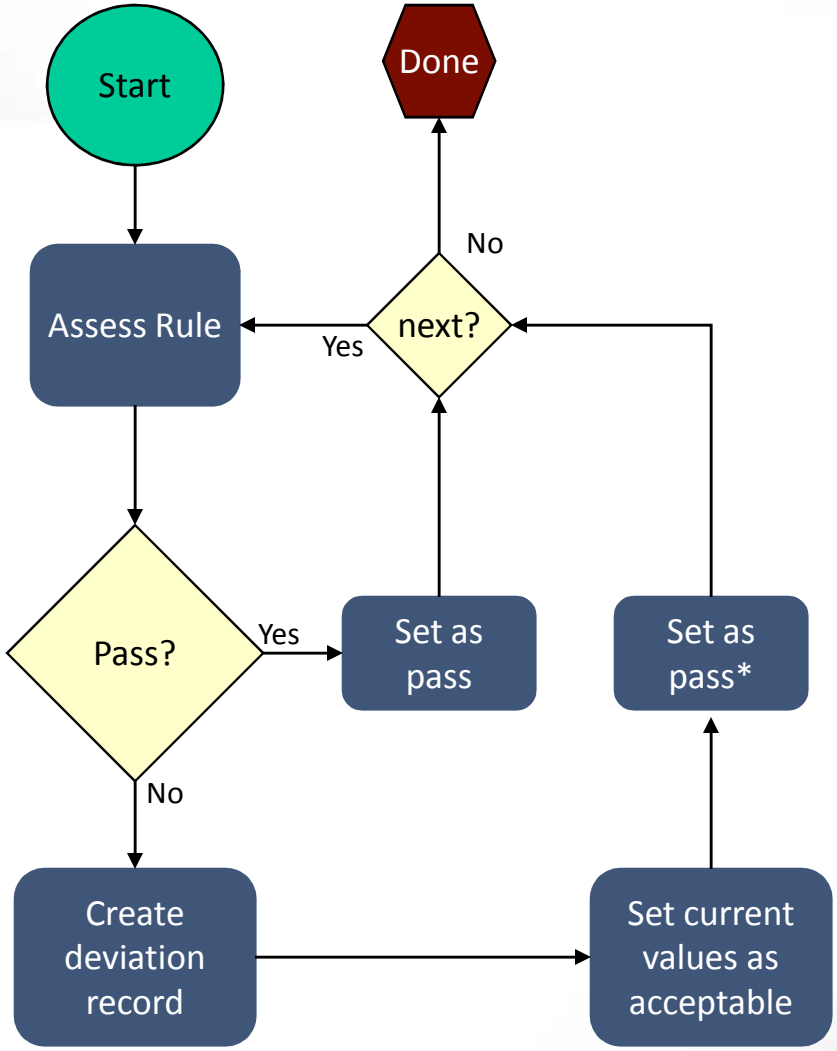
<!-- Deviation -->

Key is tied to schema, not content.

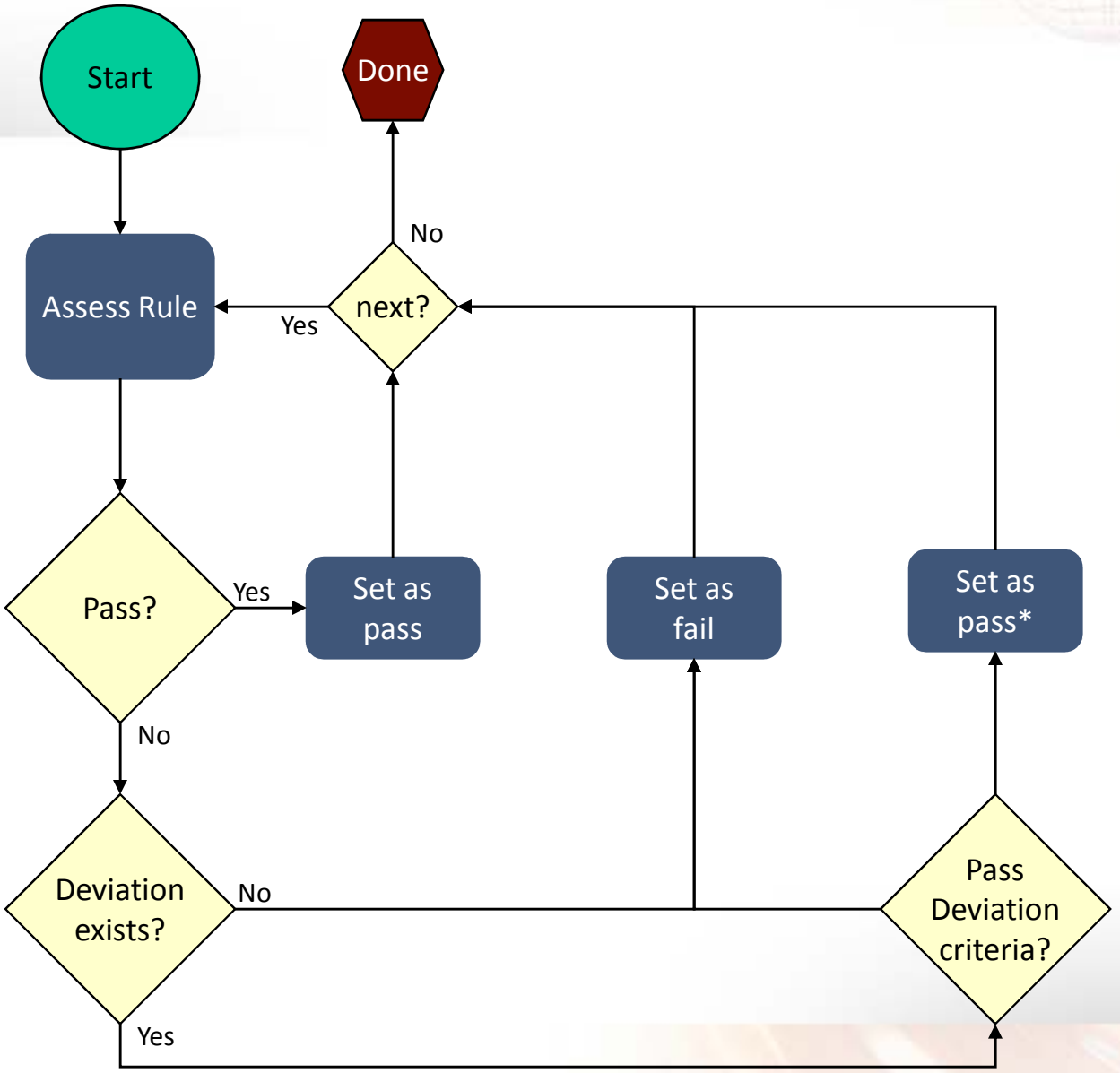
```
<passwordpolicy_deviation
key="passwordpolicy_object#windows_password_hist_len"
hint="Password Policy: Enforce password history can be greater than
or equal 3">
  <deviation operator="greater than or equal">3</deviation>
  <remediate_to>3</remediate_to>
  <dates>
    <established>2008-04-03T10:04:55</established>
    <expiration>2009-03-31T10:04:56</expiration>
  </dates>
  <accountability>
    <party>My Name</party>
    <title>My Title</title>
    <org>My Location</org>
    <email>my.email@agency.gov</email>
    <explanation>Example justification text.</explanation>
    <POAM planned="true">Example POAM text.</POAM>
  </accountability>
</passwordpolicy_deviation>
```

Text required by NIST.

Deviation Profiling



Deviation Assessments



Deviation Remediation