Remediation

April 29th, 2008

MITRE

Agenda

- Overview
  - Whys?
  - Goals
- Development Process
  - Use Cases
  - Requirements
- Content
- OVAL?

MITRE

What is remediation?

Remediation:
the act or process of correcting a fault or deficiency

- Expand this definition to allow for changing the state of a system...
  - fixing a vulnerability
  - updating software
  - Stopping/starting a service??

MITRE

Why now?

- OVAL is now substantially mature
- OVAL Board advisement
- OVAL Community requests
- Government sponsors want it

MITRE

Why us?

- Community - great mix of government, academic, and industry participants
- Experience - several years experience in working together to standardize low level statements about systems
- Good role for MITRE as an FFRDC

MITRE

Goal of Standardizing Remediation Statements

- Primary source vendors produce open standardized remediation statements.
- Enable IA tool vendors to consume and tailor authoritative remediation statements for specific organizations.
- Enable organizations to define their own remediation statements for IA tools to act on.

MITRE

Development Process

1. Use Cases – Define our core set of use cases
2. Requirements – Identify requirements based on our core use cases
3. Design – Design a solution to meet our requirements
4. Draft – A first draft is created and published

MITRE

Use Case: Vulnerability Management

A vulnerability management application detects a vulnerability on a host and must remediate the issue. The application chooses between several possible remedies:

- applying a patch
- stopping a service
- changing the affected application's configuration

Once the selected remedy is applied the application reassesses the affected host to verify the vulnerability has been addressed.

MITRE

Use Case: Configuration Management

A configuration management application has determined that a large set of hosts is not in compliance with a particular configuration setting. The configuration management system must now update all affected hosts.

MITRE

Use Case: Software Management

An enterprise Software Management application has detected that a system is running an old version of an application that does not align with corporate policy. The Software Management application must automatically update the outdated application and then report that the affected system is up to date with the current corporate policy.

MITRE

Requirements???

- SHOULD leverage existing OVAL structures.
- SHOULD be similar in style to the oval-definition-schema to enable quick ramp up for those that are already proficient OVAL authors.
- MUST be capable of pre and post remediation validation.
- MUST enable multiple remedies to be encoded for a given issue.
- MUST not force remediation statements into all OVAL Definitions.

MITRE

Requirements???

- MUST enable organizational tailoring of remediation statements.
- MUST easily accommodate new remediation methods.
- MUST enable encoding of ramifications/impact of a remedy.
- MUST support authoritative signing of remediation statements.
- MUST support verification of all referenced resources.

MITRE

Remediation Content

- Should it be hosted in a community repository?
- Are vendors willing to contribute remediation content?
- Are vendors willing to trust public remediation content?

MITRE

Is remediation in scope for OVAL?

- Should we keep OVAL focused on Assessment?
  - Does adding remediation distract OVAL from its primary goal?

MITRE