joval | CONTINUOUS MONITORING

OVAL Governance & Roadmap

Cybersecurity Innovation Forum 2015

Hi, I’m David Ries from Joval.

- I’m a co-founder of Joval Continuous Monitoring
  - Visit us at Jovalcm.com
- Joval is an embeddable, cross-platform SCAP 1.2 engine for ISVs, MSSPs and enterprises
  - Widely embedded (SAINT, AlienVault, Cavirin, ForeScout, others)
  - Widely deployed (DoD, DoE, MdD Français, DTCC, others)
- I and my Joval teammates are ongoing contributors to SCAP standards including
  - Serving on the OVAL board, actively participating in mailing list discussions
  - Authoring JunOS and NETCONF schemas, dozens of OVAL tests
  - Helping design new OVAL and repository governance models
  - Regularly presenting at conferences

Why am I speaking today?

- I am working with the OVAL migration team
  - Along with folks from Amazon Web Services, CIS, Intel, MITRE, Qualys and Threatguard
  - To develop and launch the new OVAL governance model
- We report to the OVAL Board
  - We benefit from active support by MITRE and DHS
  - We are sponsored by CIS
- But, this is a community-driven project
  - My views are my own
  - Please feel free to challenge or second them on the mailing lists!

Today's Agenda

- There is a new governance model for the OVAL standard… what is it?
  - Review the legacy model
  - Present the new model
- Now that we have a new model, what will we do to advance OVAL?
  - Revisit the purpose of OVAL
  - Assess how well we are fulfilling that purpose
  - Suggest roadmap items

The way it was…

- Historically, OVAL was “curated”
  - MITRE was sponsored by DHS to moderate and facilitate development of the OVAL standard
  - There was open discussion of issues on mailing lists.
  - The OVAL Board made final decisions on what to adopt and when to release.

- This model was a bit slow and opaque
- But it was also so successful that there’s now a thriving international community of security professionals, ISVs, and customers willing and able to take on management and moderation of the standard!

New Model: Our Goals

- Community-run: responsive, transparent and fully open to the public
- Independent: community-supported, independent of direct U.S. Government sponsorship
- Modernized: via adoption of updated tools and processes, based on lessons learned over the past decade

New Model: How it Works

1. A community member **raises an issue** describing a problem or enhancement
   - The Community is notified; at least 7 days of comment
2. Community members **make a proposal** to update the standard to address the **issue**
   - The Community is notified and may **amend a proposal** by collaborating with the contributor or making alternate proposals; at least 14 days of review and revision
   - Community members may **object to a proposal** if it does not fit within the OVAL Use Cases or satisfy the Core Criteria
3. The Supervisor charged with moderating the proposal's subject matter will **adopt the proposal**
   - After evaluating objections, ensuring proposals are valid and complete, and developing rough consensus amongst alternative proposals; **all within set timelines**

New Model: Roles

- Project Sponsor
  - Primarily administrative, minimal substantive role
- OVAL Board: nominated by community
  - Responsible for high-level strategic direction of OVAL
  - Maintain mission, use cases and other key documents
- Supervisors: selected by community
  - Each Supervisor moderates development of specific schema(s) (i.e. Linux, HP-UX, Cisco IOS, etc.)
  - Follow set timelines for review, revision and adoption of updates
  - Enforce criteria for quality and completeness of updates
- Community Members: join the mailing list!
  - Nominate OVAL board members, elect Supervisors
  - Propose updates to the language, processes and roles
  - Engage in review and general discussions

New Model: Status

- Completed
  - Developed and documented initial version of new model
  - Recruited a Sponsor: CIS
  - Recruited initial OVAL Board: Cisco, DTCC, HP, IBM, Intel, Joval, NIST, Qualys, RedHat, SecPod, SPAWAR, Symantec, ThreatGuard, VMWare, others
  - Recruited initial Supervisors: Cisco, HP, Qualys, RedHat, others
- In-process
  - Finish recruiting initial Supervisors
  - Publish project website including community processes, OVAL specifications and documentation, and information about how to engage in the project
  - Publish Github repository of schemas
  - Announce via mailing lists and begin accepting updates from Community

The Future!

- Now that we have a new model, what will we do to advance OVAL?
  - Review the mission
  - Assess how well we are delivering on that mission
  - Identify opportunities to improve

What is the mission of OVAL?

- OVAL is a standard for
  - Evaluating the configuration state of a computer system
  - Reporting on the results of that evaluation
- In other words
  - Writing tests for vulnerability assessment, patch management, configuration management, compliance assessment, and system inventory in a standard format
  - Getting the test results in a standard format
- Having a standard allows us to
  - Decouple security content, scanning technology, and reporting technology
- In other words, the benefits are
  - Better content: content marketplace; authoritative content from platform vendors
  - Better scanning technologies: reduce lock-in; choose best scanning infrastructure(s)
  - Better reporting: use reporting tools of your choice to report on data from any/all sources

So, where have we delivered?

- Mature platform coverage
  - Windows, RedHat, Cisco, HP-UX, Ubuntu
  - Proven schema coverage and tool support
  - High-quality, battle-tested and/or authoritative content (gold standard for maturity)
    - OVAL repository, NIST USGCB for Windows and RHEL, CIS Benchmarks, DISA STIGS, RedHat SCAP Security Guide, Cisco Repository, Canonical's Ubuntu Security Team Repository, and more
- Platforms with coverage and tooling
  - AIX, Juniper, OSX, iOS, Android
  - Schema coverage and tool support, but not proven
  - Authoritative content required for maturation

Areas of Interest for OVAL Development

Tier I: Active Requirements

- Additional Network Devices
  - Palo Alto, Checkpoint, F5, etc.
- Cloud and Software Defined Networking APIs
  - AWS, Azure, OpenStack, Docker, etc.

Tier II: Wish List

- Mobile Devices via interop with MDM solutions
- Printers and IP Telephony Devices
- SCADA devices
- Infrastructure Applications
  - Web servers, DNS servers, LDAP servers, domain controllers, database servers, etc.

Get Involved!

- Sign up for the OVAL developer mailing list in order to get updates on our progress and contribute
  - https://oval.cisecurity.org/community

- Email me with questions and ideas:
  - ries@jovalcm.com

- Ask questions, offer suggestions right now!