Center for Internet Security®

OVAL Repository Transition

Bill Munyan
Technical Product Executive

Content of this Presentation:

- Background
- Transition to GitHub
- Content Contributors
- Content Consumers
- Q & A

The OVAL Repository

- First, thanks go to MITRE

- MITRE has operated the “authoritative source” or “official” OVAL Repository.
  - Mature OVAL Community
  - Consensus reached by OVAL Board, DHS, and OVAL Community for CIS to stand up the new “authoritative” OVAL Repository

- CIS has added the GitHub-based Repository
  - https://github.com/CISecurity/OVALRepo
- CIS has added an OVAL Repository website
  - https://oval.cisecurity.org/repository

Transition to GitHub

- Team of dedicated stakeholders representing numerous OVAL adopters
  - Writing documentation
  - Python scripting
  - Repository serialization
  - Transition timelines, weekly status updates, reports to OVAL Board
- ETL from existing MITRE repository to a “serialized” version at GitHub
  - Definitions organized by class
  - Other artifacts organized by family, artifact type (registry_test, file_object, router_state, etc), and index (based on @id)
- Script libraries, QA procedures, search functionality, and other utilities using Python

Contributing Content – Part 1

- Uses GitHub's "fork and pull" model
- Fork the repository to the contributor's GitHub account
- Contributor clones the fork locally
- Scripts written in Python
  - Find existing OVAL content, build OVAL Definitions files
  - Modify existing OVAL definitions
    - Update OVAL Definition metadata with applicable contributor information
    - "Serialize" updated content to required folder structure
  - Create new OVAL definitions, tests, objects, states, and variables
    - Use python scripts to "serialize" new content to required folder structure
- Use python QA scripts to validate new and updated content
- Push local changes to contributor's fork

Contributing Content – Part 2

- Create a “pull request” to incorporate new/updated content into CIS repository
- CIS processes “pull request”
  - New content given ID’s using the “oval.cisecurity.org” namespace
  - Existing content retains “oval.mitre.org” namespace
- A processed “pull request” automatically notifies the contributor

Consuming Content

- CIS OVAL Repository Website
  - https://oval.cisecurity.org/repository

- See latest updates and top contributors
- Search for OVAL content
- Download OVAL content
  - In bulk, by OVAL language schema version
  - By definition class (compliance, inventory, patch, vulnerability)
  - By definition class and OS family (unix, windows, macos, etc)
  - By definition class and platform (Windows 8, RHEL 6, etc)
- Links to GitHub repository

Q&A