Recommendation Tracker

Bryan Worrell
The MITRE Corporation

MITRE

What is it?

- A graphical tool used for Benchmark creation and editing
- An intuitive, collaboration-based guidance authoring tool
- A layer of abstraction between the end user and 800-126

Functionality

Structures Guidance Document Authoring

- Breaks out the key components of a Benchmark
- Clearly identifies required input fields
- Suggests workflow
- Removes the burden of intimately understanding the underlying standards

Collaboration

- Defines user roles
- Allows synchronization across multiple clients
- Progress tracking

Standardized Content

- Generates and imports 800-126 compliant content

Capabilities we'll cover…

- Benchmark creation
- Benchmark import/editing
- Team based collaboration
- SCAP-valid output

Technologies

- **XCCDF: eXtensible Configuration Checklist Description Format**
  - **An XML specification designed for expressing security benchmarks and assessment results**
- **OVAL: Open Vulnerability and Assessment Language**
  - **An XML specification designed to express system state, enabling automated assessment and compliance checking**
- **OCIL: Open Checklist Interactive Language**
  - **An XML specification designed to express a set of questions to present to a user.**
  - **Used to handle aspects of configuration assessment which cannot be automatable.**
- **CPE: Common Platform Enumeration**
  - **A structured naming scheme for information technology systems, platforms, and packages.**

Benchmark Creation

- A benchmark is analogous to a configuration guide or a policy document
  - Meant for people to read and fall asleep to
- Rules define policy statements or configuration recommendations
  - Turn off the local guest account
  - Set the minimum password length to 8
  - Set passwords to expire every 30 days
- Groups define chapters
  - Collections of related rules

Benchmark Creation: Demo

Benchmark Editing

- The Recommendation Tracker can import 800-126 compliant XCCDF
  - XML elements/structures outside of 800-126 are ignored or mapped to similar RT elements
- After import, users can customize and edit
- Useful for defining policy based off of existing benchmarks
- eSCAPe integration
  - Allows for the editing of OVAL Definition Documents within the RT

Benchmark Editing Demo

Team-based Collaboration

- Guidance takes time to develop
  - Teams are often rolled out to handle this task
- User Roles need to be defined
  - Team leaders
  - Editors
  - Administrators
- Clients are not bound to a network
  - Can work anywhere
  - Need to synchronize data across clients

Collaboration Demo

SCAP Output

- Benchmarks are expressed as XCCDF
  - XCCDF allows for translation into human-readable formats
- Options for an HTML, human readable output
- Can produce incremental revisions of a guide through the use of statuses

Output Demo

Status

- Currently version 1.0
- Verision 2.0 scheduled for release in October
- SourceForge.Net
  - http://sourceforge.net/projects/rectracker/
  - Forums
    - Bugs
    - Feature Requests
    - Feedback!
  - Source code repository