SCAP In Action

Demos of Common SCAP Use Cases

Charles Schmidt
Bryan Worrell
Dan Haynes

MITRE

Documented SCAP Use Cases *(from NIST SP 800-117)*

- Security Configuration Verification
  - SCAP-expressed benchmarks
- Requirements Traceability
- Standardized Security Enumerations
- Vulnerability Measurement

MITRE

Common Use Cases For Today

- Benchmarks
- Incident Response
- Vulnerability Management
- Data Calls

- XCCDF
- OVAL
- OCIL
- CVE
- CCE
- CPE
- CVSS

TOOLS

- Recommendation Tracker (MITRE)
- eSCAPe (G2)
- OVAL Definition Interpreter (MITRE)
- XCCDF Definition Interpreter (MITRE)

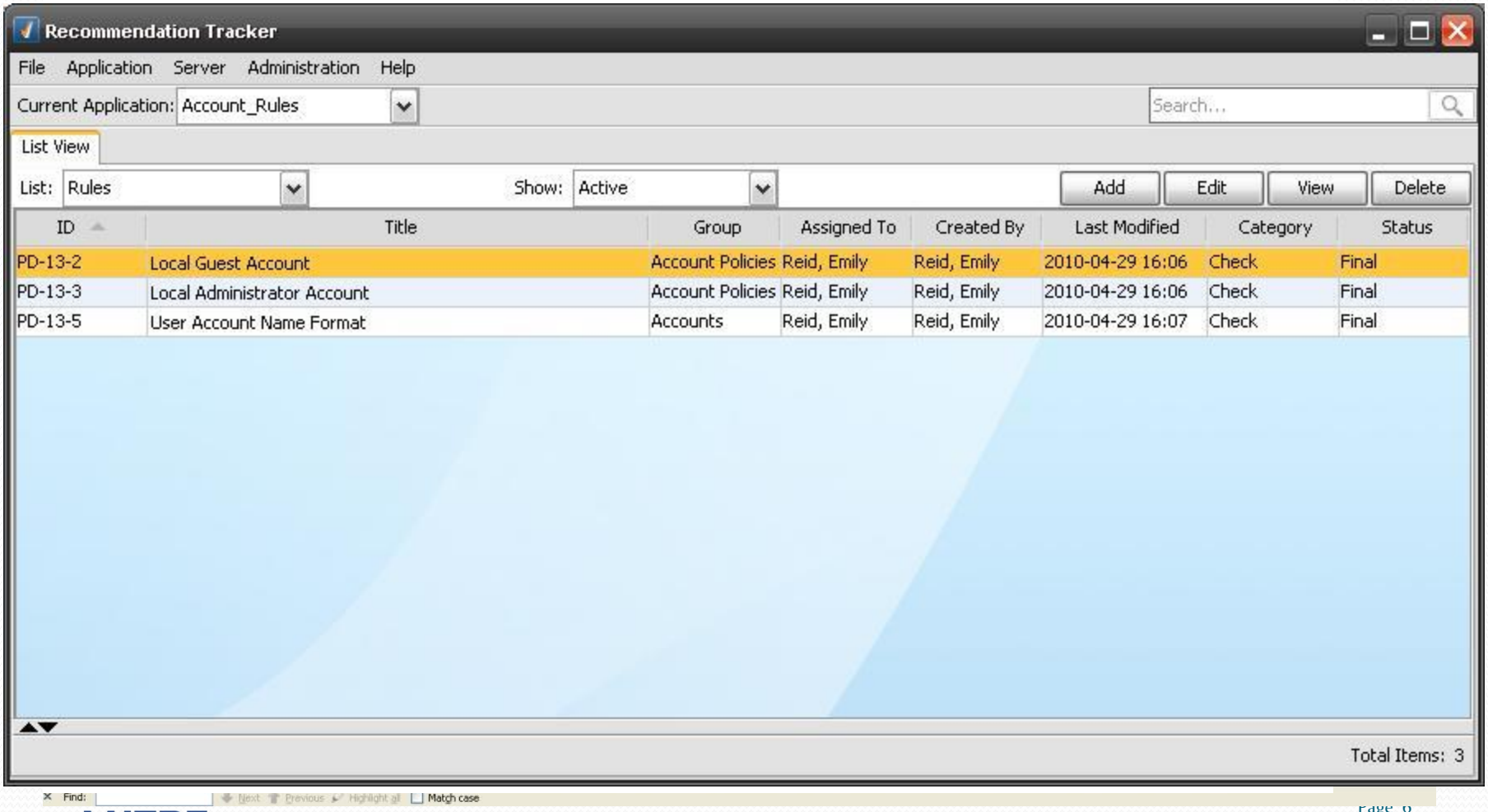
Benchmarks

- Encapsulations of policies in a standardized format
  - Human-readable descriptions
  - Machine processing instructions
- Combination of
  - Policy descriptions standards
  - Automated assessment standards
  - Information correlation standards
- Structured sets of Rules (recommendations)
  - Tailoring allows customized selection of Rules and how those rules would be automated

What can a Benchmark Rule Tell Us

- Recommendation
  - Structure encourages specific, concise, and unambiguous directives
- Rationale
  - States what the control is
  - Risks of not implementing the recommendation
  - Risks of following the recommendation, if appropriate
- How To
  - Step-by-step instructions
- References
  - Correlations to other material (CVE, CCE, CPE, and documents)
- Compliance Check
  - Reference to OVAL or OCIL

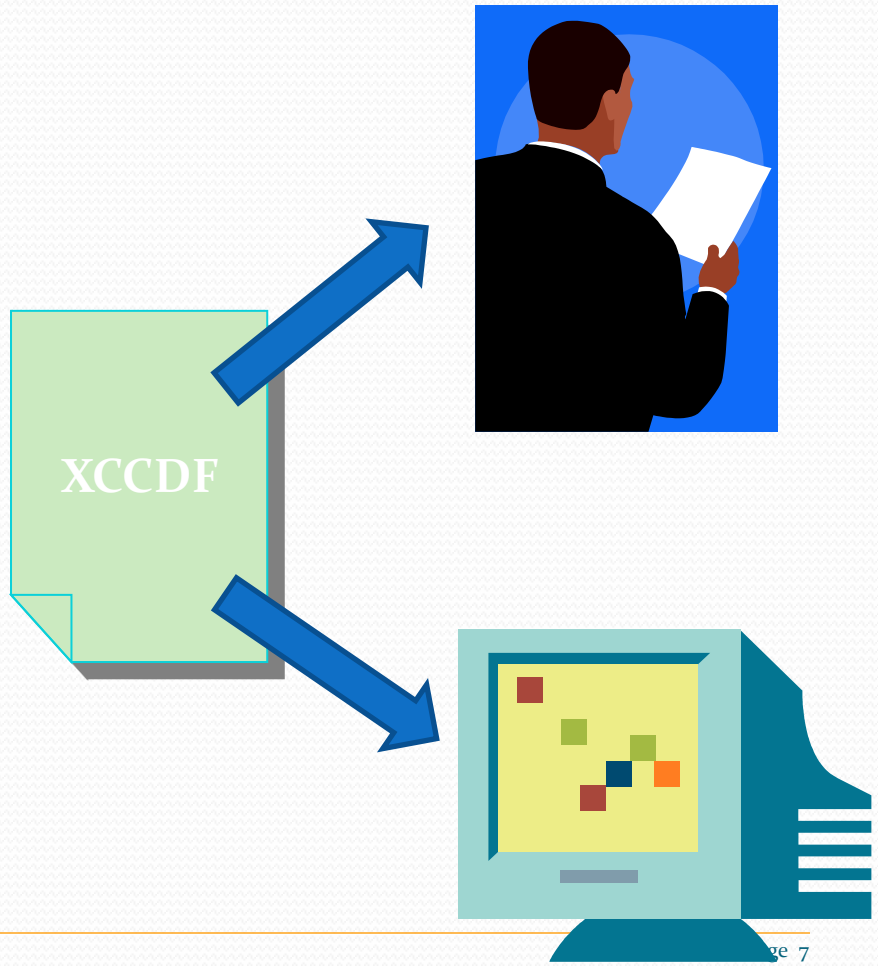
Creating a Benchmark



MITRE

XCCDF & Compliance Checks (OVAL)

- Structure and tailor machine- & human-readable
  - RT facilitates XCCDF benchmark creation
- Automated compliance checks are associated with benchmark rules
  - eSCAPe facilitates OVAL check creation



Benchmark Creation Demo

MITRE

What did we get from SCAP?

- XCCDF used to structure policy
  - Supports human readers and machine assessors
  - Allows tailoring – "One size does not fit all"
- OVAL/OCIL support automated assessment
  - Universal interpretation of compliance
  - Quick, automated results
- CPE/CCE support correlation
  - Clear expression of relevant platforms
  - Clear expression of relevant configuration controls

Incident Response

Operation Aurora

- Starting in mid-December 2009
- Publicly report in January 2010
- Claimed by Google to have originated in China
- Publicly confirmed by high profile companies

MITRE

Incident Response Demo

MITRE

What did we get from SCAP?

- CVEs to track alerts and responses
- OVAL provides a clear description of what it means to be vulnerable, mitigated, and patched
  - Content is publicly reviewed for accuracy
- SCAP compatible tools can use OVAL for automatic assessments
  - All tools will test for the same thing – no disagreement

MITRE

Vulnerability Management

- Collection of Advisories and Responses
- Aligned with Patch Management

- SCAP Use Case
  - Collection of OVAL tests to ascertain health of systems
  - Refer to CVE and CVSS to determine coverage
  - XCCDF can be used as wrapper (or not)

Data Calls

Assume broad deployment of SCAP tools in the DOE …

- SCAP can be used to automate Data Call process
  - Using XCCDF, OVAL, and OCIL
  - SCAP content distributed and executed at remote sites
- SCAP reports easily consolidated
- Less labor intensive with faster responses
  - SCAP automation
  - Standardized report formats

Useful Data Call Standards

- OCIL is a natural choice for Q&A data collection
- More technical options using OVAL
  - Is a machine running Windows 7?
  - Is this patch installed on all systems?
  - Is my system vulnerable to this attack?

MITRE

Data Call Demo

MITRE

What did we get from SCAP?

- OVAL/OCIL support automated assessment
  - Universal interpretation of compliance
  - Quick, automated results
- Many SCAP-compatible tools to process content
  - No “lock-in” to any single vendor
  - “No-frills” tools freely available
- Standardized result formats
  - Open, XML format supports mechanical roll-up & analysis

MITRE

Questions

Acronyms

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
eSCAPe	Enhanced SCAP Editor
OCIL	Open Checklist Interactive Language
OVAL	Open Vulnerability and Assessment Language
OVAL DI	OVAL Definition Interpreter
RT	Recommendation Tracker
SCAP	Secure Content Automation Protocol
XCCDF	Extensible Configuration Checklist Description Format
XCCDF DI	XCCDF Definition Interpreter
XML	Extensible Markup Language