

SCAP Tutorial

4th Annual IT Security Automation Conference
September 22, 2008

Agenda

08:30 – 09:00	Registration
09:00 – 09:15	Welcome
09:15 – 09:45	Introduction: SCAP
09:45 – 10:45	Enumerations: CPE, CVE, CCE
10:45 – 11:00	Break
11:00 – 11:45	Scoring Systems: CVSS
11:45 – 13:00	Lunch
13:00 – 14:45	Languages: XCCDF, OVAL
14:45 – 15:00	Break
15:00 – 16:00	Techniques for Content Creation
16:00 – 16:30	Discussion

Presenters

- Jon Baker (MITRE)
- Matt Barrett (NIST)
- Andrew Buttner (MITRE)
- Karen Scarfone (NIST)

Table Setting

Content vs. Tools

Information Assurance (IA) is the protection of systems and the information they contain.

- **IA content**

- Knowledge about vulnerabilities, threats, misconfigurations, best practices
- e.g.: CIS Benchmarks, US-Cert alerts, Vendor Configuration Guidance

- **IA tools**

- Vulnerability scanners
- IDS
- Patch management systems
- AV products
- Configuration management systems
- Others...

Benefits of Decoupling

- consistency, transparency, and concreteness
 - in the specification and measurement of IA requirements
- communication of IA information
 - between tool categories
 - between organizational units
- autonomous tool investments
 - made by different organizational units
 - global integrated reporting can still be achieved
- reduced duplication of effort
 - IA tool vendors can import (vs. create) authoritative IA content

Other Issues With Status Quo

- ambiguous guidance
 - written in prose
 - multiple valid technical interpretations
- roadblocks to technical collaboration
 - ambiguity leads to “drift” in technical implementations
- no shared data model
 - data models exposing system details are difficult to standardize since content used to analyze the models needs different information

SCAP

SCAP enables the separation of content
and tools