



OCIL in the Enterprise

March 24, 2011

OCIL Today

- **Primary use case is:**
 - one person
 - one target device
 - one evaluation

- **For example: simple configuration on a single box (STIG)**

- **How can this model be extended for use in an enterprise?**
 - Managed centrally
 - Directed at specific roles
 - Applied to multiple targets

- **Not completely an OCIL issue**

(Telos Presentation)

Enterprise Use Case: Requirements

- OCIL was developed towards the single device use cases
- The enterprise use case has **fundamentally different** requirements
- What needs to change to support the enterprise use case?
- Goal is awareness & discussion
 - **NOT** proposing answers or solutions

Enterprise vs. Single Evaluation Use Cases

■ “Local” (e.g. STIG)

- Questions target one **device**
 - Not a role or user
- Answers apply per **device**

■ “Enterprise” (e.g. C&A)

- **Policy**-oriented questions
- Questions target **classes** of assets
- Questions **distributed** over time
- Answers applied per **group** of devices, network, system
- Individual device results may be **inherited** from group

Targeting Questions to Roles

- Enterprise policy questions are usually specified by area of responsibility (role) instead of specific user or specific target asset
- **Where** and **how** is this specified?
 - Is the <targets> element sufficient? Can it be reused on the presentation side?
- How do you **relate** roles to users and **present** the questionnaire to an appropriate set of users
 - Need to track on the results side as well (<targets> element)
- What about workflow? (E.g. POA&M/exception approval)

Targeting Questions At Classes of Assets

- Questions need to be targeted (and results applied) not at specific assets, but at **populations** of assets
- Applies to both content and results
 - Content: *this question must be answered about all web servers*
 - Results: *this answer applies to these specific web servers*
- **Where** and **how** is this represented?
 - XCCDF? OCIL? Others?
 - Asset ID? Asset population?
- What level of abstraction does response apply toward?
 - Answers for populations with specific **exceptions**

Where do we go from here?

- We don't have all the answers
- This problem needs to be solved
- We need your participation:
 - Discussion mailing list (emerging-specs@nist.gov)
 - POC: gmcquire@mitre.org

- Thanks to:
 - Sudhir Gandhe (Telos)
 - Jim Ronayne (DoD)
 - Kent Landfield and Dick Whitehurst (McAfee)
 - Gunnar Engelbach (ThreatGuard)

(Backup) SCAP Questions

- How to use XCCDF target facts with OCIL documents?
- What identifiers and scores for non-CCE items?