SACM Requirements

Nancy Cam-Winget

(ncamwing@cisco.com)

November 2013
Use Case Focus

- Endpoint compliance, inspection, verification
- Configuration management: what types?
- Security Vulnerability management: types?
- What is in a content repository?
  - Charter may bind scope to “Posture Assessments”
What is in scope?

This could be a Posture Collector or Evaluator or both

Should the actual posture assessment evaluation be in scope?
Architectural Requirements

• Discovery
  – How to the applications know where to go to obtain the information sought? Use cases #4, 5, 7, 8, 11, 15, 17 and 18 may require the need to learn how to reach the collectors and evaluators of interest

• Many-to-Many
  – Evaluators and collectors will be interfacing with many of the different applications as defined by the use cases (and vice versa)

• Asynchronous Updates/Notifications: as called out by use cases 7, 8 and 18

• Bulk Updates or filtered updates: obtaining a full repository’s state is called out in some of the use cases
Security Considerations

• Authentication and Authorization of Sources
• Secure communication channels: privacy, integrity
• For privacy: we need to consider whether all information can be shared (many to many)
• What assumptions do we consider:
  – Communication across multiple domains
  – Protection of both content and transport?
Next Steps

• Addition of terms: Collector vs. Evaluator as called out in email

• Outlining requirements per use case
  – Need to converge the use cases 😊