Security Automation and Continuous Monitoring WG

Architecture Status Report

David Waltermire
IETF 87 – Aug 2 2013

Architecture Draft

- Describe protocol requirements (and their associated use cases) as well as a description of how SACM protocols fit together into a system
- Multiple drafts are in process dealing with different aspects (e.g., use cases, requirements, architecture)
- Current drafts are mostly focused on defining what a system looks like
- More detail is needed
  - State specific protocol use – identify gaps
  - Address and tie back to use cases and requirements

Architecture Document

- Multiple proposed I/Ds
  - Gunner Engelbach – SACM Email List
  - draft-waltermire-sacm-architecture-00
  - draft-handt-sacm-alternate-architecture-01

General Open Questions

- Should the scope of the architecture I/D be limited to "Enterprise Security Posture Assessment" only?
  - Is a broader architecture useful to provide context?
- Should we describe an abstract architecture, provide specific examples, or use a hybrid approach?

Other Questions/Comments?