SACM Information Model Submission
draft-wandw-sacm-information-model-00

Dave Waltermire

Kim Watson

July 2014

Miscellaneous Stuff

- Cooperative effort
- Focused mostly on the interfaces and schemas necessary to support endpoint assessment
- Complementary with the other submission
- Biased by what we knew and the compressed timeline
- Includes content for the purpose of starting important conversations

Our Approach

- Reviewed Use Case, Architecture, and Requirements documents
- Defined a “vision” of how endpoint assessment would “operate”
- Focused on Endpoint, Software, Configuration, and Vulnerability Management
- Resulted in Architecture assumptions, information needs, and information elements

Key Information Elements

- Asset Identifiers: endpoint and software
- Other Identifiers: platform configuration item, configuration item, vulnerability
- Catalogues: Available software and posture attributes
- Instances: Software inventory and collected posture attributes
- Guidance: Data that drives collection, evaluation, and reporting actions

Important Conversations

- Architecture considerations
- Defining tasking/collection methods
- The role of source vendors vs 3rd party vendors
- Interacting with repositories
- Defining/maintaining catalogues
- Use of existing work to support SACM information needs
- Evolution of existing work (e.g., enhancements, refactoring/splitting up)