Endpoint Compliance

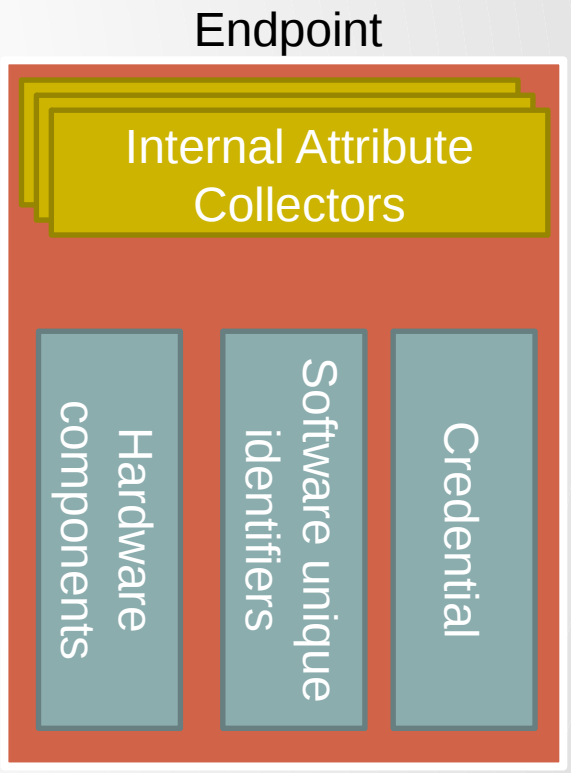
Jessica Fitzgerald-McKay
NSA IAD

Goals

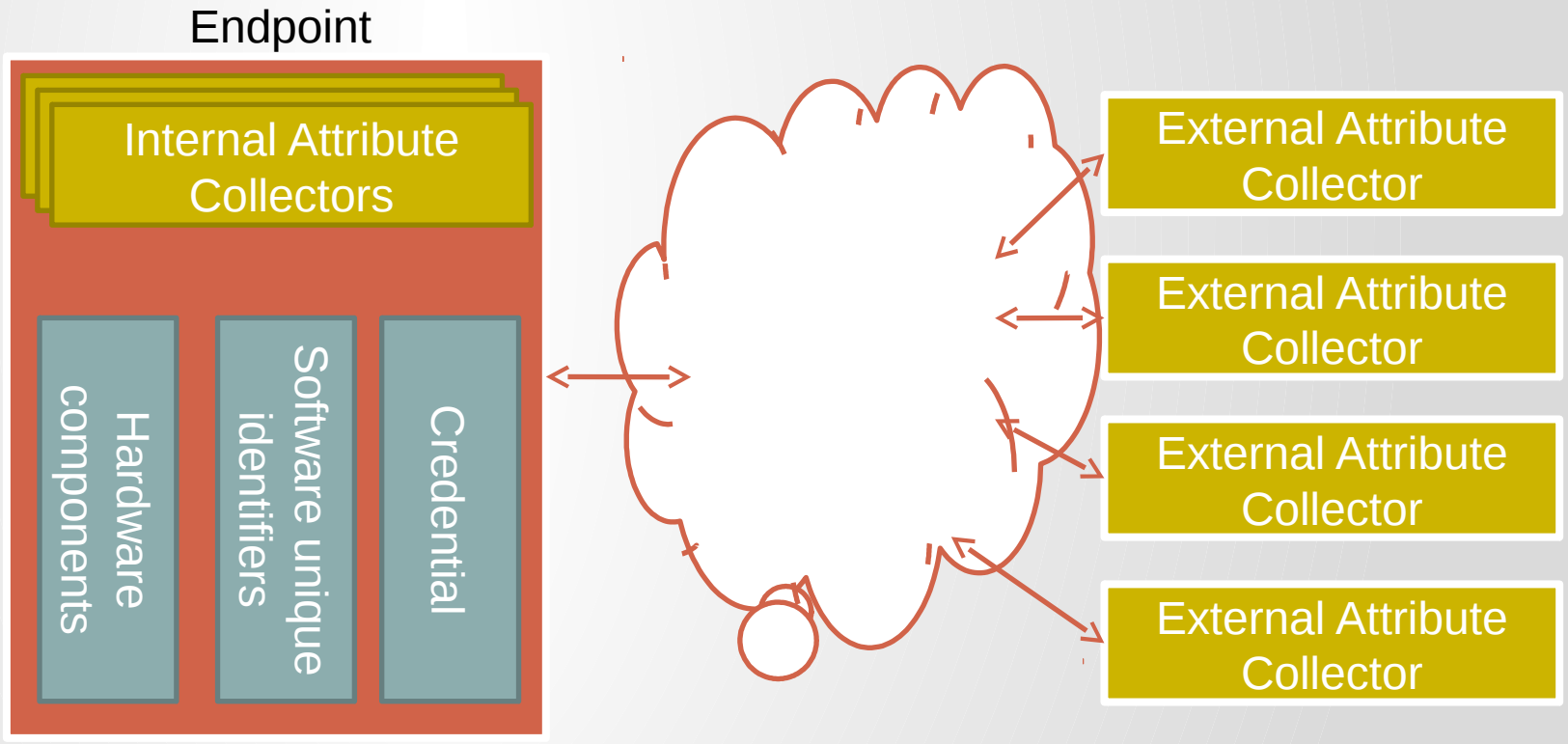
- Network-connected endpoints are known and authorized
- Applications on these endpoints are known and authorized
- All applications are patched and up-to-date
- Applications with vulnerabilities can be located and patched

Relationship to the SACM Architecture

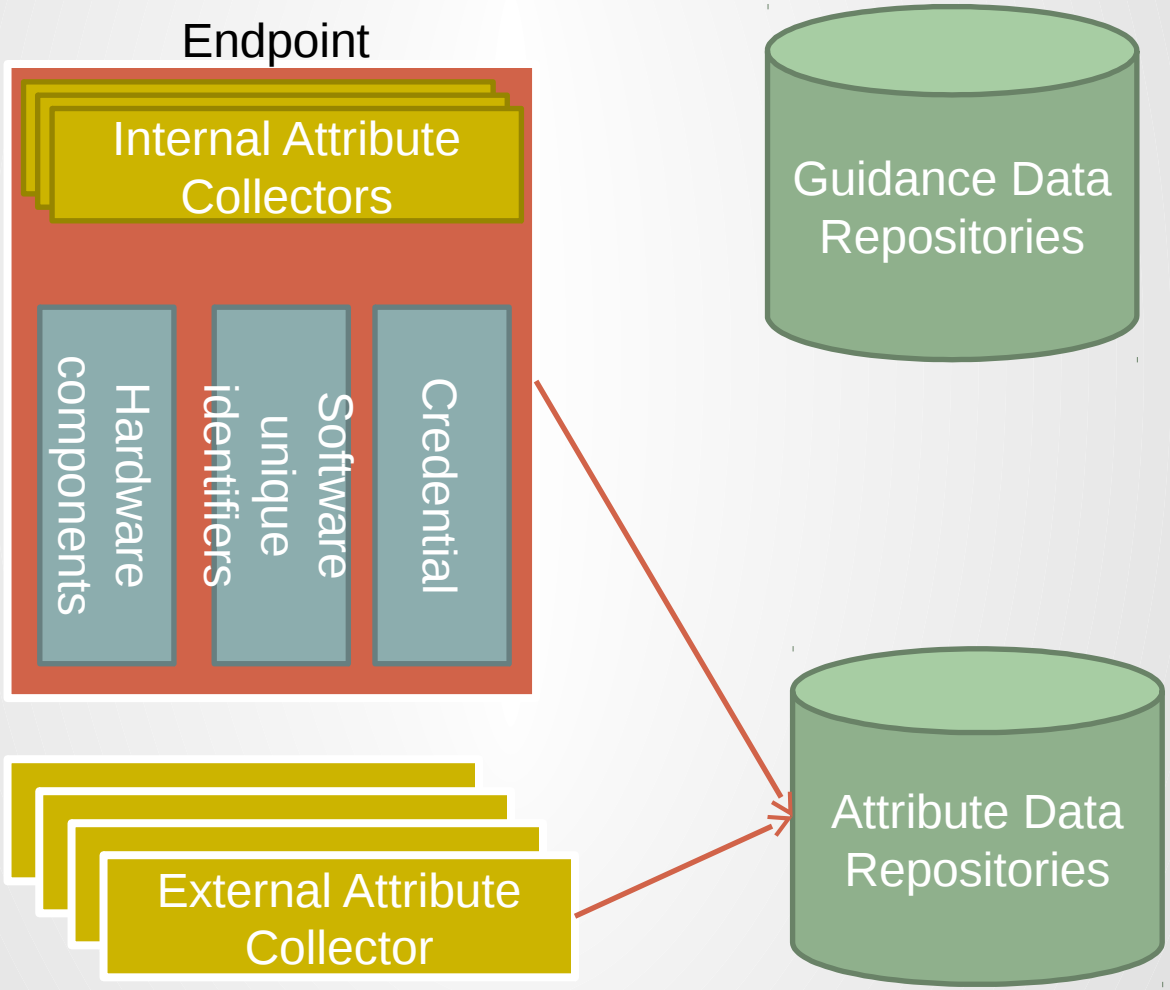
Endpoint Components



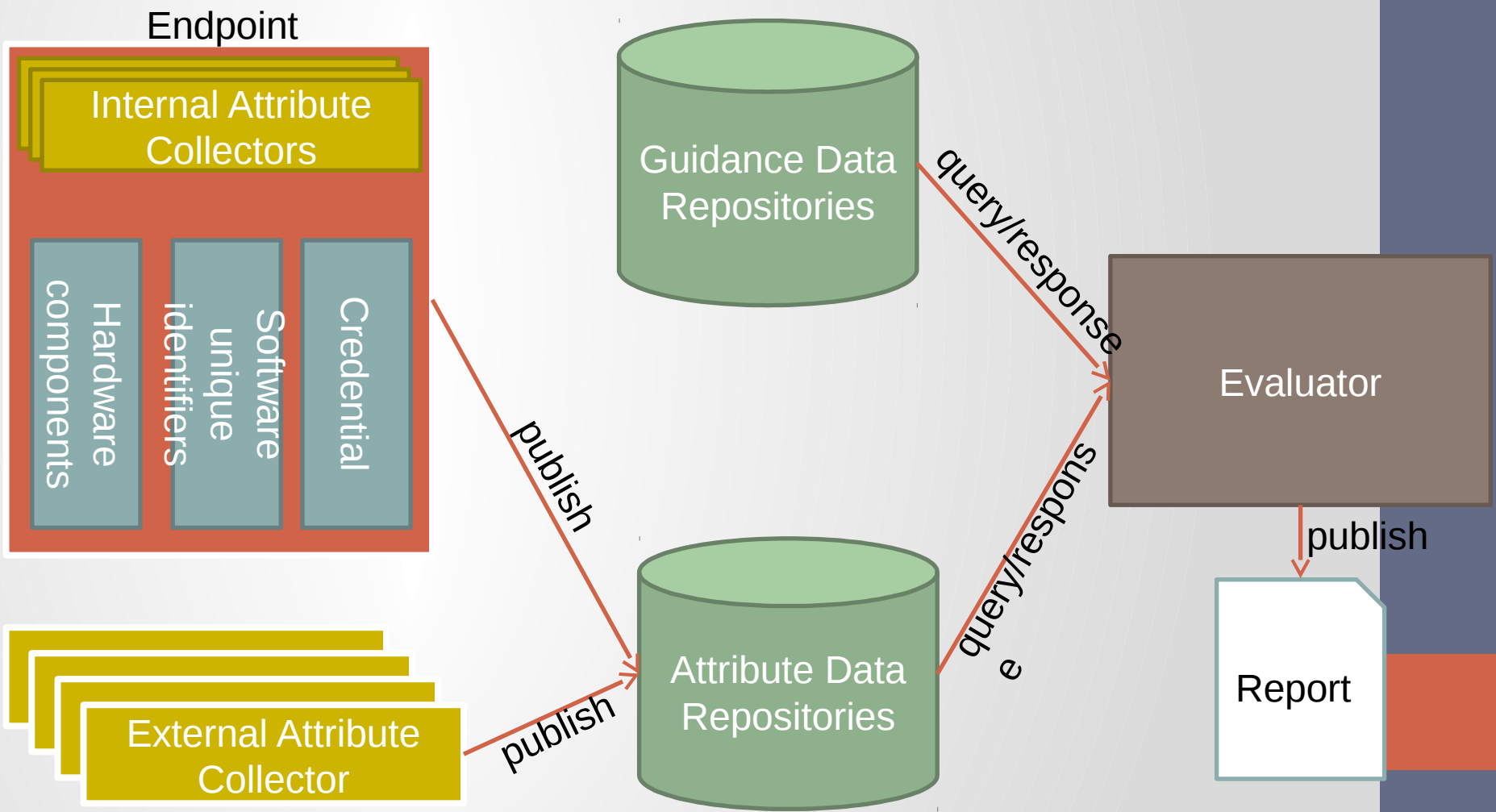
External Attribute Collectors



Data Repositories



Evaluators

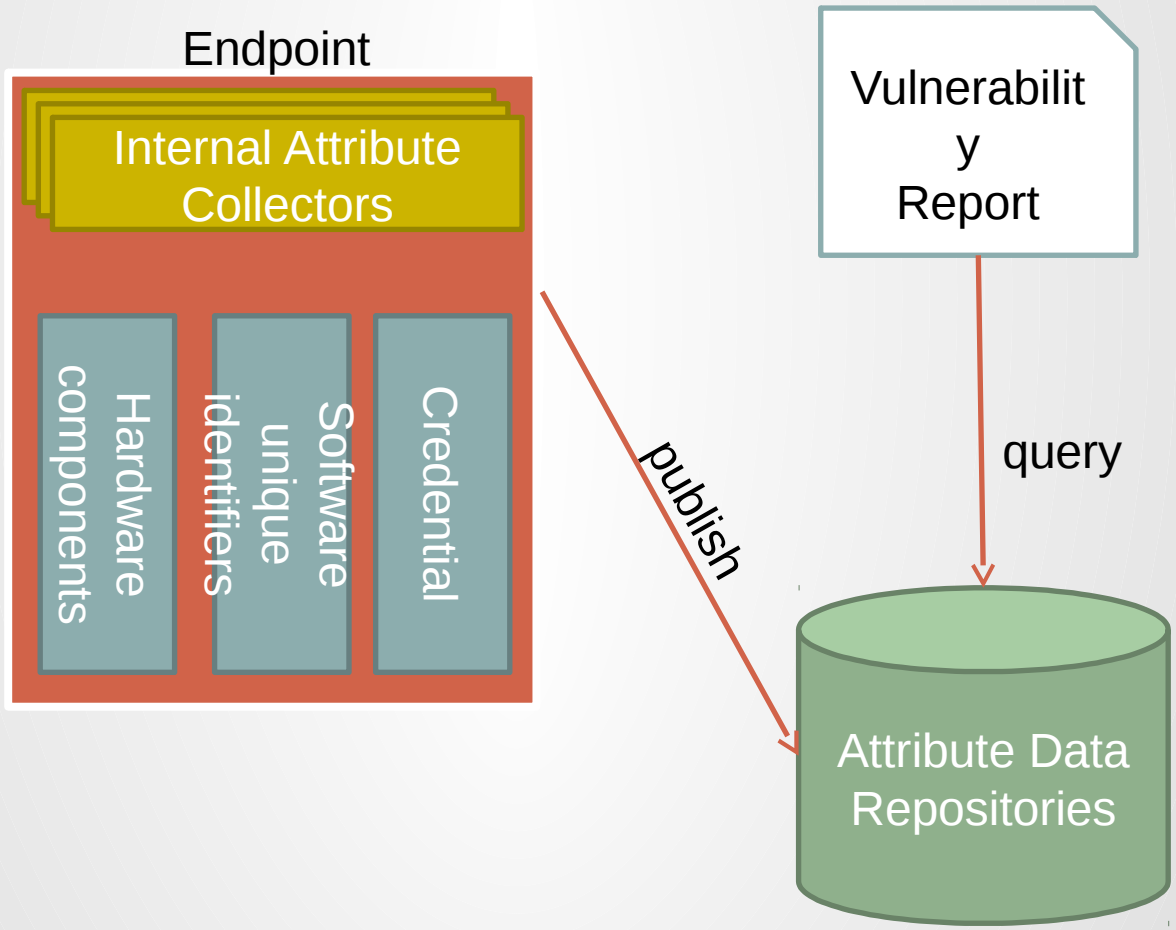

Endpoint
Internal Attribute Collectors
Hardware components
Software unique identifiers
Credential
External Attribute Collector
publish
publish
Guidance Data Repositories
Attribute Data Repositories
query/response
query/respons
e
Evaluator
publish
Report

Relationship to the SACM Use Cases

Building Blocks

- Meets needs for:
  - Data Publication
  - Endpoint Discovery
  - Endpoint Characterization
  - Endpoint Component Inventory
  - Posture Attribute Value Collection
- Enables
  - Data Query
  - Data Retrieval
  - Endpoint Target Identification
  - Posture Attribute Identification
  - Collected Posture Change Detection
  - Posture Attribute Evaluation
- Does not address:
  - Collection Guidance Acquisition
  - Evaluation Guidance Acquisition

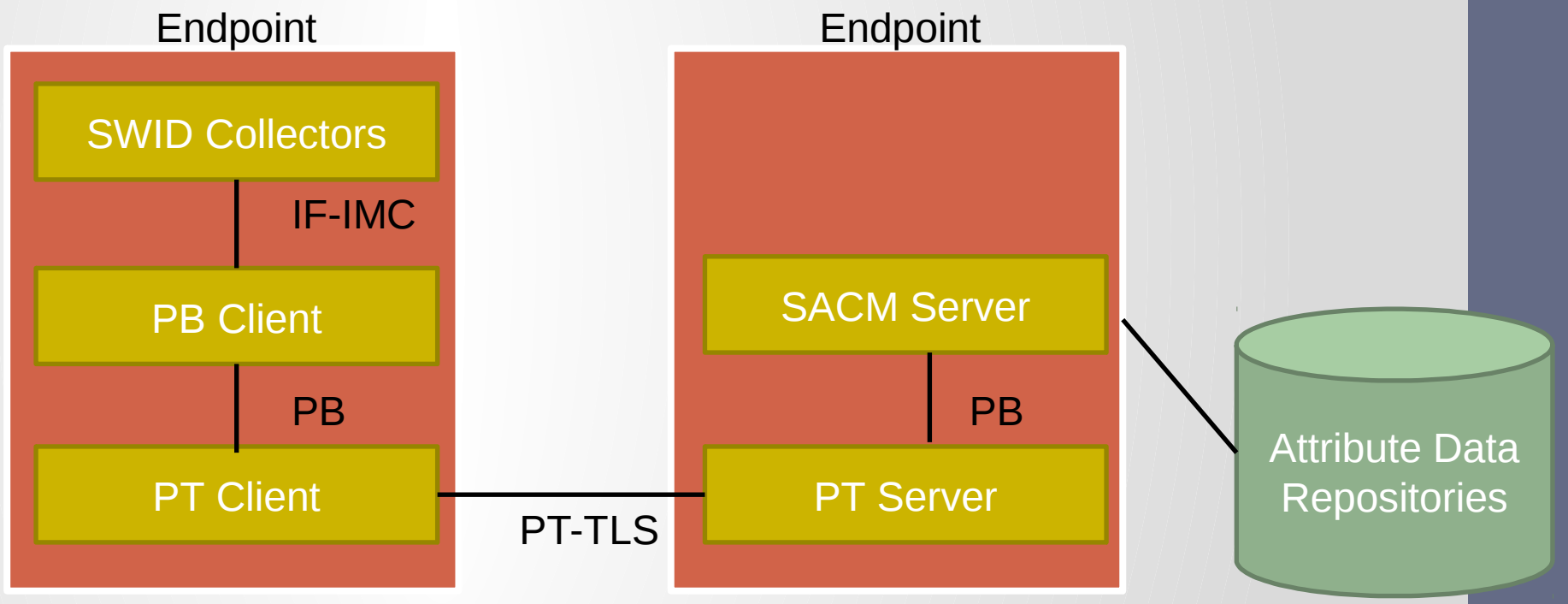
Usage Scenario- Ice Station Zebra



Vulnerability Report Data

- Hardware version/firmware
- Operating system
- Operating system attributes (e.g., version, service pack level, edition, etc.)
- Installed software name
- Installed software attributes (e.g., version, service pack level, edition, etc.)
- Open ports/services
- Operating system optional component inventory
- File system attributes (e.g., versions, size, write date, modified date, checksum, etc.)
- Shared libraries
- Software configuration information

Schema, Protocols and Interfaces


Endpoint
SWID Collectors
IF-IMC
PB Client
PB
PT Client
PT-TLS
Endpoint
SACM Server
PB
PT Server
Attribute Data Repositories

Proposal

High-level

- Focus on endpoint self-reporting of endpoint posture information, in support of use cases such as:
  - Vulnerability management
  - Software asset management
  - Hardware asset management
- Agree to rely on NEA protocols for endpoint self-reporting of posture information

Low-level

- Request TCG release the following specifications to SACM:
  - IF-IMC 1.3
  - IF-IMV 1.4
  - SWID Message and Attributes for IF-M
  - Server Discover and Validation
  - IF-M Segmentation
- Explore edits needed to these specs to meet SACM use cases
  - Separating collection and evaluation functions
  - Developing applicability language to query attribute data store
  - Defining interface between data repository and evaluators