SACM Terminology

Nancy Cam-Winget, (ncamwing@cisco.com)
David Waltermire, (david.waltermire@nist.gov)
March 2014

Current Status

- Updates in -02 draft
  - Many new terms are introduced without definitions
  - Many of the new terms are either no longer used, out of scope, part of a usage scenario definition or already defined in other RFCs

Proposed changes

- Provide Definitions with appropriate existing RFC references for:
  - Expected endpoint state
  - collection task: include its use in terms of “ad hoc” vs. direct
  - evaluation task : include its use in terms of “ad hoc” vs. direct
  - Collection guidance
  - Evaluation guidance
  - Processing artifact
  - Asset
  - Asset characteristics
  - Asset management
  - Building block
  - Endpoint target
  - Endpoint Discovery
  - Evaluation result
  - Security automation
  - Information model: include RFC 3444 reference

Discussion for proposed changes

- Do we need definitions for:
  - Capability
  - System Resource
  - Expected state criteria (or should state be part of the information model?)
- How should we handle different attribute types and states?
- Change “data collection” references to “posture collection”

Backup Slides

List of terms to Remove

- acquisition method
- actor
- actual endpoint state
- ad hoc collection task
- ad hoc evaluation task
- applicable data collection content
- Application
- Appropriate {actor, application, operator}
- Approved {configuration, endpoint configuration, hardware list, software list}
- Artifact, artifact age
- Asset management {data, system}
- Async compliance assessment
- Async vulnerability assessment
- Attack condition
- Automatable configuration guide definition
- Automatable configuration guide publication
- automated checklist verification
- automated endpoint compliance monitoring
- Baseline {compliance}
- Business logic

- Reference RFC 5209 and remove:
  - Assessment {criteria, cycle, planning, subset, trigger}
  - Attribute
  - Collected posture attribute value
  - Collection content acquisition
  - Collection process
  - Collection request
  - Collection task
  - Endpoint {attribute, posture, posture assessment, posture attribute, posture attribute value}
  - Posture {aspect, attribute, aspect change, attribute, attribute evaluation, attribute identification, attribute value, attribute value collection, attribute value query, evaluation}

List of terms to Remove

- Candidate endpoint target
- Change {detection, event, event monitoring, filter, management, management program}
- Checklist {identification, verification}
- Client endpoint
- Compliance assessment cycle
- Compliance {level, monitoring}
- Computing platform endpoint
- Configuration {baseline, data, item, item change, management}
- Content {change detection, data store, definition, instance, publication, query, repository, retrieval}
- Criteria
- Critical vulnerability
- Current sign of malware infection
- Data analysis
- Database mining
- Define content
- Desired state {identification}
- Detection timelines
- Deviation notification
- Discovery
- Endpoint compliance monitory
- Endpoint component inventory
- Endpoint {event, identification, information analysis and reporting, metadata}
- posture attribute value collection endpoint
- posture change monitoring endpoint
- posture compliance endpoint
- posture deviation endpoint
- posture deviation detection endpoint
- posture monitoring
- endpoint {state, target, target identification, type }
- enterprise {function, function definition, policy, standards}
- evaluating data evaluation content acquisition
- evaluation task
- event-driven notification expected function expected state
- Function
- Functional capability
- immediate detection indicator of compromise
- industry group
- information expression
- malicious {activity, configuration item, hardware, software]
- malware infection
- manual endpoint compliance
- monitoring
- mobile endpoint monitoring
- network access control {decision }
- network {event, infrastructure endpoint, location }
- network-connection-driven data collection
- new vulnerability on-demand detection
- ongoing change-event monitoring
- ongoing-event-driven endpoint-posture-change monitoring

List of terms to Remove

- Policy
- Posture {change, deviation, deviation detection}
- previously collected {information, posture attribute value, posture attribute value analysis}
- Process
- public content
- Repository
- publication {metadata, operations}
- publish content query
- regulatory authority
- repository content {identification, retrieval}
- Result {set }
- retrieve content
- Risk {management, management program}
- scheduled task
- search criteria
- secure configuration baseline
- Security {administrator, posture, process}
- Server endpoint
- significant {endpoint event, event}
- signs of infection state
- criteria supporting content
- Whole assessment
- Workflow trigger
- Misconfiguration
- Remediation, software flaw
- Vulnerability {management}
- target target endpoint
- task
- trigger
- unauthorized configuration {item, hardware, software }
- vulnerability {artifact, artifact age, condition, exposure, management, mitigation, remediation}
- ongoing-event-driven monitoring
- operational data operations
- organizational {policy, policy compliance, security posture}
- patch {change, management}
- performance condition
- periodic collection request
- periodic data collection