SACM
Internet-Draft
Intended status: Informational
Expires: August 19, 2014

N. Cam-Winget
Cisco Systems
February 15, 2014

# Secure Automation and Continuous Monitoring (SACM) Requirements
## draft-camwinget-sacm-requirements-03

## Abstract

This document defines the scope and set of requirements for the Secure Automation and Continuous Monitoring working group. The requirements and scope are based on the agreed upon use cases and architecture defined.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 19, 2014.

## Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

## 1. Introduction

Today's challenges of evolving threats and improved analytics to address such threats highlight a need to automate the securing of both information and the systems that store, process and transmit the information. SACM's charter focuses on addressing some of these challenges in a narrower scope by bounding the task to address use cases that pertain to the posture assessment of endpoints.

This document focuses on describing the requirements for facilitating the exchange of posture assessment information, in particular, for the use cases as exemplified in [I-D.ietf-sacm-use-cases].Also, this document uses terminology defined in [I-D.ietf-sacm-terminology].

## 2. Requirements

This document defines requirements based on the SACM use cases defined in [I-D.ietf-sacm-use-cases]. This section describes the requirements used by SACM to assess and compare candidate information models and protocols to suit the architecture. These requirements express characteristics or features that a candidate protocol or data model must be capable of offering so as to ensure security and interoperability.

### 2.1. Reference Architecture Model

A proposed architecture model is provided to highlight the functions and focus for SACM. More specifically to highlight the transport, protocols and data model by which:

- Endpoints cam be discovered for the purpose of collection of posture attributes (or values) by a general collector, a posture

attribute collector or a posture attribute evaluator.  The communications is shown as "A" in the diagram below.

- An (Posture) Assessment Consumer (which could also be a collector) can retrieve posture attributes either directly from a Posture Assessment Repository (shown as D below) or indirectly from an Evaluator (shown as B below).

How a system determines what posture attributes are to be collected or evaluated is out of scope for SACM.

```
            +-----------+             +-----------+
+---------------------+
            | Endpoint  | <....A....> | Evaluator | <....B....>  | Assessment
Consumer |
            +-----------+             |  Service  |
|                     |
                                      +-----------+
+---------------------+
                                +-------|   ^                                ^
            +-----------+       |           | C                              |
            | Endpoint  | <-----+           v                                |
            +-----------+            +-------------+                         |
                                     | Repository  |                         |
                                     +-------------+                         |
                                                                             |
                                 +--------------------+           D          |
                                 | Posture Assessment |<---------------------+
                                 |     Repository     |
                                 +--------------------+
```

Simple Architectural Model

The functional components in the proposed architecture are defined as:

- Endpoint: is the endpoint of interest that is posture validated.

- Evaluator Service: is the service that determines what posture attributes it must collect and evaluate to provide a posture assessment of an endpoint.  In order to evaluate posture, this service must determine the posture attributes it must assess; in addition, it may also provide the collection function as needed to evaluate the posture attributes.  Conversely, this service need only provide the "collection" function if the posture attribute values are the result of an already determined posture attribute evaluation (for instance, if the endpoint can provide that information).

- Repository: is the storage component bound to the Evaluator that contains the posture assessment information.

- Posture Assessment Repository: is another type of repository (or a Collector type) that holds posture assessment information. While not bound to the Evaluator, it is another source of posture assessment information (e.g. a data aggregation point aggregating posture assessment with other attributes) that can provide information to serve SACM use cases.

- Assessment Consumer: is the service that requires the posture assessments information of one or more assets.

Using this architectural reference model, the interfaces, data models and transports used to affect the posture assessment, e.g. A in the figure above have already been defined by different mechanisms, for example, an IETF defined one through NEA. As the focus of SACM is the information exchange to obtain the posture assessment information, it can be achieved through the interfaces shown as B. That is, it is not clear that there is a requirement for the Assessment Consumer to tap directly into the Repository. Similarly, it is not clear that SACM is chartered to define the interfaces and data model for how an Evaluator stores and transports the assessment results to the Repository. Thus, the focus of the requirements will revolve around the data models, protocols and transports for B, the communication of posture assessment from an Evaluator to an Assessment Consumer.

### 2.2. General SACM requirements

The use cases defined in [I-D.ietf-sacm-use-cases] apply to many deployment scenarios. To ensure interoperability, scalability and flexibility in any of these deployments, the following requirements are defined for all use cases:

G-001 The data models, protocols and transports defined by SACM must be extensible to allow support for non-standard and future extensions.

G-002 The data models, protocols and transports must be specified with enough details and state machine to ensure interoperability.

G-003 SACM must support a broad set of deployment scenarios. As such, it is possible that the size or posture assessment information can vary from a single assessment that is small in (record or

datagram) size to a very large datagram or a very large set of assessments and must be addressed by the SACM specifications defined. Thus, the data models, protocols and transports must be scalable.

G-004 Considerations for the lightweight implementations of data models and transports is required. Use cases, especially in the vulnerability assessment and threat defense applications require time criticality in both obtaining the information as well as consuming (e.g. parsing) the data. The agility requirement is to ensure that the data model, protocols, transports and its implementations are suitable to fit in different deployment models and scenarios.

G-005 Different transports must be supported to address different deployment and time constraints. Supporting the link layer, transport and application layers.

G-006 For interoperability and scope boundary, an explicit set of data attributes as mandatory to implement should be defined. While the SACM charter defines the focus to be on posture assessment, attributes corresponding to Posture Assessment should be described.

G-007 To address security and privacy considerations, the data model, protocols and transport must consider authorization based on roles to only allow authorized requestors and publishers to access the information being requested or published.

## 2.3. Requirements based on Use Cases

This section describes the requirements that may apply to information models, data models, protocols or transports as identified by the use cases in [I-D.ietf-sacm-use-cases] and referenced by the section numbers from that draft.

REQ-001 Use Cases in the whole of Section 2 describe the need for an Attribute Dictionary. With SACM's scope focused on Posture Assessment, the attribute collection and aggregation must have a well understood set of attributes inclusive of their meaning or usage intent.

REQ-002 Use Case 2.1.1 describes the need for an Information Model to drive content definition. As SACM endeavors to reuse already existing standards which may have their own data models defined by instantiating an information model, the data models can be mapped to SACM's information model. See [RFC3444] for a description and distinctions between an information and data model.

REQ-003 Use Case 2.1.1 describes the need to instantiate a data model that can map to the SACM protocols for posture content operations such as publication, query, change detection and asynchronous notifications.

REQ-004 Use Case 2.1.2 describes the need to discover endpoints and their composition.

REQ-005 Use Case 2.1.2 describes the need for the data model to support a query operation based on a set of attributes to facilitate collection of information such as posture assessment, inventory (of endpoints or endpoint components) and configuration checklist. .

REQ-006 Use Case 2.1.3 describes the need for the data model to support the means for the information to be collected through a query mechanism. Furthermore, the query operation requires filtering capabilities to allow for only a subset of information to be retrieved. The query operation may be a synchronous request or asynchronous request.

REQ-007 Use Cases 2.1.3, 2.1.4 and 2.1.5 describe the need for the data model to support the means for the information to be published asynchronously. Similarly, the data model must support the means for a requestor to obtain updates or change modifications asynchronously. Like the query operation, these update notifications can be set up with a filter to allow for only a subset of posture assessment information to be obtained.

REQ-008 Use Cases 2.1.4 and 2.1.5 describes the need for the data model to support scalability. For example, the query operation may result in a very large set of attributes as well as a large set of targets.

## 3. Acknowledgements

The authors would like to thank Barbara Fraser, Jim Bieda and Adam Montville for reviewing and contributing to this draft.

## 4. IANA Considerations

This memo includes no request to IANA.

## 5. Security Considerations

This document defines the requirements for SACM. As such, it is expected that several data models, protocols and transports may be defined or reused from already existing standards. This section will

highlight security considerations that may apply to SACM based on the architecture and standards applied in SACM.

## 6. References

### 6.1. Normative References

[I-D.ietf-sacm-terminology]
Waltermire, D., Montville, A., and D. Harrington, "Terminology for Security Assessment", draft-ietf-sacm-terminology-02 (work in progress), January 2014.

[I-D.ietf-sacm-use-cases]
Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", draft-ietf-sacm-use-cases-05 (work in progress), November 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 6.2. Informative References

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", RFC 3444, January 2003.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, June 2008.

Author's Address

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
US

Email: ncamwing@cisco.com