Security Automation and Continuous Monitoring
Internet-Draft
Intended status: Informational
Expires: March 11, 2017

M. Hansbury
D. Haynes
The MITRE Corporation
J. Gonzalez
Department of Homeland Security

September 7, 2016

# OVAL and the SACM Information Model
# draft-hansbury-sacm-oval-info-model-mapping-03

Abstract

The OVAL community has spent more than ten years developing and employing the OVAL Language. During this time, the community has made a number of design decisions and learned a number of lessons that should be leveraged as the next-generation endpoint posture assessment standards are formulated. There are also a number of places where portions of the OVAL Language align with the SACM Information Model and could serve as a starting point for related work. Another output of the work executed under the OVAL project is a number of lessons that are applicable to the SACM work. These lessons include a clear separation of data collection and evaluation; a call to focus on ensuring both primary source vendors and third party security experts feel invited to the discussion and are empowered to leverage their unique domain knowledge; and to strive for simplicity and flexibility, where possible. In addition, the OVAL community has a set of clear recommendations with respect to which parts of OVAL should be used by SACM as a means to make best use of the efforts of those that have worked on and supported OVAL over the past ten years. Those recommendations are:

- Use the OVAL System Characteristics Model to inform the development of a data model for representing endpoint posture attributes.

- Use the OVAL Definitions Model to inform the development of data models for representing evaluation and collection guidance.

- Do not use the OVAL Results Model to inform the development of a data model for representing evaluation results.

Lastly, this document will discuss the OVAL submission, how it is expected to be used, and how it aligns with the SACM Vulnerability Assessment Scenario.

## Status of This Memo



## Copyright Notice



## Table of Contents

## 1. Introduction

The Security Automation and Continuous Monitoring (SACM) IETF Working Group [SACM] has been chartered with standardizing the mechanisms by which endpoint security assessment is performed. This includes software inventory, compliance and vulnerability management, and other related activities. The Working Group has created a series of artifacts [SACM-DOCUMENTS] to capture the important concepts required to accomplish this goal. In addition to Use Cases, Requirements, and Architecture documents, the Working Group has created an initial draft of an Information Model that describes the high-level components and concepts that fulfill the already defined requirements.

This white paper discusses how the Open Vulnerability and Assessment Language (OVAL) [OVAL-DOCUMENTATION] can be used to inform the development of data models that implement the Information Model defined by the SACM group. This paper is not meant to suggest that the entire OVAL Data Model could-or even should-be supported by SACM; rather, it breaks apart the various components of the OVAL Language and discusses how each could be used to satisfy parts of the Information Model.

This document assumes that the reader is already familiar with OVAL and its structures. For those readers that require more in-depth information about OVAL, please review the OVAL Tutorial documentation [OVAL-DEFINITION-TUTORIAL] and other related documentation. This document describes how these structures can be thought of as data models whose scopes and activities overlap with the SACM Information Model.

Additionally, in later sections, the paper presents lessons learned from the ten plus years of OVAL development and curation, related gaps, and how the OVAL submission is expected to be used and how it aligns with the SACM Vulnerability Assessment Scenario [I-D.coffin-sacm-vuln-scenario].

### 1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

## 2. SACM Information Model

The information model defined by the SACM Working Group captures the types of objects and data required to fulfill the defined SACM Requirements [I-D.ietf-sacm-requirements]. It additionally provides details on the flow of data to and from the different objects in the system, in conjunction with the SACM Architecture document [I-D.ietf-sacm-architecture]. The document describes all of these things in a protocol and data format neutral manner.

The document provides descriptions of the various components that are required to perform endpoint assessments, along with some usage scenarios, and the potential mapping from OVAL to any of these defined components wherever OVAL may be relevant.

## 3. OVAL Language

The OVAL Language is made up of several parts, each responsible for encapsulating a part of the assessment model. Each part is discussed briefly below [STRUCTURE-OF-OVAL].

Note: A word about Core vs. Platform Extensions. OVAL can be broadly split into Core structures, which are those that are foundational and give the overall structure to the OVAL Language, and the Platform Extensions, which are platform-specific structures that extend the Core in order to provide ways to encode the underlying low-level, platform-specific tests used by OVAL Content. This paper is chiefly focused on mapping the Core into the SACM Information Model.

In a similar fashion, while thinking about how to implement the SACM Information Model, two distinct levels must be considered:

1. Platform-agnostic, high level concepts

2. Platform-specific concepts

### 3.1. Core OVAL Models

The OVAL Language is made up of three primary core data models which define the three steps of the assessment process (desired state, actual state, and the results of comparing the actual state against the desired state), three supplemental core data models, and a processing model which describes how all the core data models work together.

#### 3.1.1. Core OVAL Data Models

There are a number of data models defined as part of OVAL. This section discusses the three most important data models.

##### 3.1.1.1. OVAL Definitions Model

The Definitions Model is the central component of the OVAL Language. The structures in this model allow an author to encode what posture data to collect, the expected values for the data, and the rules by which to evaluate that data. However, the current design requires authors to include both what data must be collected, and how the collected data is to be evaluated in a Definition which couples these two separate, but, related concepts together. For more information, see Section 6.2 below.

The OVAL Definitions Model provides a Definition object that is the root element for any OVAL check. It contains a set of criteria, either simple or complex, to define how the evaluation should operate. In addition, the OVAL Definitions Model defines the base structures that are used by the Platform Extensions to extend OVAL, as well as Functions, and other high-level concepts.

##### 3.1.1.2. OVAL System Characteristics Model

The OVAL System Characteristics Model defines structures to encode the actual posture data that is collected. It provides basic structures for representing this data, including the Item construct, which is the base structure for recording collected data in OVAL. It also provides structures for capturing information about the endpoint from which the data was collected, including OS information, endpoint identification information (such as IP and MAC addresses), and other relevant endpoint metadata.

##### 3.1.1.3. OVAL Results Model

Finally, OVAL provides a third model to encode the results of the evaluation, the OVAL Results Model. This model provides structures to capture essential information about the evaluation results, such

as the overall results of each definition evaluation and when the assessment occurred. Additionally, the Results model provides a way to include both the guidance (Definitions) and collected data (System Characteristics) used for the evaluation. By capturing this additional data, the Results model provides a comprehensive way to capture the information used to determine the result in addition to the results themselves.

#### 3.1.2. Additional Core OVAL Data Models

Additional data models are defined that support specific capabilities that are sometimes useful in conjunction with the OVAL models previously discussed. The models discussed in this section are not intended to stand alone, and require the use of one or more of the core OVAL models.

##### 3.1.2.1. OVAL Common Model

The Common Model is a very simple collection of global building blocks, such as enumerations used throughout the other models, along with some other foundational pieces. Common values are defined in this model once and then applied within other OVAL models, thus reducing redundancy between each OVAL data model. Examples of the elements provided by the OVAL Common Model are enumerations that provide useful value sets for use within OVAL, such as family types ("windows", "unix", etc.), data types (e.g., "string," "boolean," "int," etc.), and class types (e.g., "vulnerability," "compliance," etc.).

##### 3.1.2.2. OVAL Variables Model

The OVAL Variables Model provides a simple framework for externally specifying variable values used for the evaluation of an OVAL Definitions document at runtime.

##### 3.1.2.3. OVAL Directives Model

The OVAL Directives Model provides a very simple model with structures to indicate the level of detail that should be present in an OVAL Results document. This can be used by an evaluator to produce a desired level of result detail.

#### 3.1.3. Processing Model

The OVAL Processing Model describes in detail how the core OVAL data models are used to produce OVAL Definitions, OVAL System Characteristics, and OVAL Results.

## 4. Relating the OVAL Models to the SACM Information Model

The following section discusses each piece of the SACM Information Model, where one or more OVAL models align, wholly or in part.

### 4.1. Attribute Collector

The SACM Information Model defines both Internal and External Attribute Collectors. Both are components that perform the collection of posture information from an endpoint. The Information Model lists a number of examples of Collectors such as Network Intrusion Detection Systems (NIDS), NEA posture collectors, and vulnerability scanners. While OVAL is not directly applicable for some types of Attribute Collectors such as NIDS, it is certainly applicable for NEA posture collectors and vulnerability scanners that require the collection and evaluation of configuration and other endpoint state information.

An Attribute Collector needs to be instructed as to what specific posture attributes must be collected, when or how often those attributes must be collected, and how to share the collected attributes. In some cases, an Attribute Collector may simply collect data and directly respond to the caller with the required results. In others, it may monitor the endpoint for changes and report these changes when the change occurs, or may execute the data collection at a future time or at some interval. In these last two cases, the collector will need to know how to share the collected data. The OVAL Language does not provide any mechanism for instructing tools where to send collected data, but the OVAL Definitions Model can (among other things) encode what data must be collected; however, it does not allow (as currently constructed) for providing any notion of what constitutes valid data collection (i.e., how recent data must be to be considered acceptable, and how and where it was collected).

Additionally, the OVAL Definitions Model could be modified to support monitoring of events. As it is today, OVAL doesn't have any explicit way to include these instructions, but it would be simple to modify the model to include this notion.

The OVAL System Characteristics Model allows the encoding of collected information and can be used to implement a data format for sharing collected data. While OVAL does not require that tools store data using a standardized format (though they are free to do so), a standardized format is required to allow tools to exchange data. The OVAL System Characteristics Model provides a standardized way to encode this information for exchange.

### 4.2. Evaluator

An Evaluator is the component that analyzes inputs such as Posture Attributes and Evaluation Guidance to determine the result of a particular assessment. It is the piece that answers a question about the security posture of one more endpoints. The Evaluator must be able to ingest inputs of various types, understand the question or questions asked of it, and analyze the inputs to make a determination.

In this case, OVAL could be used to provide several of the required inputs to an Evaluator. The format defined in the OVAL Definitions Model could be used to express Evaluation Guidance. Note that when mapping the OVAL Definitions Data Model to the SACM Information Model, it is important to distinguish between Collection and Evaluation within the OVAL Definitions Model. The OVAL Definitions Model structures currently combine both the Collection ("what to collect") and Evaluation ("what the data should look like"). One of the key concepts within the SACM Information Model is that Collection and Evaluation should be separate concepts. Nonetheless, OVAL contains building blocks that could inform solutions that satisfy this need.

Similarly, the structures defined in the OVAL System Characteristics Model and the OVAL Results Model could be used to inform the solutions that define the Attributes input to the Evaluator and the results of an assessment respectively.

### 4.3. Endpoint Attribute Assertion

According to the SACM Information Model, an Endpoint Attribute Assertion is a way to indicate that a specified set of posture attributes or events were present on an endpoint during a specific interval of time. For example, an Assertion could be made that a particular Windows server had the following attributes from 1/1/2015 - 1/8/2015:

- os = Windows 7

- mac-address = 01:24:42:58:34:2b

OVAL does not have a direct corollary to this construct; however, the structures defined by the OVAL System Characteristics Model could provide a base from which such a construct could be built. The System Characteristics Data Model is designed to capture posture attributes, and as such, could be extended or modified to include the concept of a time interval.

Additionally, it is important to note that the SACM Information Model also states that Events can be included within an Endpoint Attribute Assertion. While "event" and "attribute" are often used interchangeably, in the SACM Information Model, these two concepts are considered distinct. The distinction is that an "event" is something that has a value that does not change until something causes a change, whereas an "attribute" is something that is observed at a moment in time. The Endpoint Attribute Assertion deals with both posture attributes and events during a time interval. No special treatment is given to Events within OVAL as it is currently constructed, although, as stated previously, adding a time interval to support Events is simple to do.

## 4.4. Evaluation Result

An Evaluation Result is the representation of the analysis of a given set of Posture Attributes against Evaluation Guidance. The OVAL Results Model structures can be used to encode one or more Evaluation Results.

## 4.5. Collection Guidance

Within the SACM Information Model, Collection Guidance is defined as information that describes which Posture Attributes must be collected from one or more endpoints. It is the means by which an Attribute Collector determines what information it must collect, as well as when that information must be collected (including intervals for repeated collection activities).

The OVAL Definitions Model provides structures capable of expressing information about what data must be collected for an assessment. It is important to note that the method by which the OVAL Definitions Model accomplishes this will not necessarily directly apply to the SACM Information Model in its current state. In many cases, which specific posture attributes should be collected is not distinct from its evaluation guidance. For the OVAL Definitions Model to be used to implement the SACM Information Model, work would need to be undertaken to de-couple these concepts.

While the model provides the ability to encode details such as what data must be collected from the endpoint, it does not currently provide the ability to include information such as collection interval. The model can be extended, however, to add this capability. Adding the concept of an "interval" to the model to capture the concept may be a way to accomplish this goal.

Important Note: One of the key drawbacks to OVAL is that Platform Extensions (using the OVAL Definitions Model as a base) must be

created for each platform and data source to capture any Posture Attributes that must be collected for a given platform and data source. As a result, it is not easy or scalable to create or update extensions for rapidly changing platforms and products in a timely manner.

With this in mind, it is important that any use of the OVAL Definitions Model to satisfy Collection Guidance for SACM should warrant consideration of updates that change this from a solution where the low-level platform details are part of the language itself, to one where the format provides a way for domain experts (ideally primary source vendors) to instruct tools what Posture Attributes to collect.

This also applies to the next section (Evaluation Guidance).

### 4.6. Evaluation Guidance

The Evaluation Guidance component contains the information that directs an Evaluator how to perform one or more assessments based on collected data. Evaluation Guidance must direct the Evaluator on what the expected state of collected data should be. Additionally, it must be able to specify desired characteristics of the data. That is, it must be able to not only cite the specific posture attributes under evaluation, but also to specify characteristics such as the type of tool that was used to collect the data, how old the data is, etc.

The Evaluator must then ingest this guidance, locate the required data-whether locally or remotely available-and then execute the analysis required.

OVAL offers the OVAL Definitions Model to provide the structures for encoding the expected state or values for evaluating collected data. The OVAL Language does not currently provide a way to specify the expected characteristics of the data, but the OVAL Definitions Model could be augmented to include this type of information. Alternatively, the concept could be added elsewhere and re-used as appropriate. Allowing for the description of characteristics information will be important to allow evaluation to do things like only use data if it's been collected within the past x days or only query data that is collected by a credentialed collector.

Again, as Collection and Evaluation are intertwined currently in the OVAL Language, some work will be required to de-couple them for use with the Evaluation Guidance component.

### 4.7. Provenance

While the SACM Information Model does not attempt to define provenance, it does describe metadata that should be included when exchanging and evaluating posture attribute information (e.g., source of origin, time of collection, observation, etc.). This metadata aims to provide SACM users with enough information to make a determination about the provenance of data as it applies to their enterprise.

Within the OVAL Common Model, a Generator structure is defined to express both what created the content, and when it was created. While the purpose of this structure does not meet all the metadata needs for SACM, it could be used as a building block and be extended to achieve this goal.

## 5. SACM Constructs with No OVAL Mapping

Finally, while there are many similarities between what is defined by the SACM Information Model and the OVAL data models, there are some things discussed in the SACM Information Model document that are either different from or not supported within OVAL.

### 5.1. Tasking

The SACM Information Model discusses Tasks in a few places, including the Collector, Evaluator, and Reporting sections. Tasks represent of notion of "do something at this time", "do something until told otherwise", or "do X when Y occurs". OVAL does not support any notion of a tasking model as currently defined.

While the OVAL Definitions Model (or some derivative) could be referenced by a model that captures tasking, it may be difficult to support all of the needs of tasking in this way. Tasking may already be well defined by another, existing model, and if so, it might be best to leverage that existing work.

### 5.2. Event-driven Actions

Within the SACM Information Model, in addition to posture attributes, events are also often part of the data collection activities. Events are discussed as both part of an Endpoint Attribute Assertion, and an Endpoint Attribute Collector. In each case, it is clear that, in addition to the collection of posture attribute data, event data must also be taken into account.

The OVAL Language does not have any notion of capturing events directly. It is constructed to allow the representation of Posture

Attribute data within the OVAL System Characteristics Model, but event data is absent from that model. OVAL can be modified to support Events in large part by simply extending it to include a time interval.

### 5.3. User and Authorization

The Information Model talks about Users (i.e., one or more end users or roles) and Authorizations (i.e., their authority to undertake actions). While OVAL includes some entities that may relate to these types of concepts, they appear in very specific low-level tests like Windows and UNIX user-related tests. OVAL lacks any general concept of Users or Authorizations that could be applied across its core data structures. The recommendation is to identify and integrate an external solution into relevant OVAL models to achieve required capabilities in this area.

### 5.4. Location

Similar to Users and Authorization, Locations are defined in the Information Model. Locations include physical location (e.g., department, room, Global Positioning System (GPS), wall-jack, etc.) and logical location (e.g., authentication points, which network infrastructure endpoints it is connected to, etc.).

Again, as for Users and Authorization, the recommendation is for the relevant OVAL models to be integrated with other solutions to meet these requirements.

## 6. Lessons Learned and Gaps

Over the course of ten-plus years in moderating the OVAL project, those involved in the project have released over 15 distinct versions of the Language, 25 versions of the OVAL Interpreter, and have processed over 25,000 OVAL Definitions in the OVAL Repository. In addition, the team has spent a lot of time interacting with security tool vendors, researchers, primary source vendors, and commercial and government end users, discussing their needs and struggles. As such, the following lessons learned are presented to help ensure that the collective experience of the group is shared with the larger community.

In addition to a description of the lesson, each also has a suggested application for the SACM work.

### 6.1. Simplicity is Key

#### 6.1.1. Lesson

Endpoint assessment covers a broad set of activities. From organization to organization, assessment has different meanings, and what is "good enough" for one group, barely scratches the surface for another. Experience suggested that caution must be used to avoid unnecessary complexity as a means to address this diversity.

The team has seen that when information sharing is required across diverse parties, the simpler the exchange mechanism design, the more successful the sharing effort will be.

#### 6.1.2. SACM Implications

Review both the diversity of the different organizations that are sharing information within the SACM framework, and the types and volume of information that must be shared. Include only the information that is required to successfully implement the desired use cases. The modular organization of OVAL supports use of parts of OVAL for different use cases. This organizational structure allows for use of only the parts that are needed to support a use case and nothing more.

### 6.2. Collection and Evaluation Must Be De-coupled

#### 6.2.1. Lesson

As OVAL - and the security automation space in general - has evolved, it has become clear that the close coupling found in OVAL between the OVAL Object and OVAL State (i.e., what to collect and what the collected data is expected to look like) is an undesirable feature. By forcing these two concepts into a single model, the Language does not easily allow for easy extension, dynamic querying of previously collected data, or efficiencies in data collection and data exchanges.

#### 6.2.2. SACM Implications

Keep the mechanism by which data is collected and evaluated separate.

### 6.3. Keep Separate Core and Extensions

#### 6.3.1. Lesson

OVAL, by design, must be frequently updated to keep up with new and expanding sets of assessment platforms. However, tool vendors incurred great cost in updating to new versions of the Language, including implementing new tests in the updated version, as well as general quality testing, updating release and deployment, etc.

As the project matured, so too did the Core Models that define the building blocks for endpoint assessment. Over the past few years, the Core Models rarely changed-in some cases, going years without any required update. The Platform Extension Models, however, will always require a frequent revision cycle, and often were out of date very quickly. Despite the fact that these two models had distinct release cycle requirements, with one continually getting longer in the Core Models, and one requiring agility in the Platform Extensions, a full release of both was required to include changes to any part of the OVAL Language.

#### 6.3.2. SACM Implications

SACM should focus on providing the foundational building blocks that allow those that know how best to express what data must be collected to assess an endpoint. The SNMP standard [RFC1157] could be used as a model for this type of separation. SNMP defines the building blocks for sharing information about network devices, but defers the low-level details of this information sharing to those that best understand the products via Management Information Bases (MIBs). While this is not a perfectly analogous model for the SACM work, this clean separation of core building blocks and protocols from the low-level details of products should be emulated, if possible.

### 6.4. Empower Subject Matter Experts

#### 6.4.1. Lesson

As the security automation field has matured, more primary source vendors and other subject matter experts have taken increased responsibility in ownership of how their products are assessed. This step in maturity is critical and, within OVAL, as these vendors have become more involved, the quality in tests available to tools and end users has greatly increased.

#### 6.4.2. SACM Implications

Ensure that usage of SACM means that those that best understand the component being assessed are empowered to instruct what data must be collected for the assessment, along with the meaning of this data.

As much as possible, keep the mechanism by which this information is conveyed as simple as possible to ensure that it is as easy as possible for subject matter experts to participate.

## 6.5. Carrots Work Better than Sticks

### 6.5.1. Lesson

As much as possible, ensure that usage and compliance with the defined standards is encouraged by offering primary source vendors and subject matter experts incentive to do so. Forced compliance typically encourages organizations to do the least possible, and does not entice them to continually stay engaged.

### 6.5.2. SACM Implications

Find ways to encourage participation that drives long term engagement and willing participation. Engage with vendors to understand their problems and, where possible, construct SACM use cases and requirements that not only address the needs of the SACM end users, but also those of the vendors. Build a compelling story for use of SACM that not only shows value to end users, but shows a clear return on investment for vendors.

## 6.6. Use Caution Defining Data Collection

### 6.6.1. Lesson

When providing information about what data must be collected as part of an assessment, it can be quite easy to provide this information in a way that dictates how to collect the required data. Doing so can limit innovation and architectural choices for organizations implementing security automation tools.

On the other hand, it is not always feasible to express what data must be collected without implying or instructing specific data collection mechanisms. Over the years, there have been a few cases where the OVAL community could not agree on significant issues related to data collection. Discussions on whether to allow open scripting in the Language and how best to support both third party and primary source contributions were very challenging. With good arguments on both sides of these issues, it was difficult to achieve consensus.

### 6.6.2. SACM Implications

This will be one of the bigger challenges for SACM to navigate. SACM must allow those that best understand platforms and products to instruct what data must be collected for assessment. At the same time, third party support will be critical in some cases as well, and allowances must be made for this.

Additionally, deciding how many, if any, collection methods are allowed as part of the collection instructions will be challenging. Again, a balance should be struck to best allow clarity in data collection instructions, without limiting innovation and product-specific decisions.

## 6.7. Perspective Matters

### 6.7.1. Lesson

When evaluating collected posture attributes, it is important to be able to include additional context to this evaluation in some cases. For example, the method by which data was collected could be an important piece of information when performing evaluation. If the scanner was a remote, unauthorized scanner of an endpoint, it is entirely possible that the scanner could not properly scan for a number of posture attributes. If, however, the scanner ran locally on the endpoint as an administrative user, it is much more likely that it accurately collected posture attributes from the endpoint.

Other examples of this type of perspective and context include how old the collected data is, and whether the scanner was active or passive.

### 6.7.2. SACM Implications

Ensure information that provides necessary context can be provided as part of data collection, thereby allowing context-based decisions to be made.

## 6.8. Flexible Results Fidelity is Important

### 6.8.1. Lesson

After data collection and evaluation is complete, evaluation results must be shared, often with multiple parties, and in multiple ways. It is important to provide a reasonable amount of flexibility with respect to what levels of fidelity are allowed with evaluation results. While OVAL did try to achieve a reasonable amount of flexibility with evaluation results fidelity, challenges still exist.

#### 6.8.2. SACM Implications

As much as possible, allow the end users of evaluation results to determine exactly what level of fidelity they need to achieve their goals.

### 6.9. Evaluation Guidance is Platform-Specific

#### 6.9.1. Lesson

In the early days of OVAL, initial adoption of the effort was spearheaded by third party security vendors, as opposed to the primary source vendors for software. As the effort matured, more primary source vendors became involved and adopted OVAL in some way. It quickly became evident that, while third party vendors made great strides in determining how to evaluate the security posture of many platforms and products, understanding the best way to evaluate is hard, and very platform-specific. Additionally, OVAL content is costly to create, even for seasoned content authors, due to the need to understand these very low-level product and platform complexities.

#### 6.9.2. SACM Implications

As cited above, the primary source vendors are best suited to provide evaluation guidance. It is very challenging for third party organizations to truly understand platform-specific evaluation. Empower primary source vendors and other subject matter experts by providing simple and effective ways to provide this information. Also, as discussions on complex topics arise, engage these primary source vendors to understand their valuable views.

## 7. Recommendations

In order to successfully standardize the mechanisms by which endpoint posture assessment is performed, the following recommendations are offered to SACM for consideration.

### 7.1. Use the OVAL System Characteristics Model for Encoding Collection Data

The OVAL System Characteristics Model is used within the OVAL Language in order to encode the underlying data collected as part of endpoint posture assessment. Each of the posture attributes collected by an OVAL-enabled tool can be represented using the OVAL System Characteristics Model. As such, this model should be used to inform the development of a data model to encode collected posture attributes within SACM.

Within the OVAL System Characteristics Model, information such as metadata about the document (who/what created the document, creation timestamp, etc.), endpoint identification information (OS name, host name, and other asset-related information), and the foundational constructs to allow the encoding of posture attributes can be found. It is understood that modifications to the model will be required in order for it to fully implement all of the requirements for SACM. However, the use of this well-supported, standardized mechanism for encoding collected data is recommended as SACM begins moving from Information Model into Data Models and actual implementations.

The expectation is that SACM will need to make use of multiple types of standardized formats to encompass a complete solution for endpoint posture assessment. As such, the OVAL System Characteristics Model could be used to inform the development of a data model for encoding collected data from an endpoint.

### 7.2. Use the OVAL Definitions Model for Collection and Evaluation Guidance

Similar to the OVAL System Characteristics Model, the OVAL Definitions Model also has aspects that could be very useful in guiding the development of a data model to capture Collection Guidance. Collection Guidance is the mechanism by which a content author can dictate what rules should be used for collecting data from an endpoint. While the OVAL Definitions Model, as it is today, is used for guidance of both Collection and Evaluation, it is well suited to inform the development of a data model for Collection Guidance.

This model provides several key features that should be used as building blocks for this capability. For instance, within the OVAL Definitions Model, there is a series of structures that can serve as the base for instructing tools as to what data must be collected, including abstract structures for identifying required posture attributes, Variables, and Functions (which allow several types of data manipulation during collection). The model also supports a number of different data types, such as strings, Booleans, integers, records, and others.

While the recommendation is to make use of many of the structures found within the OVAL Definitions Model, it is equally important to note that the current approach for extending OVAL into various platforms is flawed, and should be fixed. Specifically, for every new check that is to be added to the Language, a new concrete test must be created. OVAL provides an abstract Test structure that must be extended to create checks (e.g., "registry_test," "file_test,"

"ldap_test," etc.). For SACM, it is imperative that a more scalable and flexible approach be implemented.

One aspect of SACM that has been discussed, but only partially worked into the Information Model at the time, is the concept of high-level, platform-agnostic configuration items and low-level platform-specific configuration items. In the discussed concept, the high-level items will capture the concepts of configuration that must be defined by those who write the guidance, while the low-level items will be provided by the appropriate vendors and/or subject matter experts to allow those that best know the platforms and products to instruct data collection. With this approach in place, some of the concepts defined within the OVAL Definitions Model (e.g., Objects, which instruct tools as to what data to collect) will need to be modified or removed to accommodate the shift in how posture attributes are defined for Collection. As such, the recommendation is to use many of the underlying structures in the OVAL Definitions Model, including the data types, Variables, Functions, etc., as a base from which to build a complete solution for fulfilling the SACM Information Model.

In addition to utility in supporting Collection Guidance, the same OVAL Definitions Model should also be used to inform the development of a data model for Evaluation Guidance. Again, with the current OVAL Language, Collection and Evaluation are wrapped together in the single model. The OVAL Definitions Model provides a series of structures that can be used to support Boolean logic statements, which could be useful for defining evaluation criteria and could be used as the basis for a further enhanced data model for Evaluation Guidance.

### 7.3. Do NOT Use the OVAL Results Model for Results Sharing

Despite the fact that the Results Model could be used to share the results of the evaluation part of an endpoint posture assessment, the recommendation is to not use this model to represent this information within SACM. The OVAL Results Model has, over the years, been a source of contention at times within the OVAL Community. Some feel like it provides too little information, while others believe that it offers too much. While there is some flexibility, in the form of OVAL Directives, in how much or how little information is included in the results, it really is not flexible enough to handle the broad set of requirements for SACM without extensive re-working.

Furthermore, SACM is working hard at separating data collection and evaluation, which makes the OVAL Results Model a poor fit, as it was constructed with a more combined Collection and Evaluation framework. It is expected that to properly model all of the results requirements within SACM, an alternative solution will be required.

While considering an alternative way to encode the results of an assessment, the following requirements have been stated by the OVAL Community as critical factors and should be considered in the development of a new data model for representing evaluation results:

- Allow evaluation results with appropriate granularity
- Ensure support for enterprise scale uses
- Provide results that include only the actionable information
- Ensure that data is clear and identifiable within the results
- Ensure interoperability

## 8. OVAL Submission

The OVAL submission to the IETF consists of seven Internet-Drafts (I-Ds) that define the six core data models and the processing model as described in Section 3.1. Each of the core data model I-Ds include the text from the OVAL Specification that defines the the specific data model as well as the corresponding XML Schema that implements it. The I-D for the processing model includes the text from the OVAL Specification that defines how each of the core data models work together. Given that the processing model describes how the core data models work together, there is no XML Schema associated with it.

The decision to split the OVAL Specification up into separate Internet-Drafts was made to encourage SACM to leverage the parts of OVAL that make the most sense and to emphasize that OVAL is not a monolithic data model but rather several distinct data models.

Moving forward, SACM should review each of the OVAL models, consider the recommendations in this document, and determine what concepts from OVAL make sense to build upon. From there, SACM should prioritize its data model efforts with respect to Collection Guidance, Evaluation Guidance, Posture Attributes, and Evaluation Results as well as determine how the data models should be implemented (e.g. JSON, XML, etc.). Lastly, SACM should begin development on its highest priority data model leveraging OVAL concepts where appropriate and making improvements and design decisions based on lessons learned.

## 9. Alignment with the SACM Vulnerability Assessment Scenario

The SACM Vulnerability Assessment Scenario [I-D.coffin-sacm-vuln-scenario] describes a concrete, operational vulnerability management scenario in an effort to break the SACM problem space into one of several more manageable pieces. Specifically, the scenario focuses on the following steps to determine which endpoints on an enterprise's network are in a vulnerable state:

1. Endpoint identification and initial (pre-assessment) data collection

2. Vulnerability description data

3. Endpoint applicability and secondary assessment

4. Assessment results

The OVAL submission provides concepts and lessons learned that will be valuable in developing the data models for Collection Guidance, Evaluation Guidance, Posture Attributes, and Evaluation Results which are necessary to support Steps 1, 2, and 4 of the scenario. However, OVAL does not provide any protocols or interfaces for communicating the configuration information that would be expressed using these data models. As a result, the Endpoint Compliance Profile [ECP] which provides an extensible framework for collecting, communicating, and evaluating endpoint information could be extended to support these data models as it was for software inventory information expressed using Software Identification tags [ISO.19770-2].

The following sections describe how the OVAL submission fits into each of these steps.

### 9.1. Endpoint Identification and Initial Data Collection

The first step of the SACM Vulnerability Assessment Scenario relies on the ongoing collection of basic information about an endpoint (e.g., type, criticality, hardware inventory, software inventory, configuration settings, etc.) to identify and characterize an endpoint. In order to do this, an Attribute Collector must first know what information to collect from an endpoint. This can either be hard-coded in an Attribute Collector or it can be driven by Collection Guidance with the latter being the more scalable approach. The OVAL submission, more specifically the Objects section of the OVAL Definitions Model, provides a data model for expressing what configuration information should be collected from an endpoint. This can be leveraged as a starting point for Collection Guidance that can

be modified to accommodate the lessons learned around empowering subject matter experts ( i.e. primary source vendors) to identify what configuration information should be collected on their platforms and not dictating how tools must collect this information off of an endpoint.

Once the configuration information has been collected from an endpoint, it needs to be expressed in a format that is consumable by other tools (i.e. Posture Attributes) for identification, correlation, and evaluation purposes. The OVAL submission includes the OVAL System Characteristics Model which can serve as a starting point for expressing this collected configuration information as Posture Attribute in a way that is scalable and enables subject matter experts to define it in a manner that makes sense to them.

### 9.2. Endpoint Applicability and Secondary Assessment

In this step, the Posture Attribute information collected, in Step 1, is evaluated to determine the applicability of vulnerability description data to an endpoint and to determine if an endpoint is in a vulnerable state. If additional information is required to make these determinations, it can be collected during this step of the scenario. The OVAL Submission aligns with this step in that it provides the concepts and lessons learned to drive the development of the Collection Guidance and Posture Attributes data models as described above. Furthermore, the OVAL Definitions Model and OVAL Processing Model, in the OVAL submission, provide a starting point for expressing the expected state of Posture Attribute information as well as defining the logical framework and algorithms necessary to compare the actual Posture Attribute information to the expected state defined in the Evaluation Guidance.

### 9.3. Assessment Results

Lastly, the OVAL submission aligns with the Assessment Results step of the scenario in that it identifies several problem areas that have impacted the usefulness of the OVAL Results Model which in turn led to several community-defined requirements for the next-generation assessment results data model. These shortcomings and requirements supplement the information needs defined in the scenario and should be significant in shaping the next-generation data model for assessment results.

## 10. Acknowledgements

The authors would like to thank Brant Cheikes (MITRE), Juan Gonzalez (DHS), Adam Montville (CIS), Charles Schmidt (MITRE), David

Waltermire (NIST), and Kim Watson (JHU APL) for reviewing this document and providing helpful feedback.

## 11. IANA Considerations

This memo includes no request to IANA.

## 12. Security Considerations

This memo documents, for informational purposes, the mapping between the OVAL Data Models and the SACM Information Model as well as the lessons learned from the past 10+ years of developing OVAL. As a result, there are no specific security considerations.

## 13. Change Log

### 13.1. -02 to -03

There are no textual changes associated with this revision. This revision simply reflects a resubmission of the document so that it remains in active status.

### 13.2. -01 to -02

Updated to reflect the latest changes to the SACM Information Model.

Added text that describes how the OVAL submission is expected to be used by the SACM WG.

Discusses how OVAL aligns with the SACM Vulnerability Assessment Scenario.

Updated references to documents on the MITRE OVAL website to the OVAL community documentation site on GitHub.io.

Added the OVAL Processing Model to the list of core models supported in OVAL.

### 13.3. -00 to -01

There are no textual changes associated with this revision. This revision simply reflects a resubmission of the document so that it goes back into active status. The document expired on November 6, 2015.

# 14. References

## 14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

## 14.2. Informative References

[I-D.coffin-sacm-vuln-scenario]
Coffin, C., Cheikes, B., Schmidt, C., Haynes, D., Fitzgerald-McKay, J., and D. Waltermire, "SACM Vulnerability Assessment Scenario", draft-coffin-sacm-vuln-scenario-01 (work in progress), January 2016.

[I-D.ietf-sacm-architecture]
Cam-Winget, N., Ford, B., Lorenzin, L., McDonald, I., and l. loxx@cisco.com, "Secure Automation and Continuous Monitoring (SACM) Architecture", 2015, <http://www.ietf.org/id/draft-ietf-sacm-architecture-03.txt>.

[I-D.ietf-sacm-requirements]
Cam-Winget, N. and L. Lorenzin, "Secure Automation and Continuous Monitoring (SACM) Requirements", 2015, <http://www.ietf.org/id/draft-ietf-sacm-requirements-04.txt>.

[ISO.19770-2]
"Information technology -- Software asset management -- Part 2: Software identification tag", ISO/IEC 19770-2, 2009.

[OVAL-DEFINITION-TUTORIAL]
United States Government, "The OVAL Definition Tutorial", 2015, <http://ovalproject.github.io/getting-started/tutorial/>.

[OVAL-DOCUMENTATION]
United States Government, "The OVAL Definition Tutorial", 2015, <http://ovalproject.github.io/>.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "A Simple Network Management Protocol (SNMP)", 1990, <https://www.ietf.org/rfc/rfc1157.txt>.

[SACM] The IETF SACM WG, "IETF Security Automation and Continuous Monitoring (sacm) Working Group Charter", 2015, <https://datatracker.ietf.org/wg/sacm/charter/>.

[SACM-DOCUMENTS] The IETF SACM WG, "IETF Security Automation and Continuous Monitoring (sacm) Working Group Documents", 2015, <https://datatracker.ietf.org/wg/sacm/documents/>.

[STRUCTURE-OF-OVAL] The MITRE Corporation, "Structure of the OVAL Language", 2015, <http://ovalproject.github.io/getting-started/best-practices/#2-structure-of-the-oval-language>.

## Authors' Addresses

Matthew Hansbury
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: mhansbury@mitre.org

Daniel Haynes
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
USA

Email: dhaynes@mitre.org

Juan Gonzalez
Department of Homeland Security
245 Murray Lane
Washington, DC 20548
USA

Email: juan.gonzalez@dhs.gov