

The MITRE Adoption Programs and the NIST SCAP Validation Program

Program Overviews and How the Programs Interrelate

Abstract

The MITRE Corporation moderates several information assurance data standards including CPE, CCE, OVAL, and CVE. As a part of its moderation role, MITRE runs adoption programs by which MITRE can both educate vendors about the standards and receive constructive technical feedback to evolve them. The National Institute of Standards and Technology has established the Security Content Automation Protocol (SCAP), which uses several MITRE moderated standards. The NIST SCAP Validation Program manages the formal testing of products to ensure proper implementation of the standards within products. The SCAP Validation program will test and validate a product's conformance to each individual standard moderated by MITRE independent of testing conformance to SCAP. The purpose of this document is to provide an overview of both programs and to describe how they interrelate to one another.

The MITRE Adoption Program and NIST SCAP Validation Program are independent but complementary efforts. This document defines common terms used in the MITRE Adoption Programs and NIST SCAP Validation Program and provides an overview to adopting organizations of the typical flow through the MITRE Adoption Programs and NIST SCAP Validation Program. Additionally, the roles and responsibilities of MITRE and NIST are defined.

Key Concepts of the MITRE Adoption Programs

Vendors may choose to participate in the MITRE Adoption Programs which are associated with the various MITRE moderated standards. The purpose of the Adoption Programs are to: a) Educate vendors on best practices regarding the use and implementation of the standards; b) Provide vendors with an opportunity to make formal self-assertions about how their products utilize the standards; and c) Allow MITRE to gain deeper insights into how the standards are, or could be, utilized so that the standards can be evolved. More information about the individual Adoption Programs can be found here:

- <http://cce.mitre.org/adoption/index.html>
- <http://cpe.mitre.org/adoption/index.html>
- <http://cve.mitre.org/adoption/index.html>
- <http://oval.mitre.org/adoption/index.html>

The following is a list of key concepts of the MITRE Adoption programs.

Moderator

The organization which moderates the community guidance process for the standard and who has editorial oversight of the dictionaries and schemas associated with the standard. Currently, the MITRE Corporation is the

moderator of CVE, CCE, CPE and OVAL, but this may change at some point in the future based on the guidance of the supporting communities and the strategic interests of MITRE's sponsors.

Declaration

The first phase of the MITRE Adoption Programs is where a vendor publicly registers their intent to support and incorporate the standard. A declaration does not involve any formalized testing of products, or any detailed, structured self-assertions regarding implementation. In no way does a declaration imply that the standard has been implemented yet, nor that it has been implemented correctly.

Questionnaire

The second phase of the MITRE Adoption Programs is where a vendor submits detailed answers to a structured questionnaire that describes how the product implements and uses the standard. A questionnaire does not involve any formal product testing. Completed questionnaires are posted on the MITRE web site associated with the appropriate standard. (Products containing capabilities that are testable by the NIST Validation Program will have their Questionnaires posted only after the product has successfully completed the appropriate NIST Validation.)

Technical Use Case

A Technical Use Case defines an intended "best-practice" usage of a standard. Technical Use Cases are defined and documented by each standard moderator based on the input and guidance of the standard's supporting community, which includes those vendors participating in the Adoption Program. Technical Use Cases are expected to evolve as individual standards evolve and mature based on the input and guidance of participants. A Technical Use Case may or may not be available for validation based on a number of factors. Those not available for validation are considered to be "emerging", meaning that their implementation and/or use within the industry are incomplete or limited. This in turn makes validation testing impractical or unnecessary. An emerging use case could become available for validation testing once the need and means to do so are identified.

Key Concepts of the NIST SCAP Validation Program

The NIST SCAP Validation Program operates as a part of the NIST Security Content Automation Protocol project with the purpose of validating products to ensure that they correctly implement and use the SCAP standards. More information about the NIST SCAP Validation Program is available here:

- <http://nvd.nist.gov/validation.cfm>

The following is a list of key concepts of the NIST SCAP Validation Program

Capability

A Capability is a set of functionalities within a product that are verified by the NIST SCAP Validation program. Capability should not be confused with "product category". For example, Vulnerability Scanning may be a Capability that is present in several different product categories. Where applicable and appropriate, capability definitions will be derived from Technical Use Cases, as documented by the MITRE Adoption Programs for each standard. There are two primary types of Capabilities: Tested and Untested. A Tested Capability is a Capability for which Requirements and Test Procedures have been defined. An Untested Capability may not have Requirements or Test Procedures. A Capability may be Untested for any number of reasons, but the most likely reason will be that the Capability is based on an emerging Technical Use Case for a standard. There are also Capabilities that may be Untested because testing them is cost prohibitive or not possible to due to other limitations.

Requirement

Each Capability is defined by a collection of Requirements. A Requirement represents a granular item that defines a piece of functionality or information that must be present and can be tested during Validation. Where applicable and appropriate, Requirement definitions will be derived from Technical Use Cases, as documented by the MITRE Adoption Programs for each standard.

Test Procedure

A single step to follow during Validation to verify that a given requirement has been followed. Each Requirement has one or more test procedures.

SCAP Validation Program vs. SCAP Validation

“SCAP Validation Program” is the name given to the overarching program that consists of separate validations for each effort. This overarching program allows for efficiency in supporting validations across numerous standards. “SCAP Validation” is one of several validations offered in the “SCAP Validation Program” and is comprised of multiple SCAP Capabilities. Other validations include CVE Validation, CCE Validation, CPE Validation, OVAL Validation, CVSS Validation, and XCCDF Validation. A product can receive one or more of these validations based on its functionality.

National Voluntary Laboratory Accreditation Program (NVLAP)

Laboratories participating in this program are authorized by NIST to perform conformance testing of products for the SCAP Validation Program. The laboratories send their conformance test reports to NIST for review and approval. More information on the NVLAP program and participating laboratories is available here:

<http://ts.nist.gov/Standards/Accreditation/index.cfm>

Summary Timeline of Key Concepts

MITRE Adoption Program

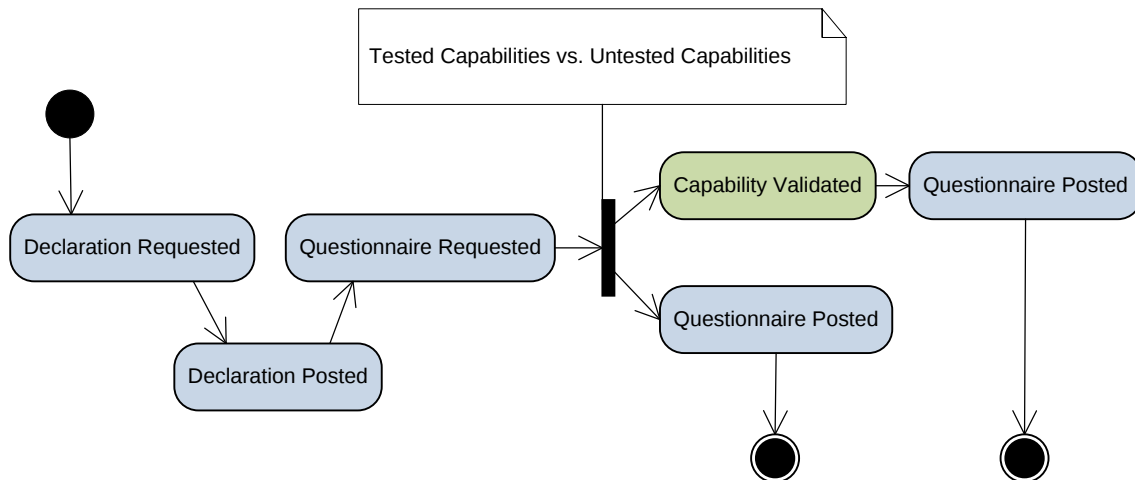
- Moderated consensus on standard definition and best practices
- Technical Use Cases documented

NIST SCAP Validation Program

- Testable Capabilities defined (based on Technical Use Cases)
- Requirements for testable Capabilities defined (based on Technical Use Cases)
- Test Procedures defined

Flow from an Adopting Organization’s Perspective

This section describes the typical flow through the MITRE Adoption Programs and NIST SCAP Validation Program for a vendor that is working to implement a standard and become Validated for doing so correctly. The diagram below depicts this flow:



Items in blue align with MITRE responsibilities. Items in green align with NIST responsibilities.

The process begins with an organization requesting a Declaration of Intent to support the standard. Once the Declaration of Intent is complete it is submitted to the standard moderator and posted for on the standard's web site. Next, the adopting organization requests a Questionnaire. Once the Questionnaire is completed the adopting organization submits it to the standard Moderator. Then, if the Capability being supported is a Tested Capability the organization is directed to the list of accredited labs for Validation. Once Validation is complete, the completed Questionnaire is posted on the standard's web site. If the Capability being implemented is an Untested Capability, the Questionnaire is immediately posted on the standard's web site.

The posting of the product's validation entry on the NIST SCAP Validation Program website marks a vendor's completion of the relevant validation activities. The posting of the Questionnaire marks a vendor's completion in the relevant MITRE Adoption Programs. Thus, vendors that choose to participate in both programs will start their standards adoption lifecycle by using the Adoption program. When they have a completed implementation they will participate in the Validation program. Finally, they will end their activities by posting the product Questionnaire on the Adoption program website.

MITRE and NIST Responsibilities

The responsibilities of each organization are detailed below.

MITRE

MITRE's role in the process is largely focused on advancing the standards, supporting organizations that are considering adopting a standard, and evolving the standards based on feedback from organizations that are looking to adopt or have already adopted the standards. The following list outlines the activities that MITRE is responsible for in the MITRE Adoption Programs and NIST SCAP Validation Program.

- Educate organizations about the Adoption and Validation Program
- Define intended Technical Use Cases for each standard
 - Define Technical Use Cases through collaboration with the standard's community and NIST.
 - Publish Technical Use Cases as a publicly available document on the standard's web site.
- Providing technical support related to adopting a standard
 - Help organizations understand and properly implement the standard.
 - Answer questions related to incorporating standards and how the standard relates to the organization's product.
 - Create tutorials about how the standards work
 - Evolve Technical Use Cases in light of new developments
- Encouraging organizations to participate in the Adoption and Validation Program
 - Promote and advertise the MITRE Adoption Programs and NIST SCAP Validation Program through:
 - conversations
 - discussion lists
 - booth interactions
 - face-to-face meetings
 - web site material
 - Seek out new organizations that would benefit from implementing capabilities based on the standards.
 - Educate organizations about the program and its benefits
 - Identify new Technical Use Cases for the standard through discussions and interactions with industry, academia and government
- Manage declarations of intent to use a standard
 - Develop declaration form
 - Distribute form to interested organizations
 - Collect completed forms
 - Follow up with declared products to ensure successful adoption
 - Identify whether declared capabilities will include Validation and appropriately educate the declarer of the path ahead
 - Promote declarations on web site
- Administer Questionnaires
 - Develop questionnaires
 - Work with organizations as they prepare for questionnaire
 - Answer questions about possible design decisions
 - Distribute questionnaire to interested organizations

- Collect completed questionnaires
 - Post completed questionnaires on web site
- Direct organizations to Validation Program once questionnaire has been submitted

NIST

NIST's role in the process is largely focused on the Validation Capabilities once an organization has completed implementing a Tested Capability. The following list outlines the activities that NIST is responsible for in the MITRE Adoption Programs and NIST SCAP Validation Program.

- Define Capabilities based on Technical Use Cases
- Define Requirements based on identified Capabilities
- Define Test Procedures based on Requirements
- Manage Labs
 - Work with NVLAP to accredit labs for SCAP testing
 - Provide accredited labs with detailed testing instructions
 - Verify that the labs are testing correctly
 - Provide technical support to the labs
 - about the testing process
 - questions that arise during testing
- Document the Validation procedure
 - A public document
 - To help guide organizations through the process
 - what is expected
 - how do organizations start testing
 - how do organizations complete testing
- Provide technical support related to the Validation process
 - Answer questions from organizations about the Validation process
- Review the results of Validation
 - Verify that the labs are testing correctly
 - Periodically review the testing process of each lab
- Award Validation upon successful completion of testing

Conclusion

The interactions between the MITRE Adoption Programs and NIST Validation Program described above are intended to clarify the relationships between these programs. This separation of responsibilities should support growth and maturation of the standards over time beyond what was previously possible while leveraging the strengths and aligning with missions of both MITRE and NIST.