# SCAP Vulnerability Management

First published in 2009, the Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the assessment of endpoints across multiple enterprise security use cases including:

* Configuration Management
* Software Asset Management
* Hardware Asset Management
* Vulnerability Management

SCAP does this by providing a common language with which to talk about different aspects of endpoint assessment including common identifiers for expressing vulnerabilities, platforms, and configuration items, a common format for expressing security configuration guidance, and a common language for expressing what information to collect from endpoints and how to assess it.

SCAP v2 aims to build on this foundation by integrating additional standardized data models, protocols, and interfaces to improve collection and assessment capabilities as well as improve interoperability among tools.

# What is Vulnerability Management?

SCAP defines vulnerability management as the process of: (1) retrieving vulnerability information applicable to the network; (2) determining if and where the vulnerability is present on the network, and; (3) applying a remedy that eliminates or mitigates the vulnerability.

Security advisories can be written using open, standardized formats that allow these advisories to be assessed using any SCAP-compliant tool. With these advisories, an SCAP tool can gather information from endpoints and compare it against these advisories using automated procedures. The result is a report of all endpoints that have vulnerable software present. Furthermore, applicable advisories can be selected in an automated fashion using the software inventory data collected from endpoints as described in the SCAP Software Asset Management use case.

A screenshot of a cell phone

Description automatically generated

Figure 1: Identifying Software and Security Advisories for Endpoints

# SCAP Workflow

The SCAP architecture employs three components, each supporting different aspects of assessment and data management. The first component is the Collection Manager which manages the collection of information from endpoints and stores that information in the Configuration Management Database (CMDB). The next component is the CMDB which stores and hosts endpoint information and assessment results for later use. Finally, there is the Evaluation Manager which assesses endpoint information against defined policy. Together, these components securely communicate information from the endpoint to the Evaluation Manager in support of the vulnerability management use case as shown below.

A screenshot of a computer

Description automatically generated

Figure 2: SCAP Vulnerability Management Workflow

# Benefits

Vulnerability management using SCAP provides a number of benefits over non-standards-based solutions.

* **Transparency of Operations:** See what information is collected from endpoints and how it is assessed
* **Standardized Data:** Collection results and evaluation results are represented using standardized formats
* **Interoperability Among Products:** Standardized formats, interfaces, and protocols enable interoperability and best-of-breed product selection

# Interested in Learning More or Getting Involved?

To learn more about SCAP, please visit the SCAP v2 website (<https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol-v2>). If you have any questions or comments, please send an email to [scap@nist.gov](mailto:scap@nist.gov).

To get involved in the development of SCAP, please join the SCAP Community (https://csrc.nist.gov/projects/security-content-automation-protocol-v2/scapv2-community) and share your thoughts.