SCAP Content Authoring Use Case Questions

Organization and Interviewee Name:

NIST, Dragos Prisaca

1. What type of SCAP content (vulnerability, specific compliance programs, OVAL, XCCDF, etc.) are you authoring and for what operating systems or applications?

☒	OVAL
☒	XCCDF
☒	Vulnerability Content (Specify Below)
☒	Compliance Program Content (Specify Below)
☒	Other (Specify Below)

Unit tests for the SCAP Validation Program. Unit tests for the previous versions of the specifications. The SCAP Validation Program covers major adopted operating systems: Microsoft, RHEL, Mac OS X. But, we are looking to add support for databases, network devices, containers, and virtualization.

2. Approximately how many SCAP Content authors are there in your organization?

#	OVAL
#	XCCDF
#	Authors create all types of SCAP content
#	Other (Specify Content Type Below)

One SME for the SCAP Validation Program.

3. What specific areas of content authoring are the most difficult for your authors?

☒	Getting content to run on multiple OVAL engines
☐	Writing XML that validates
☐	Learning what XML elements to populate
☐	It is difficult to know what OVAL schemas to use
☒	Other (Specify Below)

Getting consistent and reliable results using multiple tools across OSes and products; Challenges to interpret complex scan results. No easy way to unit test low level OVAL constructs.

SCAP Content Authoring Use Case Questions

4. What automation would assist you in the authoring of the content that you are developing?

☒	Automate creation of simple, common elements (registry key checks, etc.)
□	Support for macros that can be defined for common actions
☒	Support for automated filing and tracking of versions to simplify reuse
□	Example templates
☒	Support for managing complex structures
☒	The ability to compose and split source data stream collections
☒	Other (Specify Below)

Ability to create and test OVAL test types: for instance, create an OVAL registry_object, trigger only data collection for that object and present the collection in user friendly format.
Ability to create valid XCCDF and SCAP source data streams.

5. What customizations to existing SCAP content or 3rd party SCAP content do you perform?

The ability to tailor and customize SCAP content.

6. How do you store the content you create?

☒	Directories in a file system
□	Database
□	Content is loaded into scanning tools
□	GitHub/Other Source Control Mechanism (Specify Below)
□	Excel
□	Other (Specify Below)

IMO, the format to store and deliver SCAP content must be standardized. Storing the content in file format is good, but not optimal.

7. From which external SCAP sources do you collect content?

NIST NCP repository (USGCB, DISA, NSA etc.), CIS OVAL repository, RH repository.

8. What tools do you use to create SCAP content? What enhancements, if any, would you like to see with your current tools?

Oxygen XML Editor, Python scripts.

9. How willing would you be to change the tools that you are currently using if a general-purpose SCAP authoring solution was to be developed?

80% willing to change the current process as long the new tools will be supported for at least 5+ years (more the better). The major drawback of exiting SCAP authoring tools is the support to maintain and keep up with the new revisions of the specifications.

SCAP Content Authoring Use Case Questions

10. Are there any challenges your organization would face when adopting a new SCAP authoring solution?

☐	Programming language lock-in
☐	Operating System Lock-in
☐	Ongoing internal tool development
☐	Browser-based versus compiled code
☒	Other (Specify Below)

I don't see any challenges as long as the new tools fully implement the current specifications.

11. Would your organization be willing to provide occasional feedback during the development of an authoring solution?

Yes, I would love to be involved in this process.

12. Would your organization consider contributing software development resources toward the development of an SCAP authoring solution (architects, developers, beta testers)?

Possible.

Requirements

Please specify importance of the following high-level features and capabilities to your organization:

- Simplified SCAP content creation for authors with little-to-no SCAP knowledge.

☐ **Very important** ☐ **Somewhat important** ☒ **Not important**

Comments:

This is not currently important, but it will be helpful for new developers.

- Tooling that makes SCAP experts more efficient (facilitating content re-use, ID management, change tracking, etc.).

☒ **Very important** ☐ **Somewhat important** ☐ **Not important**

Comments:

Click or tap here to enter text.

SCAP Content Authoring Use Case Questions

- Automation-friendly tooling (APIs, code libraries, etc.) that provides a simple, stable mechanism for generating SCAP component elements (OVAL elements, XCCDF Benchmarks, etc.).

  ☒ Very important ☐ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

- Support for the latest SCAP component specification versions (OVAL, XCCDF, etc.).

  ☒ Very important ☐ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

- Support for legacy SCAP component specification versions more than a few years old.

  ☒ Very important ☐ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

- Creating individual OVAL Definitions and OVAL Definitions Files (no XCCDF Benchmark).

  ☐ Very important ☒ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

- Creating XCCDF Benchmarks using existing OVAL checks (no OVAL creation).

  ☐ Very important ☒ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

- Creating XCCDF Benchmarks and corresponding OVAL checks.

  ☐ Very important ☒ Somewhat important ☐ Not important

  Comments:

  Click or tap here to enter text.

SCAP Content Authoring Use Case Questions

Additional Capabilities

Which of the following capabilities would you be interested in seeing in a general-purpose SCAP authoring tool?

☒	The ability to specify common actions (e.g., "check registry key," "check file presence") and have the tool generate content without forcing the author to understand the underlying OVAL/XCCDF language structures.
☒	Support for version/revision control in your tools for content.
☐	The ability to define "macros" and "libraries" that can be saved to be used in future content.
☒	The ability to compose and split source data stream collections
☒	Difference tracking between content sources.
☐	Other (Specify Below)

Click or tap here to enter text.

Do you have any other comments or suggestions?

Couple of comments that I think are very important:
1. Standardization of the SCAP repository: storage, interfaces, version control, etc. Proof of concept, public repository, adoption, etc..
2. Fully support of each SCAP component specification
3. Maintenance and support. For how long will the SCAP authoring tools be maintained and supported?

Thank you for your time! We would like to host the responses on the SCAP Community GitHub site, which is open to the public. Do you have any issues with your responses becoming part of that public collection?

Interviewer:

Click or tap here to enter text.