***Organization and Interviewee Name:***

DISA – Joe Wolfkiel

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) |

Reused some OVAL content. Don’t write OVAL content. Write XCCDF benchmarks linked to CPE definitions.

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

|  |  |
| --- | --- |
| 0 | OVAL |
| 2 | XCCDF |
| # | Authors create all types of SCAP content |
| # | Other (Specify Content Type Below) |

Click or tap here to enter text.

1. 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) |

Complexity of writing an XCCDF benchmark.

1. 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) |

Click or tap here to enter text.

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

Editing benchmarks and creating new benchmarks by fusing existing OVAL checks together for things they want to track.

1. 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) |

Click or tap here to enter text.

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

McAfee, NVD

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

McAfee Policy Auditor content creator. The ability to bring back the minimum amount of data in the result set. If checking a patch, maybe just bring back name of the patch and if it passed or failed.

1. 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?

McAfee Policy Auditor, Tenable Nessus, and Tanium on every endpoint and separate content from each vendor bringing back different results at different time periods and is too much data. Would like to have one tool on an endpoint and have content that can be run.

1. 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) |

Vendor lock-in with custom content.

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

Happy to talk with the community, but, often contract content authoring out.

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

No, but, maybe beta testers.

**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:

Click or tap here to enter text.

* 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.

* 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.

**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?

Identifier management for control mappings.

**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:***

Danny Haynes, Joe Sain