***Organization and Interviewee Name:***

Kent Landfield - McAfee

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) |

Windows current, legacy, Linux (RH, others) AIX, Sun OS. Also do CIS documents. Content translated into multiple languages. Compliance templates.

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

|  |  |
| --- | --- |
| # | OVAL |
| # | XCCDF |
| ~8 | Authors create all types of SCAP content |
| # | Other (Specify Content Type Below) |

Fluctuates by project. Automated a great deal of this process. Windows, RH content is relatively easy to automate. Compliance required authors.

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) |

Dealing with XML in general. Instituted a great deal of automation. Created libraries of checks and for compliance. Anything that runs on the McAfee engine is compatible.

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) |

We created our own tool for creating SCAP content. Automate the creation of common elements… we support automatic filing and tracking. Support the use of content libraries. We build the ability to use multiple scripting languages into our content automation system.

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

Tailoring capabilities are available in the product. Can be our content or others. For the most part, McAfee doesn’t use external SCAP content. All internal components are done in house.

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) |

For development – done inside content management system. For runtime – database driven, loaded into the product. SCAP package set update 1300 released June 12.

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

None at this point.

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

In house developed tools, We developed the entire content management. We would like to see another checking language.

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?

Not interested. We will update our content management system as needed.

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) |

We are happy with our current content development environment.

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

Not certain at this point. Tools developer may be interested in the development process.

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

Possibly.

**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:

It is part of our product set.

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

**Very important  Somewhat important  Not important**

Comments:

Also part of our content management system.

* 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:

Done internally.

* 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:

Very important for our customers.

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

**Very important  Somewhat important  Not important**

Comments:

We do not use OVAL outside SCAP.

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

**Very important  Somewhat important  Not important**

Comments:

Already done in our content management system.

* Creating XCCDF Benchmarks and corresponding OVAL checks.

**Very important  Somewhat important  Not important**

Comments:

Already done in our content management system.

**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) |

Already done in our content management system.

Do you have any other comments or suggestions?

Advice: Develop an SCAP content management environment, not a general purpose SCAP authoring tool.

**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:***

Joe Sain