There were eleven responding organizations for this survey:

* Altex-Soft
* Borelli Security Software
* Canonical
* Center for Internet Security
* DISA FSO
* DISA
* NIST SCAP Validation (G2)
* Joval
* McAfee
* Red Hat
* Siemens

1. **What type of SCAP content are you authoring and for what operating systems or applications?**

|  |  |
| --- | --- |
| **OVAL** | **8** |
| **XCCDF** | **11** |
| **Vulnerability Content** | **8** |
| **Compliance Program Content** | **8** |

Operating systems supported started with Windows releases to various flavors of Linux, MacOS, AIX, Solaris, and Cisco IOS.

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

|  |  |
| --- | --- |
| **OVAL** | **2 to 3** |
| **XCCDF** | **2 to 4** |
| **Authors create all types of SCAP content** | **4 to 15 (avg: 9.5)** |

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

|  |  |
| --- | --- |
| **Getting content to run on multiple OVAL engines** | **5** |
| **Writing XML that validates** | **3** |
| **Learning what XML attributes to populate** | **4** |
| **It is difficult to know what OVAL schemas to use** | **3** |

**Other answers included:**

* OVAL is incredibly complex, doesn’t scale well, and is difficult to write
* XCCDF cannot be authored and maintained in an acceptable way without an authoring tool.
* Figuring out how to use OVAL tests and constructs accurately.
* Dealing with XML in general is difficult.
* New platform coverage in SCAP formats.
* Getting consistent and reliable results using multiple tools across OSes and products.

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

|  |  |
| --- | --- |
| **Automate creation of simple, common elements** | **6** |
| **Support for macros that can be defined for common actions** | **4** |
| **Support for automated filing and tracking of versions to simplify reuse** | **3** |
| **Example templates** | **3** |
| **Support for managing complex structures** | **6** |
| **The ability to compose and split source data stream collections** | **2** |

**Other answers included:**

* We developed our internal .net software for SCAP content creating.
* Assistance in the creation of new OVAL schema documentation and proposal to the OVAL community.
* Ability to wrap OVAL around something like a bash or PowerShell script.
* Ability to create and test OVAL test types.
* We created our own tool for creating SCAP content.
* A standard that is easier for people to pick up and use.

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

* We correct errors in CIS OVAL content.
* We built our tool from scratch as there was no good starting point.
* CIS is a content creator. Our authoring platform allows for the creation of CIS SCAP content and allows our SecureSuite members to tailor that content as well.
* None. DISA authors all of their content.
* Tailoring and customizing SCAP content.
* Editing benchmarks and creating new benchmarks by fusing existing OVAL checks together for things they want to track.
* We rewrite checks to improve them.
* 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.
* We base internal baselines on externally available SCAP content.

1. **How do you store the content you create?**

|  |  |
| --- | --- |
| **Directories in a file system** | **4** |
| **Database** | **6** |
| **Content is loaded into scanning tools** | **4** |
| **GitHub/other source control mechanism** | **4** |

**Other answers included:**

* We write directly to the DISA checklists but will probably back up a step to produce raw XCCDF output as well, to facilitate testing with NIST.
* Company Git Repos and servers.
* Will implement a GitHub-like solution soon.
* IMO, the format to store and deliver SCAP content must be standardized. Storing the content in file format is good, but not optimal.
* 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?**

|  |  |
| --- | --- |
| **CIS OVAL repository** | **5** |
| **Red Hat** | **2** |
| **Novell (SuSE)** | **1** |
| **NIST NCP** | **1** |
| **McAfee** | **1** |
| **IASE/DISA** | **2** |
| **Canonical** | **1** |

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

|  |  |
| --- | --- |
| **Manual Creation – Oxygen XML Editor/Scripts** | **3** |
| **Developed In-House Tool** | **5** |
| **Developed .NET application** | **2** |
| **McAfee Policy Editor Content Creator** | **1** |

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** | **1** |
| **Not Very Interested** | **2** |
| **It Depends** | **4** |
| **Willing** | **2** |
| **Very Willing** | **2** |

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

|  |  |
| --- | --- |
| **Programming Language Lock-in** | **4** |
| **Operating System Lock-in** | **1** |
| **Ongoing Tool Development** | **6** |
| **Browser-based vs. Compiled Code** | **1** |

**Other Answers included:**

* We would prefer the ability to use editor of choice on a Linux-based system.
* A new SCAP authoring solution would need to meet a very high threshold/standard in order to be adopted internally. We currently support multiple teams involved in both Benchmark and SCAP content creation.
* No serious challenges, provided that the tool fully implements the current specifications.
* Vendor lock-in with custom content.
* We would need confidence in the quality and completeness of the solution and/or ability to improve and extend it.

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

|  |  |
| --- | --- |
| **Yes** | **8** |
| **Possibly** | **1** |
| **Need More Info** | **1** |
| **Not Sure** | **1** |

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

|  |  |
| --- | --- |
| **Yes** | **2** |
| **Beta Testers** | **3** |
| **Possibly** | **4** |
| **Probably Not** | **1** |
| **Need More Info** | **1** |