February 6, 2019 SCAP Community Telecon

SCAP Content

Danny Haynes began the meeting by providing a recap of key ideas and discussion points from December 6, 2018 teleconference on SCAP Content. Key discussion points that he mentioned:

* There appears to be community interest in many of the new capabilities proposed in the US Government vision for SCAP v2. Among these are interest in event-driven reporting.
* Opinions are mixed among the community on whether SCAP Content is difficult to author and the impact that this has on overall content production. While everyone agreed that there are aspects of SCAP content that could be made easier, it remained unclear as to whether this should be a priority.
* It was noted that there are significant gaps in the coverage of existing SCAP content, and many felt that this was an important blocker to further adoption. Furthermore, even when content exists, it can be difficult to discover.

# Bill Munyan from CIS

Bill observed that currently SCAP Content is monolithic. For example, a Windows 10 benchmark has hundreds of recommendations. All of this ends up getting sent to each endpoint. This often includes the full XCCDF content, which includes tailoring structures and prose blocks that the endpoint has no need for. The result is a great deal of data movement, much of which is probably unnecessary.

Organization of content is not especially mature. There are some ways that repositories can readily be broken down (e.g., vulnerability vs. configuration checks), but that the built-in relationships that SCAP Content uses doesn't reflect the range of relationships users might be interested (such as by technology and platform families). Because content remains bundled in large blocks, it is challenging to download very specific content elements (such as for a single targeted CVE).

Some work proposed in SCAP v2 is also being worked in IETF SACM defines an architecture that tries to decouple functionality that is currently conflated in SCAP content. For example, OVAL combines collection and evaluation, and XCCDF combines machine instructions and prose descriptions. At a given point in processing, only one of those parts are really needed, but currently everything tends to be shipped to all parts of the process because it is hard to separate it. The proposed architectures, with separate roles would compliment (and require) similar separations of roles in content.

## Bill asked the audience what other benefits they saw in decoupling SCAP functions?

* Danny noted that for event driven collection one could move away from monolithic content.
* Dave Waltermire (NIST) observed that the SCAP v2 architecture would allow separation of SCAP Content without significant changes. One could send OVAL Objects to endpoints rather than the entire benchmark and then then evaluator could be given the OVAL States to guide evaluation. The XCCDF wouldn't be needed on the endpoint at all. He also felt that this separation simplifies the applications themselves – software could be written to only support a single role rather than needing to do everything. He also noted that separation of collection and evaluation allows greater flexibility in the architecture. For example, it could mean that different standards for collection (NEA, SNMP, NETCONF, Common Information Model, PowerShell, etc.) could all be used when most appropriate and the evaluator could be agnostic as to how the actual collection occurred.
* David Solin (Joval) noted that it is not strictly necessary to define an architecture in order to achieve this separation. One could achieve the benefits of separating content and only distributing what was necessary without first standardizing an architecture. Dave Waltermire agreed but noted that, without a standard, tool users would find it challenging if they wanted that separation, or if they wanted other features like event-based collection. Without a standard, tool customers would have no reliable way to request or evaluate tools against those criteria.
* Charles Schmidt (MITRE) asked if customers have made requests to any attendees requesting specific architectural features. Bill said his customers have not. However, they do often ask for content according to certain criteria. E.g., "Can we assess over CVE X", "Can we assess against CVE Y". They would like greater granularity, at least with regard to vulnerabilities. Dave Solin felt that most of his customers didn't care about architecture as long as they got the results. Jack Vander Poll (SPAWAR) agreed, noting that most users don't know the processes by which SCAP evaluations occur and thus wouldn't know how to break it down.

## Jack Vander Poll asked how many had customers doing SCAP vulnerability scanning

* Jack noted most of his customers focused on policy.
* Both Bill Munyan and David Solin noted that their customers did a lot of vulnerability scanning.

Martin Mathew (JPMC) noted that he was working on SCAP security baselines and that it was often hard to get a mapping to CVE. Dave Waltermire noted that most vulnerability content has direct references. Martin noted that he was mapping content from an internal ecosystem, which was where things got messy.

A representative from OSCIA asked if there were plans to establish a uniform way of delivering content, such as from the National Vulnerability Database (NVD). Dave Waltermire responded that there are several plans for CVE. One consists of working with the CVE community to enhance the information in CVE entries to make it more actionable. They also plan to switch to using SWID tags to identify software. Also, NVD plans to start using the IETF ROLIE standard for content distribution. Bill Munyan noted that a more atomic content structure could make the content more searchable and easier to identify, which would help make content more data-driven. Dave noted that ROLIE would support this.

Bill Munyan talked about how the decoupling of functions in the SCAP architecture would address information model needs. He noted there would still likely be value in data bundles, but that once an organization collected the bundles they could then decouple the pieces. He noted that there would need to be some mechanism for identification of all pieces – OVAL already includes unique identifiers in all its sub-pieces, but the same would need to be done for other content.

OSCIA asked about the level of effort needed to get content updated, asking if the new model would make this faster. Bill felt that this would depend on the repository. Dave Waltermire felt that having a more automated content management system would support improved updating. He noted that this is something ROLIE tries to address. He noted that proprietary solutions can also automate content distribution, but that this makes it harder if one is pulling from multiple sources.

Jack Vander Pol asked about the implication of content breakdown on digital signatures. He asked if the expectation would be that every atomic piece be signed, or just the bundle (in which case the signature would be invalidated as soon as the bundle was broken apart). Dave Waltermire suggested that the top-level bundle might be signed and validated on download. The downloading entity could then sign the sub-components it extracted from the bundle, if this was necessary to preserve a chain of custody. Dave also noted that, rather than full digital signatures on every piece, one could create a signed manifest of hashes, which would be more efficient.

A caller asked if SCAP might lead to issues when one travelled from one domain to another. For example, if one travelled from the US to Europe, would the difference context result in changes to acceptable policy. Dave Waltermire noted that that would be up to an organization's own management. He noted that enterprises get to manage what content their managed devices use and when. Charles added that SCAP does not impose any management decisions on devices/enterprises. The SCAP standards are a tool that those organizations can use in their own management decisions, but ultimately SCAP use is wholly at the discretion of enterprises.

Bill concluded with a list of future activities. He noted that the architecture needed to be solidified, that the components would need to be specified at a more granular level, and that interfaces would need to be defined. He noted some of this work is going on in IETF SACM and invited others to participate.

# David Ries – Joval

David introduced four issues that he wanted to discuss:

1. Increase content coverage
2. Increase schema/OS coverage
3. Add an applicability mechanism to OVAL (wonky)
4. Simplify SCAP formats to make them easier to learn, author, maintain, re-use, etc.

## Content Coverage

David observed that SCAP content has moderate coverage of OS vulnerability and configuration checking, but is generally weak with regard to application vulnerability scanning and compliance (PCI, HIPAA, etc.) checking. He felt that it was not hard to create content streams and that there were ways to work with vendors to increase the content they provide.

A representative from OpenSCAP felt that the chart David presented probably over-stated the coverage. He felt that there was a high barrier for entry as an SCAP content developer. He observed that many of the parties he works with are not looking to become long-term SCAP content creators, but just want to focus on creating content for a specific issue and then move on. While for those interested in long term content creation the ramp up time might not be significant overall, for those seeking to do something quick and simple on a one-time basis, the challenge is significant.

### Is the coverage gap in SCAP content a pressing need?

* The OpenSCAP representative felt that having more SCAP content would be helpful. These days, many people are seeking alternatives (such as Ansible) due to the complexity of writing SCAP. Dave Waltermire asked if it might be possible to bring those communities together. OpenSCAP noted that there are some efforts to build translators.
* David Kennel felt that expanding content would be helpful.
* The OSCIA representative noted that different organizations have different needs for content, but that it would be helpful to be able to get all of one's content from a single source or format. They noted that having to mash content from multiple sources is a headache and significant cost.

Dave Waltermire asked whether anyone was considering SCAP for SecDevOps. He noted that when building open source software, one often pulls in other libraries and sometimes those have vulnerabilities. He noted that people would want to track these vulnerabilities better, but that this represents a different kind of checking from traditional SCAP scanning. A party responded that they were asked about this question regularly and that some groups, such as OWASP, are looking into enhancing SecDevOps. Dave Waltermire noted that people had been asking him about it as well.

## Schema Coverage

David Ries noted that some SCAP content models such as OVAL cannot cover certain products until schemas have been developed. As such, addressing gaps in schema coverage would be a prerequisite for addressing gaps in content coverage.

### Do people have need for SCAP to be able to cover more platforms?

* Bill Munyan said yes.
* OSCIA suggested support for Azure and AWS as well as FedRamp.
* Thomas Harris felt that expanding support for network device coverage would be good.

Charles Schmidt noted that much of the need for platform specific schemas in OVAL is due to the fact that OVAL specifies both what one is asking and how the system is to be interrogated to determine the answer. He asked if it was better to focus on building more schemas to cover more topics, of if it would be better to try to abstract away the schema-specific elements of checking and try to develop a language that standardizes the question of "what" one was asking and then leave it to tool implementers to determine the how. OSCIA felt that this would move significant complexity on to the implementer, potentially to a prohibitive degree.

Michele asked if, for mobile, if one could think of platforms like services. For example, with regard to content provisioning, did the connection route through AT&T or through Verizon. David Waltermire felt that this was worth considering further.

## Separate OVAL Applicability Mechanism

David Ries noted that many OVAL checks contain significant logic just testing for the presence of a specific version of an application. A vulnerability check might be mostly about identifying a piece of software, and then maybe an additional check for settings. David noted that it should be possible to separate out the software applicability portion of a check from the rest of the check. He noted that, if one did this, and if one had an inventory of an endpoint, one could quickly determine which OVAL definitions were applicable and only collect necessary additional information if the endpoint was known to have applicable software. He noted this would also assist with some of the packaging issues Bill Munyan raised - since each check would be associated with specific software it would be much easier to index and query stores based on those criteria.

Hai Nguyen felt that this would be a good capability to add. Marek Haicman noted that, currently, CPE handles applicability and asked why this was not used? David Ries noted that CPE is used primarily in XCCDF and generally is just a pointer to OVAL checks. David Solin added that it would be best to take inventories first and then use that to filter applicable OVAL definitions.

## OVAL Complexity

David Ries noted that OVAL has a number of issues as a language. In particular, he noted that it is highly relational, text based, and very verbose. He also noted that OVAL is an assertion based language, which is not suited to conditional and looping logic, which many people want to use it for.

David proposed a script-based language be employed to simplify aspects of OVAL. He noted that the script code would not be directly interpreted (which people have security concerns about) but could simply be a short-hand that was converted to XML prior to interpretation. He felt that a code-oriented OVAL would be much easier to use. Dave Waltermire felt that the examples that David Ries provided were much easier to read than regular OVAL. DC Coleman agreed. Both noted that they had a coding background. OSCIA also felt that this was a good direction to move.

Danny Haynes asked if David Ries had seen InSpec, which is based on Ruby and is intended to provide a code-based checking language. David had not and agreed that this should be looked into.