Published on *OASIS* (https://www.oasis-open.org)

Call for Participation: Static Analysis Results Interchange Format (SARIF) TC

Submitted by censign on Fri, 2017-08-04 20:52
Type:
Call for Participation

A new OASIS technical committee is being formed. The Static Analysis Results Interchange Format (SARIF) Technical Committee (TC) has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in this proposal will constitute the TC's official charter. Submissions of technology for consideration by the TC, and the beginning of technical discussions, may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

(a) you must be an employee or designee of an OASIS member organization or an individual member of OASIS, and

(b) you must join the Technical Committee, which members may do by using the `Roster "join group: link on the TC's web page at [a].

To be considered a voting member at the first meeting:

(a) you must join the Technical Committee at least 7 days prior to the first meeting (on or before 31 August 2017; and

(b) you must attend the first meeting of the TC, at the time and date fixed below (06 September 2017).

Participants also may join the TC at a later time. OASIS and the TC welcomes all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.

----------?
[a] https://www.oasis-open.org/apps/org/workgroup/sarif/ [1]

[b] See http://www.oasis-open.org/join/ [2]

[c] http://www.oasis-open.org/committees/sarif/ [3]

?CALL FOR PARTICIPATION?
OASIS Static Analysis Results Interchange Format (SARIF) Technical Committee Charter

The charter for this TC is as follows.

Section 1: TC Charter

(1)(a) TC Name

The name of the TC shall be "Static Analysis Results Interchange Format (SARIF) TC."

(1)(b) Statement of purpose

The purpose of the TC is to define a standard output format for static analysis tools, which will be called the Static Analysis Results Interchange Format (SARIF).

A static analysis tool is a program that examines programming artifacts in order to detect problems, without executing the program. Software developers use a variety of static analysis tools to assess the quality of their programs. To form an overall picture of program quality, developers must often aggregate the results produced by all of these tools. This aggregation is more difficult if each tool produces output in a different format. A standard output format would make it feasible for developers and teams to view, understand, interact with, and manage the results produced by all the tools that they use.

The goals of the format are:

* Comprehensively capture the range of data produced by commonly used static analysis tools.

* Be a useful format for analysis tools to emit directly, and also an effective interchange format into which the output of any analysis tool can be converted.

* Be suitable for use in a variety of scenarios related to analysis result management, and be extensible for use in new scenarios.

* Reduce the cost and complexity of aggregating the results of various analysis tools into common workflows.

* Capture information that is useful for assessing a project's compliance with corporate policy or conformance to certification standards.

* Adopt a widely used serialization format that can be parsed by readily available tools.

* Represent analysis results for all kinds of programming artifacts, including source code and object code.

(1)(c) Scope of work

The scope of work of the TC is to produce a specification that defines the SARIF format.

Specifically, the SARIF specification will describe:

* Multiple "runs" of different analysis tools in a single log file.

* The analysis tool that performs each run, including:
* Tool name
* Tool version

* The invocation of the analysis tool, including:
* Command line
* Begin and end time

* The files that were analyzed, including:
* URI
* MIME type

* Nested files, such as files contained within a compressed archive such as a ZIP file.

* The analysis rules that were executed.

* Information about each analysis result that was produced, including:
* The location of the result.
* The rule that was violated.
* The severity of the violation.
* Execution paths through the code that are relevant to the result.
* Call stacks relative to the result.
* Possible fixes for the problem.

* Notifications produced by the analysis tool, including:
* Progress messages.
* Configuration information.

The following are not within the scope of work of the TC:

* The definition or implementation of any application programming interfaces (APIs) for accessing, manipulating, or managing the information contained in a SARIF file.

* The definition or implementation of any experiences for viewing or otherwise interacting with the information contained in a SARIF file.

(1)(d) Deliverables

The TC's primary deliverable is a specification that defines the SARIF format. Projected completion date is 9 months from the date of the first meeting of the TC.

The TC may also produce other such educational or explanatory non-normative materials as it judges useful to assist in adoption of the specification.

(1)(e)

IPR Mode

The TC will operate under the "RF on RAND Terms" IPR Mode.

(1)(f) Anticipated audience or users

The SARIF specification will be used by the following classes of users:

* Developers and others who use static analysis tools to measure, assess, and track the quality of their software products.

* The developers of static analysis tools, who will use it to enable their tools to produce output in the SARIF format.

* The developers of conversion tools, who will use it to write tools that convert the output of existing static analysis tools to the SARIF format.

* The developers of "result management systems" who will use it to enable their systems to consume the output from any tool that can produce the SARIF format. (A results management system consumes the output of analysis tools, and produces reports that allow teams to assess the quality of their software products and to track it over time.)

* The developers of Integrated Development Environments (IDEs), who will use it to provide experiences for viewing, interacting with, and managing the results from any analysis tool that produces results in the SARIF format.

(1)(g) Language

The TC shall conduct business in English.

Section 2: Additional Information

(2)(a) Identification of Similar Work

- SCARF (SWAMP Common Assessment Result Format): https://github.com/mirswamp/swamp-scarf-io/blob/master/docs/SCARF.pdf [4]

- Static Analysis Tool Exposition (SATE) output format: https://samate.nist.gov/SATE5.html [5]

The TC proposers are in discussions with the relevant parties to drive alignment between the various efforts through the work done by this Technical Committee.

(2)(b) First TC Meeting

Wednesday, September 06, 2017
09:00 - 11:00 U.S. Pacific time / 12:00 - 2:00 U.S. Eastern Time / 16:00 - 18:00 UTC
By telephone
Sponsored by Microsoft

(2)(c) Ongoing Meeting Schedule

We will conduct one 2-hour teleconference every other week for the first three months (to produce a Committee

Specification Draft). The first meeting in each month will focus on a portion of the spec comprising approximately one third of the entire spec. The second meeting in each month will focus on closing issues raised in the first meeting.

(2)(d) TC Proposers

* Michael Fanning - Microsoft - mikefan@microsoft.com [6]
* Laurence J. Golding - Microsoft - lgolding@microsoft.com [7]
* Luke Cartey - Semmle - luke@semmle.com [8]
* Yekaterina Tsipenyuk O'Neil - Hewlett Packard Enterprise - katrina@hpe.com [9]
* Chris Wysolpal - CA Technologies - cwysopal@Veracode.com [10]
* Kevin Greene - U.S. Department of Homeland Security - kevin.greene@hq.dhs.gov [11]

(2)(e) Primary Representatives' Support

* I, Steve W. Wierenga (steve.wierenga@hpe.com [12]), as HPE Primary Representative to OASIS, confirm our support for the SARIF Technical Committee proposed charter and the participation of our organization's co-proposer [Yekaterina Tsipenyuk O'Neil] as named above.

* I, Paul Lipton, paul.lipton@ca.com [13], as OASIS primary representative for CA Technologies, confirm our support for this charter and endorse our listed proposer above [Chris Wysopal] as named co-proposer.

* I, Oege de Moor (oege@semmle.com [14]), as Semmle Primary Representative to OASIS, confirm our support for the SARIF Technical Committee proposed charter and the participation of our organization's co-proposer as named above.

* I, Ram Jeyaraman (ram.jeyaraman@microsoft.com [15]), in my role as Microsoft?s Primary Representative to OASIS, approve the proposed SARIF Technical Committee charter, and endorse the participation of proposers from Microsoft as named above.

* Derek Nisco (derek.j.nisco@hq.dhs.gov [16]) - As the US DHS Primary Representative to OASIS, I confirm our support (with Kevin Greene participating) for the SARIF Technical Committee proposed charter and our intention to participate in the TC

(2)(f) TC Convener

Ram Jeyaraman - Microsoft - ramjay@microsoft.com [17]

(2)(g) OASIS Member Section

None. The TC does not intend to affiliate with any Member Section.

(2)(h) Anticipated Contributions

* Static Analysis Results Interchange Format, available at https://rawgit.com/lgolding/sarif-spec/master/Static%20Analysis%20Results%20Interchange%20Format%20(SARIF).html

(2)(i) FAQ Document

None at this time

(2)(j) Work Product Titles and Acronyms

* Static Analysis Results Interchange Format (SARIF)

Associated TC:
Static Analysis Results Interchange Format (SARIF)
Deadline:
Fri, 2017-08-04 - Wed, 2017-09-06

Links:
[1] https://www.oasis-open.org/apps/org/workgroup/sarif/
[2] http://www.oasis-open.org/join/
[3] http://www.oasis-open.org/committees/sarif/
[4] https://github.com/mirswamp/swamp-scarf-io/blob/master/docs/SCARF.pdf
[5] https://samate.nist.gov/SATE5.html
[6] mailto:mikefan@microsoft.com
[7] mailto:lgolding@microsoft.com
[8] mailto:luke@semmle.com
[9] mailto:katrina@hpe.com
[10] mailto:cwysopal@Veracode.com
[11] mailto:kevin.greene@hq.dhs.gov
[12] mailto:steve.wierenga@hpe.com
[13] mailto:paul.lipton@ca.com
[14] mailto:oege@semmle.com
[15] mailto:ram.jeyaraman@microsoft.com
[16] mailto:derek.j.nisco@hq.dhs.gov
[17] mailto:ramjay@microsoft.com