Industry leaders collaborate to define SARIF interoperability standard for detecting software defects and vulnerabilities

Common data format for static analysis tools is being advanced by CA Technologies, Cryptsoft, FireEye, GrammaTech, Hewlett Packard Enterprise (HPE), Micro Focus, Microsoft, New Context, Phantom, RIPS, SWAMP, Synopsys, U.S. DHS, U.S. NIST, and others.

12 October 2017 - Members of the OASIS nonprofit consortium are working together to define an international interoperability standard for static analysis. The goal is to make it easier for software developers to assess the quality and security of their programs by aggregating data from multiple tools.

The new OASIS Static Analysis Results Interchange Format (SARIF) Technical Committee brings together major software companies, cybersecurity providers, government, security orchestration specialists, programmers, and consultants to agree on a data format that will be parseable by tools across the industry.

"At a time when more corporate value and liability is being driven by software, organizations need new ways to efficiently improve the quality and security of their systems," said Chris Rommel, Executive Vice President of VDC Research. "With SARIF, they will be able to do just that and better leverage the combined, unique insights available from the range of static analysis solutions available today."

"SARIF represents a leap forward in the usability of static analysis tools," said David Keaton, co-chair of the OASIS SARIF Technical Committee. "Many organizations in the safety and security communities use several competing tools on their code. SARIF will allow them to combine and compare the results more easily to gain a sharper picture of the issues in their code that need to be addressed."

SARIF co-chair, Luke Cartey of Semmle, agreed, "With SARIF, engineering teams will have easy access to a broad range of potential defects and vulnerabilities in compliance with a range of privacy and accessibility standards. SARIF will support the development of products whose code spans languages and operating systems."

"I'm impressed by the traction we're already seeing for SARIF and by the companies driving this work," said Laurent Liscia, CEO and Executive Director of OASIS. "Clearly, people involved in static analysis appreciate the need for interoperability, and they are committed to making it happen with SARIF."

Participation in the SARIF Technical Committee is open to all through membership in OASIS. Providers of static analysis tools, developers of Integrated Development Environments (IDEs), conversion tool vendors, software developers, and others impacted by this work are invited to join the group.
Support for SARIF

GrammaTech VP of Engineering, Paul Anderson, said, "SARIF fills an important gap in software engineering tools. It enables the integration of static-analysis tool results in a plug-and-play manner into a highly-automated software development ecosystem. It has the potential to lower the cost of static-analysis tool adoption, which will benefit both tool vendors and tool users alike."

Micro Focus VP of Product Management, Jason Schmitt, said, "It is important that developers have static analysis solutions that are standardized and interoperable to not disrupt the software development lifecycle when using several tools. As an active participant in the SARIF Technical Committee, we are committed to helping to drive this standard for static analysis and determine a consistent data format for easily comparing and managing results."

Microsoft Principal Software Engineer Manager, Michael C. Fanning, said, "SARIF’s cost reductions speak to programming leads because they can't afford to short-change quality due to limited bandwidth or budgets. Advanced analysis techniques, such as machine learning, favor more inputs not fewer. And so there?is a clear need for a format like SARIF that reduces the cost of merging code quality data from many sources."

RIPS Technologies CEO, Johannes Dahse, said "Developers need a standard output format from static analysis tools in order to evaluate and compare different analysis results in the same way. That way they can learn and grow, and work together to build more secure applications. Moreover, a standard enables easy combination and integration of results from multiple tools. RIPS Technologies is proud to be part of the technical committee and is proud to help build the SARIF standard."

U.S. Department of Homeland Security Software Assurance Program Manager, Kevin E. Greene, said "DHS S&T is a huge supporter of SARIF because it builds upon our initial investments in technologies like Code Dx, Thread Fix, and Tool Output Integration Framework (TOIF), all designed to create workflows for developers to use multiple static analysis tools to increase the fidelity of results. SARIF is the realization that the sum of many is better than the sum of one."

More information

OASIS SARIF Technical Committee [1]

About OASIS

OASIS is a non-profit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for cybersecurity, privacy, cloud computing, IoT, SmartGrid, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users, and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 65+ countries. http://www.oasis-open.org

Media inquiries: communications@oasis-open.org; +1.941.284.0403

Links: