FOR IMMEDIATE RELEASE:
September 18, 2014

Editorial Contact:
Robin Lutchansky
Lutchansky Communications
(408) 607 7118
robinL@Lcomm.com

HOMELAND SECURITY-FUNDED SOFTWARE ASSURANCE MARKETPLACE (SWAMP) ANNOUNCES PARTNERSHIPS WITH COMMERCIAL VENDORS

Veracode, Parasoft, Red Lizard Software and GrammaTech Join Secure Decisions to Partner with the SWAMP to Improve Software Security and Continuous Software Assurance Practices

Madison, Wisconsin - September 18, 2014 – The SoftWare Assurance MarketPlace (SWAMP) announced today that it has formed partnerships with Veracode, Parasoft, Red Lizard and GrammaTech. They join existing partner Secure Decisions so that together, they can enhance the software security services offered by the SWAMP. Through these partnerships, the no-cost and open-source SWAMP facility will now offer an array of both commercial and open-source software security testing tools as well as an integrated commercial results viewer to significantly improve remediation of software flaws. Today's announcement broadens the SWAMP's capabilities, enabling the Department of Homeland Security Science and Technology Directorate (DHS S&T) funded facility to further advance the state of cybersecurity, better protect the nation's critical infrastructure and improve the resiliency of open-source software.

Designed to accelerate the adoption of continuous software assurance practices, the SWAMP facility addresses the growing realization of the power of using multiple tools to create a comprehensive view of an application's potential vulnerabilities. In fact, according to the latest National Institute of Standards and Technology (NIST) research report, tools mostly find different weaknesses, and over two-thirds of detected software defects can be discovered by only one tool. The report went on to explain that it was very rare for the same code defect to be detected by three or more tools. (Software Assurance Metrics and Tool Evaluation published in January of 2013) In addition, the National Security Agency (NSA) Center for Assured Software published a separate study of over 60,000 test cases with several million lines of source code (6.5 million+ for C/C++ and 3.2 million for Java) which showed that only 14 percent of the known software defects were able to be detected, even when using multiple tools.

-- MORE --

The four new commercial vendors will join Secure Decisions, a long-time SWAMP partner that already provides its software assurance analytics tool, Code Dx®, to SWAMP users. Since software security requires the use of multiple testing tools to conduct a comprehensive analysis of software vulnerabilities, and since there is a lack of standardized naming and security rating conventions between tools, managing the remediation process usually requires tedious hours of manual vulnerability data analysis. Code Dx automates this process by consolidating, normalizing, prioritizing and displaying weaknesses detected by disparate code analysis tools onto a central platform to ensure the most critical weaknesses are remediated quickly. By allowing SWAMP users to easily visualize and correlate the detected security weaknesses from ALL the tools used, developers can achieve acceptable software assurance levels more easily while injecting security best practices into the Software Development Life Cycle (SDLC).

"Software applications have become a core fabric to all aspects of our lives and are integral for the operation of our cars, home appliances, medical devices and, of course, our mobile devices. Software even powers the critical infrastructures that support our daily life support needs such as electricity and water," said Software Assurance Manager Kevin E. Greene of The Department of Homeland Security Science and Technology Directorate (DHS S&T). "The Department of Homeland Security funded the SWAMP because these software applications are quickly moving from behind the protection of corporate firewalls onto the web, making the need for improved software assurance capabilities more essential than ever to provide a first line of defense in protecting our nation's critical infrastructure and e-commerce environments."

As a result of these new partnerships, the SWAMP now offers powerful new capabilities:

- Veracode's cloud-based service provides SWAMP users with easy access to binary static analysis (SAST) with actionable guidance that helps developers quickly prioritize and remediate critical software vulnerabilities such as an SQL Injection or cross-site scripting (XSS) error.
- Red Lizard Software's Goanna software analysis tool performs whole program analysis on applications to detect hard-to-find C/C++ software flaws. Built using cutting-edge software assurance research coming from NICTA, Australia's Information Communications Technology (ICT) Research Centre of Excellence, Goanna also integrates with most IDE's and build systems to detect bugs early in the development cycle before they are released to customers.
- GrammaTech's static analysis tool, CodeSonar, helps developers eliminate the most costly and hard-to-find defects. Designed for zero-tolerance defect environments, CodeSonar's engine analyzes both source code and binaries. The binary analysis capability enables users to analyze software components even when source code is unavailable. CodeSonar's new distributed analyses capability, developed through DHS S&T funding, can efficiency run in large clusters of computers. As a result, Code Sonar's unique ability to exploit the power of distributed computing makes it particularly well-suited to the SWAMP's high throughput computing environment.
- Parasoft's Static Analysis Engine (SAE) for Java and C/C++ will help SWAMP developers prevent defects by unobtrusively applying thousands of rules based on academic research, industry standards, and proven best practices. As part of Parasoft's Development Testing Platform family of software quality solutions, SAE enables developers and testers to identify vulnerabilities at the earliest possible stage of the SDLC and eliminate them while the costs of remediation are at their lowest.

The new tools testing capabilities complement the seven open-source static analysis tools already being used by SWAMP users. These tools include FindBugs, PMD, Cppcheck, Clang and Clang Static Analyzer, GCC, Google's error-prone and Checkstyle. With the addition of the open-source tool Pylint and the full

implementation of these commercial tools, SWAMP will soon be able to offer users access to 12 software analysis tools. The SWAMP currently assesses programs written in the Java and C/C++ programming languages and PHP, C# and Python language support are being added to the SWAMP's capabilities as well. Currently, nine Unix/Linux-based platforms are supported in the SWAMP. Android platform support will be added shortly with Macintosh and Windows support to follow. In addition, dynamic and mobile testing support will also be added to the SWAMP's capabilities within the next year. The number of supported programming languages, platforms and software analysis tools will continue to grow in the future.

Hosted at the Morgridge Institute for Research in Madison, Wisconsin, the SWAMP is run by the Morgridge Institute for Research and three academic institutions with a team that offers deep expertise within software assurance, security, open-source software development, national distributed facilities and identity management. A state-of-the-art, secure facility with 700 cores, 5 TB of RAM, and 100 TB of HDD, the SWAMP uses advanced networking capabilities to meet the continuous assurance needs of multiple software and tool development projects.

The SWAMP is also promoting the adoption of continuous assurance practices from multiple angles by offering its infrastructure to tool developers to enhance and create better tools capable of finding a greater quantity and variety of software weaknesses. An absolutely critical need to improve the state of software assurance as a whole, the SWAMP facility provides an ideal resource for tool developers to test their tools by hosting almost 400 publicly available software packages including the NIST Juliet Testing Suite. Additionally, the SWAMP's intuitive user interface and its support staff ensure that tool developers are able to work effectively and attain useful results by testing against the documented vulnerabilities in these applications.

"We are actively working with interested developers to bring their own tools into the SWAMP so they can leverage SWAMP's capabilities to advance their tool's capabilities," said Miron Livny, Chief Technology Officer of the Morgridge Institute for Research and lead principal investigator of the SWAMP. "SWAMP is now more powerful than ever as a result of these new partnerships and provides even easier access to the diverse collection of software analysis technologies needed to obtain a truly comprehensive view of an application's vulnerabilities. This makes it easier to adopt the continuous software assurance practices needed to match the new world of continuous software development."

ABOUT THE SWAMP

The SWAMP, (**S**oft**W**are **A**ssurance **M**arket**P**lace) is a Department of Homeland Security funded facility designed to reduce the cost and complexity challenges of software assurance testing. SWAMP consists of a no-cost security testing platform that offers high throughput computing services combined with a comprehensive array of software security testing tools. The SWAMP also includes a broad library of open-source code samples with known weaknesses to help developers improve the quality of their static and dynamic testing tools. All SWAMP activities performed by users will be kept confidential although sharing is encouraged to create a collaborative platform for innovation. The SWAMP was funded to advance cybersecurity, protect critical infrastructures and improve the reliability of the open-source software used extensively throughout the software community. SWAMP is a joint project run by the Morgridge Institute for Research in Madison, Wisconsin; Indiana University; the University of Illinois at Urbana-Champaign; and the University of Wisconsin-Madison. For more information, please contact the SWAMP at www.continuousassurance.org.

###

SWAMP PARTNER QUOTES

‘“Web applications are the number one attack vector for organizations worldwide. As a result, all code needs security auditing, whether it is developed internally or comes from third-party and open source developers,” said Chris Wysopal, co-founder and CTO, **Veracode**. “By making static analysis more accessible via a cloud-based platform, the SWAMP program is helping to reduce unnecessary risk at government agencies and protecting our critical infrastructure.”

“I'm very excited to be working with the Software Assurance Marketplace (SWAMP). Software security plays a critical role in almost every aspect of our daily lives today, and all too often, it's found wanting, as witnessed by the unending stream of security breaches in the news,” said **Parasoft** evangelist Arthur Hicken. “Software security is hard, from figuring out which tool(s) to use, to installing them, keeping them up-to-date, the configuring, and workflow. It's time-consuming and expensive. The SWAMP allows everyone to simply submit their code and get back great static analysis results combined from a variety of tools. It's fast, easy, and the price is right. Why wouldn't you use it?”

"**GrammaTech** is proud that SWAMP is using CodeSonar to analyse source code and binaries. SWAMP combines deep security expertise, state-of-the-art software-assurance tools, and, more importantly, a vision of how to make it easier for organizations to benefit from software-assurance technologies,” said Dr. Paul Anderson, Vice President of Engineering at GrammaTech “As a result, SWAMP is positioned particularly well to address the growing software-security challenge."

“We have been strong supporters of and actively involved with SWAMP from the start. It's right in line with our own philosophy of combining different application security testing tools to gain greater vulnerability coverage while making it easier to interpret and prioritize the results," said Anita D'Amico, Director of **Secure Decisions**, the developer of Code Dx®. “We’re pleased to provide SWAMP users with our Code Dx viewer so they can consolidate, visualize and prioritize the testing results produced from multiple tools. Seeing the results of multiple tools in a unified display makes it that much easier for today’s organizations to adopt SWAMP’s SwA best practices.”

"We are delighted to support the SWAMP security initiative by sharing our Goanna analysis capabilities, especially with the open source community and the educational sector, to harden next generation software," said Ralf Huuck, **Red Lizard Software** founder.’