SWAMP
SOFTWARE ASSURANCE MARKETPLACE

December 12
2013

WP001

SWAMP Capabilities

This document defines the SWAMP, its target audience, the initial capabilities, and privacy and security.

Citation Information

MLA

"SWAMP Capabilities." *Continuous Software Assurance Marketplace*, 12 Dec. 2013. Web. <https://www.swampinabox.org/doc/SWAMP-WP001-Capabilities.pdf>.

APA

(2013, December 12). SWAMP Capabilities [PDF file]. *Continuous Software Assurance Marketplace*. Retrieved from https://www.swampinabox.org/doc/SWAMP-WP001-Capabilities.pdf

330 N. Orchard Street
Madison, WI 53715

(608) 316 - 4266

https://continuousassurance.org/
https://www.mir-swamp.org/#

What is the SWAMP?

The Software Assurance Marketplace (SWAMP) is a no-cost, national resource for continuous software assurance technologies (CSwA), available for use by research institutions, government and civilian agencies and their communities. Our initial operating capabilities, slated for January 2014, will include the following core services: simultaneous software package testing against 5 static analysis tools, assurance tool testing against 100 software packages, and an integrated weaknesses results viewer that features sorting, filtering and merging capabilities. SWAMP users can choose from eight different OS platforms and schedule assessments for continuous or one-off testing, all in a secure, access-controlled environment.

It is our hope that widespread adoption of SWAMP services will lead to a more secure and safer software ecosystem. We aim to facilitate enhancements in software engineering methodologies and SwA tool development. To this purpose, we will continue to enhance SWAMP's assessment and reporting services, add capabilities and provide technical support to our user communities during our five-year project and beyond. **Learn more about our project timeline.**

Who will use the SWAMP?

We've identified five distinct user groups that will benefit from SWAMP's services, including software developers, SwA tool developers, SwA tool researchers, infrastructure operators and educators/students. The design and implementation of the SWAMP will facilitate sharing within these five target groups.

Software developers will find SWAMP's continuous assurance services to be a valuable resource in the development lifecycle, whether they're assessing individual sprints or entire applications. Instead of running individual assessments in multiple venues, developers can run tools simultaneously, resulting in greater efficiency and time savings. The reporting mechanism—powered by Secure Decisions' CodeDX platform—offers an improved vulnerability results viewer. Armed with these reports, developers have an opportunity to identify, prioritize and remediate exploitable weaknesses such as injections, buffer handling, and web deceptions, to name a few.

Tool developers and researchers who aim to improve the quality of SwA tools can use the SWAMP to test their own suites, use those provided by NIST's SAMATE or SATE, or by the SWAMP community. We hope that the test results will lead to iterative improvement of tools that may, in turn, be added to the SWAMP tool repository for use by the broader community. Indeed, our essential service offerings are predicated upon the concepts of universal access, sharing and collaboration.

Our other user groups, including the infrastructure operators, educators and students, can use SWAMP as an essential, evaluative tool to identity exploitable weaknesses in software. For security and IT professionals, this may provide another "line of defense" against malicious or unintentional system attacks when deploying in enterprise environments, an increasingly important step as organizations incorporate open source software and bring-your-own devices into systems.

We are particularly passionate about availing SWAMP services to educators, researchers and students, whose incorporation of continuous assurance best practices and training has the ability to positively impact the safety of our software ecosystem. **To learn more, visit our website.**

What are the SWAMP Capabilities?

The SWAMP is a state-of-the art research facility that has robust operating capabilities. At launch, we will be able to analyze over 275 millions lines of code each day, with infrastructure designed to scale this capacity as demand is generated through the addition of CPU cores and storage capacity. Here is a snapshot of our capacity:

Platforms:

- Debian 7.0 64-bit
- Fedora 18.0 64-bit
- Fedora 19.0 64-bit
- RHEL 6.4 32-bit
- RHEL 6.4 64-bit
- Scientific Linux 5.9 64-bit
- Scientific Linux 6.4 64-bit
- Ubuntu 12.04.2 64-bit
- Windows 7 SP1 64-bit

Tools:

- Findbugs
- Cppcheck
- Clang and Static Analyzer
- GCC
- PMD

Software Packages:

- Asterisk
- Audacity
- VLC
- JSP Wiki
- Broadleaf commerce
- HT Condor
- Hadoop
- Open MPI
- omniORB
- Apache httpd
- dovecot
- database servers
- MySQL
- Pro
- Suricata
- Wireshark
- Lua
- Clojure
- JUnit
- uncrustify
- R
- Blast+
- Apache Camel
- Scribe
- Sling
- webgoat

Hardware Infrastructure:

- Intel Xeon Processors
- 700 cores
- 5 TB of RAM
- 104 TB of HDD space
- 12 teraFLOPS (12 trillion floating-point operations per second)

Privacy and security of the SWAMP

We respect your privacy and the confidentiality of your SWAMP activities. To this end, we're designing a secure system where you are in control of who sees your assessment results. If you are working on an open source project and wish to share your tool or software assessment results, mark your project "public" when you create it. As much as possible, we encourage sharing results as a means to improving and innovating software assurance activities and tools. Alternatively, you can conduct private assessments in the SWAMP by selecting "private." We do not share your results or your personal data with anyone. Our use of SWAMP user data extends only to depersonalized, metadata reporting so that we can assess the effectiveness of existing tools and better plan our own development path.

Security is our primary concern, which is why we're exceeding best practice security measures. Our Chief Security Officer, Von Welch of Indiana University, states, "we are putting together a complete SWAMP cybersecurity program, starting with a risk assessment and culminating with both typical controls (e.g. physical controls, encrypted access, audits, firewalls, intrusion detection) and features specific to the SWAMP role as a flagship software assurance facility." **Learn more about our team who is designing the SWAMP and its security protocols.**

Get Involved

The SWAMP team invites tool and software developers who are interested in improving our nation's cybersecurity to get involved. Became a beta tester or first user of the SWAMP.

We believe that community participation is critical to our mission. Won't you join us?

330 N Orchard St
Madison, WI
608-316-4266