SWAMP FAQ

What is the SWAMP?

The Software Assurance Marketplace (SWAMP) is an open facility that is designed, built, and operated by four research institutions. The SWAMP provides no-cost access to an array of open-source and commercial software analysis tools. The SWAMP also includes a (growing) library of open-source applications with known vulnerabilities to help tool developers improve the effectiveness of their static and dynamic analysis tools. One of the main goals of the SWAMP is to provide an open marketplace of software packages and analysis tools, with the ability to control how packages, tools, and expertise are shared with the entire software community. With the computing capacity required to support continuous assurance, the SWAMP provides the automation to continuously run multiple analysis tools against software packages. Results are viewable in an integrated results viewer that offers the developer the capability to view weakness reports with integrated CWE (common weakness enumeration) data from multiple tools.

All SWAMP activities performed by users are confidential. Users have the option to share software packages and assessment results with other SWAMP users and can choose to form groups through a project.

The ultimate goal of the SWAMP is to promote continuous assurance technologies and practices through an open and collaborative framework that protects confidential data and facilitates sharing, thus, making it easier for software developers to adopt continuous assurance practices.

Who owns the SWAMP?

The SWAMP (Software Assurance Marketplace) is hosted at the Morgridge Institute for Research, a private, not-for-profit research institute located on the University of Wisconsin-Madison campus. Collaborating partners include, the University of Wisconsin-Madison's Middleware Security and Testing Team, the University of Illinois at Urbana-Champaign's National Center for Supercomputing Applications, and Indiana University's Center for Applied Cybersecurity Research. The Morgridge Institute for Research owns all data in the SWAMP. Morgridge is committed to keeping the confidentiality of all SWAMP data. The SWAMP is funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS-S&T) to advance our nation's cybersecurity, protect our critical infrastructure, and improve the reliability of the open-source software used extensively throughout the software community. **DHS-S&T has explicitly disowned any rights to access or own data in the SWAMP.** The SWAMP Privacy Policy is available at https://www.swampinabox.org/doc/SWAMP-Privacy-Policy.pdf.

SWAMP FAQ

What is SWAMP-in-a-Box (SiB)?

The Software Assurance Marketplace (SWAMP) provides continuous software assurance capabilities to developers and researchers. For users that need or prefer to run software assurance tools on their own computing infrastructure, the SWAMP offers a standalone software application called “SWAMP-in-a-Box” (SiB). The SiB package can be deployed on your own servers if you have higher security or compliance requirements for your software, or, being open-source, when you want to customize the software. SWAMP-in-a-Box is available as an open beta, downloadable from GitHub at https://github.com/mirswamp/deployment.

Can SWAMP-in-a-Box (SiB) operate without internet access or a network connection?

Yes, SWAMP-in-a-Box can be configured to run assessments without needing access to the internet or an external network connection. This requires software packages to build without access to the internet and to not have OS packages dependencies. After downloading SiB, its dependencies must also be installed. See the SWAMP-in-a-Box Administrator Manual (https://platform.swampinabox.org/siab-latest-release/administrator_manual.html) for the necessary configuration and a detailed list of dependencies. Alternate versions of tools that use a fixed snapshot of vulnerability data will also need to be installed.

How does SWAMP fit into my current development process?

The SWAMP offers several plug-ins for Eclipse, Git and Subversion, and Jenkins to integrate into your software development lifecycle and to support continuous integration. These plug-ins allow assessments with any of the tools supported by the SWAMP. Results can be viewed directly in the SWAMP, or for Eclipse and Jenkins, directly within the product. Each plug-in requires a valid SWAMP account. Visit https://github.com/mirswamp for more information.

How does the SWAMP compare to other services like Fortify?

The SWAMP facility is unique in offering access to multiple tools, automation, and computing capacity needed to support continuous assurance and an integrated viewer for assessment results from multiple tools. Unlike other similar offerings of no-cost software assessment services by commercial entities, the SWAMP is designed, built, and operated by a partnership of four not-for-profit research institutions that have a long, demonstrated commitment to open source, cybersecurity, and software assessment and are driven by an underpinning vision of an open software assurance framework that facilitates easy adoption of new software analysis technologies.

SWAMP FAQ

What kind of static analysis code tools can be used in the SWAMP?

The current list of open-source and commercial static analysis tools offered by the SWAMP can be found at https://www.mir-swamp.org/#tools/public. Several commercial tool vendors have also partnered with the SWAMP to support a "bring your own license" model for their tools to work with SWAMP-in-a-Box. The SWAMP will continue to add support for additional open-source and commercial tools throughout the life of the project. The SWAMP welcomes input from users on software analysis tools they would like to see in the SWAMP. Input, comments, or suggestions can be made at support@continuousassurance.org.

Can I bring my own tool into the SWAMP?

If you would like to use or offer your own software analysis tool in the SWAMP, contact us at support@continuousassurance.org. We are happy to work with you to integrate your tools.

Any tool uploaded to the SWAMP is assumed to be private unless you decide to release it to the public.

Note that before a tool can be integrated, the SWAMP must support the platform (OS) required for your analysis tool and the programming language that your tool can analyze. Both of these potential limiting factors can be addressed and resolved in a timely manner within reason.

How do I access commercial tools in the SWAMP?

If you would like access to a commercial tool supported in the SWAMP, you must first request permission. Log in to your SWAMP account, and click on your SWAMP username at the top of the page to go to your account. Select the Permissions tab. For each commercial tool you would like to use in the SWAMP, select the Request button, and then fill out and submit the form. A member of the SWAMP team will follow-up with the commercial tool vendor for authorization, and the vendor may reach out to you directly. Once authorization has been received from the tool vendor, your access will be granted to use that commercial tool in the SWAMP.

To add-on and access commercial tools with SWAMP-in-a-Box, review the SWAMP-in-a-Box Administrator Manual at https://platform.swampinabox.org/siab-latest-release/administrator_manual.html.

SWAMP FAQ

Which programming languages and operating systems (OS) are supported?

The current list of programming languages supported by the SWAMP can be found at https://www.mir-swamp.org/. Supported platforms/operating systems (OS) can be found at https://www.mir-swamp.org/#platforms/public. The SWAMP will continue to add support for additional programming languages and platforms throughout the life of the project. The SWAMP welcomes input from users on programming languages and platforms they would like to see in the SWAMP. Submit suggestions to support@continuousassurance.org.

Does the SWAMP support RHEL as a platform?

RHEL 6 and 7 are supported and tested as a host OS to run SWAMP-in-a-Box. Due to licensing and distribution, we do not provide a RHEL image to run assessments within the SWAMP or SWAMP-in-a-Box. CentOS is derived from RHEL with only small differences. CentOS contains the same development tools, libraries, and software as RHEL and can be used as a substitute.

Can anyone get an account?

Yes, anyone can gain access to the SWAMP or SWAMP-in-a-Box. The SWAMP (https://www.mir-swamp.org/) supports verification through GitHub, Google, and university accounts affiliated with CI Logon, as well as the ability to create an account with SWAMP.

Are the uploaded projects and tools available to the public, or do I have an option to set them private?

Any project, as in software package, uploaded to the SWAMP is assumed to be private unless explicitly shared with other SWAMP users. Users control access to their software packages and assessment results by controlling which Projects can access the software or results. Project owners control membership in their projects. To make a software package or tool public, contact support@continuousassurance.org. The owner can change sharing options at any time.

What is continuous software assurance?

Continuous software assurance is the automated, repeated assessment of software by software assurance tools. The goal is to ensure that applications are assessed for weaknesses any time that code changes are made, throughout the software development life cycle. This ensures that new weaknesses introduced as code is added or updated can be remediated during more cost-effective development and testing phases, not after software is released. “Do it early. Do it often.”