Infrastructure operators can use the SWAMP as a factor in determining the risk in using the software by using the SWAMP's software assurance (SwA) tool results to determine the software's security and quality. The SWAMP's SwA results can also be used to provide metrics to encourage software suppliers to improve the quality and security of their software.

- **Reduce cost of acquiring quality software.** A large human cost in using SwA tools is the effort required to select, acquire, install, configure, maintain, and run these tools on software the infrastructure operator wishes to deploy. The SWAMP manages most of these tasks and makes it possible for infrastructure operators to view SwA tool results from external entities who have imported software into the SWAMP for assessment. Since the costs of performing SwA in the SWAMP are lower, the return on investment is increased. As new SwA tools and capabilities are added, the infrastructure operator automatically benefits.

- **Leverage community input to improve software quality.** Commonly deployed software can be assessed by the software developer or user community. For open source packages maintained as a SWAMP software package, the community can view assessment results and provide feedback that can encourage software providers to improve in the area of quality and security.

- **Improve visibility to changes in deployed software.** Continuous Software Assurance (CSwA) is the automated, repeated assessment of software by software assurance tools. As new SwA tools are added to the SWAMP, deployed software will be analyzed with improved rigor, identifying potential problems that need to be addressed by the software provider. As new versions of software are released, SWAMP analysis will quickly identify changes in deployed software that will better inform infrastructure operators of key features of interest that may impact their organization.

SWAMP Software Developer Use Case Diagram

Support for the Infrastructure Operator at IOC

We expect infrastructure operators to be able to perform the following common activities, all described in further details in the Software Developer Use Case:

- Manage Membership:
    - Apply for, receive, and manage membership in the SWAMP.
- Assess Software Using SwA Tools:
    - Directly assess software that has source code or Java bytecode available.
    - View assessment results performed by an external entity:
        - developer of the software package.
        - contracted third party.

Detailed Narrative of Use Case

Manage Membership

Before using the SWAMP, each user must register for an account. Any personal information required is kept in strict confidence and not shared with any other SWAMP user. For access to SWAMP capabilities, the user's account must then be associated with an active SWAMP project. The user may request the creation of a new SWAMP project or with the permission of the project owner join an existing SWAMP project. Each project request is reviewed by SWAMP administration to ensure the requested use is supported by and aligned with the SWAMP's capabilities and mission. Once access is granted, one can use the account management interface to update personal information and change passwords as needed. Projects and users may disassociate themselves from each other at any time. When a user no longer needs access to the SWAMP, they may cancel their account.

Directly Assess Software Using SwA Tools

The infrastructure operator uses the SWAMP to assess software using SwA tools acting like a software developer. This functionality is detailed in the Software Developer Use Case. The operator will have to interpret the assessment results directly to make a judgement about the software's security and quality.

View Assessment Results from an External Entity

The infrastructure operator, as part of their SwSCRM process, requires the software developer or a trusted third party to use the SWAMP to assess the software. The infrastructure operator can then use the assessment results directly to make a judgement about the software's security and quality, or use a third party assessment to decide whether to accept the software. The decision can be based on factors such as the type and quantity of weaknesses reported along with known design, implementation and deployment factors.

Future Support for the Infrastructure Operator

Besides the enhancements outlined in the Software Developer Use Case's Future Support section, we plan to add the following capabilities aimed at the infrastructure operator in the years following IOC:

- Allow subscriptions to software packages undergoing CSwA with notifications sent when new assessment results are available.

- Allow subscriptions to existing versions of software packages that are deployed in the infrastructure operator's environment. These software packages will be assessed again as new SwA tools or new versions of existing SwA tools are added to the SWAMP with notifications sent when new weaknesses are discovered.

- Allow infrastructure operator to determine the authenticity of their software by retrieving secure hashes of the software artifacts from the SWAMP. This will aid the detection of counterfeit or malware modified versions of the software.

- Allow downloading of the software package artifacts, such as the source code, and artifacts from building the software such as installers, executables and libraries.

- Enhance the privilege model to allow the disclosure of specific weakness results, or summary results without disclosing other facts about the software such as its source code. Also provide the viewer assurance how the results were generated (result provenance). This allows true third party assessments where a third party assesses the software supplier's source code and present the results or a summary to the acquirer.

- Enhance the reporting to be more appropriate for the infrastructure operator's needs.