INDIANA UNIVERSITY

PERVASIVE TECHNOLOGY INSTITUTE

Software Assurance Tools at Indiana University:

A Return to the SWAMP

Rob Quick
Research Technologies
Manager High Throughput Computing
Operations Officer - OSG
Operations Officer - SWAMP

SWAMP
SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

Top 10 Common Weakness Enumerations

- CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('**SQL Injection**')
- CWE-78 Improper Neutralization of Special Elements used in an OS Command ('**OS Command Injection**')
- CWE-120 Buffer Copy without Checking Size of Input ('**Classic Buffer Overflow**')
- CWE-79 Improper Neutralization of Input During Web Page Generation ('**Cross-site Scripting**')
- CWE-306 Missing Authentication for Critical Function
- CWE-862 Missing Authorization
- CWE-798 Use of Hard-coded Credentials
- CWE-311 Missing Encryption of Sensitive Data
- CWE-434 Unrestricted Upload of File with Dangerous Type
- CWE-807 Reliance on Untrusted Inputs in a Security Decision

http://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html#Listing

Software Assurance Motivation

- The world we live in today is **software-centric**, introducing **significant risks** to confidential data and physical resources
- Applications are leaving the protected enterprise network environment and moving onto the web
- Anything with an outward face to the Internet is a entry point for an attack
- Few developers are trained and equipped to build secure code
- Even those well equipped often utilize code developed by others

SWAMP
SOFTWARE ASSURANCE MARKETPLACE
Do It Early. Do It Often.

V. Welch

The Tools

- Key assets in this battle are the software assessment tools that can scan the program for defects(weaknesses). However, using these tools comes with challenges:
  - Each tool is good at finding some particular problem; no tool is good at everything (or even most things).
  - Configuring, maintaining, and using these tools can be cumbersome, time consuming and tricky.

SWAMP SOFTWARE ASSURANCE MARKETPLACE
Do It Early. Do It Often.

V. Welch

A Framework

- No single Software Assurance(SwA) tool is going to bridge the gap between software and assured software.
- A software assurance (SwA) framework allows construction and automation of SwA workflows.
- Our framework provides code analysis, result normalization and labeling, result merging and integration, visualization, result evaluation and annotation, and risk assessment.
- Aggregates, orchestrates and automates use of SwA tools rather than being a tool itself.
- Should support use cases of software developers, SwA Tool developers, SwA researchers, software users, and educators.

SWAMP
SOFTWARE ASSURANCE MARKETPLACE
Do It Early. Do It Often.

V. Welch

Welcome to the SWAMP

- A continuous assurance platform that enables significant improvements in the quality of SwA tools while broadening adoption of SwA methodologies
- Consists of:
  - 30(and growing) static analysis assessment tools
  - State-of-the-art assessment results viewer
  - "Plumbing" that simplifies access to SwA tools
  - Provides a hub for software assurance projects
  - Supports managed access to tools, packages and results
  - Maintains confidentiality of software and results at the discretion of the user

SWAMP SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

V. Welch

Vision of Continuous Assurance

- **Continuous integration (CI)** is the practice, in software engineering, of merging all developer working copies with a shared mainline several times a day.
- **Continuous Assurance (CoA)** takes the software engineering practice of Continuous Integration to a new level. CoA incorporates SwA tools into the frequent process of building and testing the software throughout its life cycle.

SWAMP SOFTWARE ASSURANCE MARKETPLACE
Do It Early. Do It Often.

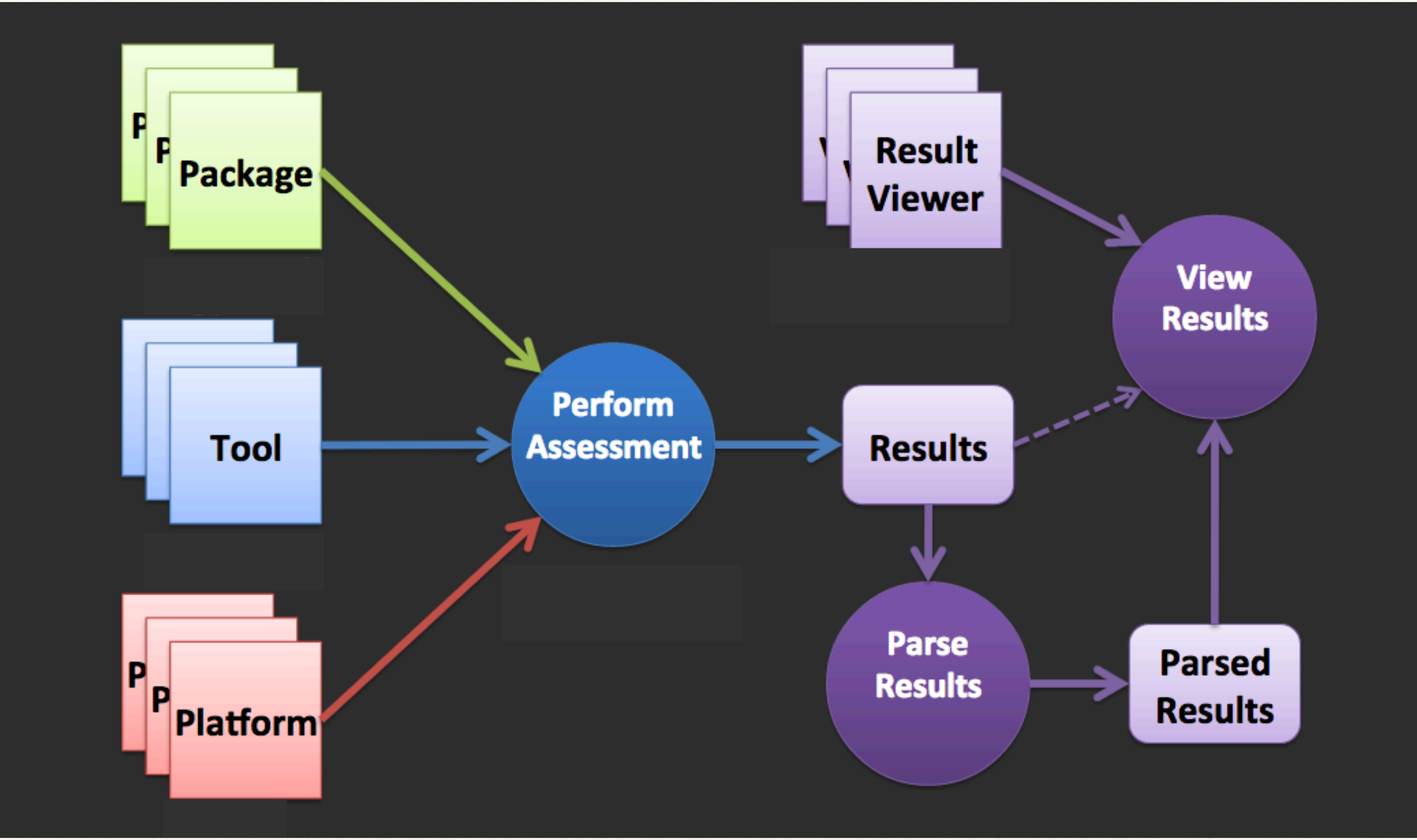
V. Welch

What is the SWAMP?

- The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.
- This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

SWAMP SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.


Package
Tool
Platform
Perform Assessment
Results
Result Viewer
View Results
Parse Results
Parsed Results

Languages Supported

SWAMP

- C/C++
- Java source
- Java bytecode
- Python
- Ruby
- PHP
- Javascript
- HTML
- CSS
- XML

SiB

- C/C++
- Java source
- Java bytecode
- Python
- Ruby
- **Coming Soon:**
  - PHP
  - Javascript

SWAMP SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

Tools Supported

SWAMP

- **Open tools**
  - Android lint
  - Bandit
  - Brakeman
  - checkstyle
  - Clang Static Analyzer
  - cppcheck
  - CSS Lint
  - Dawn
  - error-prone
  - ESLint
  - Findbugs
  - Flake8
  - Flow
  - GCC
  - HTML Tidy
  - JSHint
  - OWASP Dependency Check
  - PHPMD
  - PHP_CodeSniffer
  - PMD
  - Pylint
  - Reek
  - Ruby-lint
  - Retire.js
  - RevealDroid
  - RuboCop
  - ruby-lint
  - XML Lint
- **Commercial tools**
  - GrammaTech CodeSonar
  - Parasoft C/C++test
  - Parasoft Jtest

SiB

- Bandit
- Brakeman
- checkstyle
- Clang Static Analyzer
- cppcheck
- Dawn
- error-prone
- Findbugs
- Flake8
- GCC
- OWASP Dependency Check
- PMD
- Pylint

CONTINUOUS ASSURANCE SWAMP SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

Platforms Supported

SWAMP

- Android
- CentOS Linux 5 32-bit and 64-bit
- CentOS Linux 6 32-bit and 64-bit
- Debian Linux
- Fedora Linux
- Red Hat Enterprise Linux 6 32-bit and 64-bit
- Scientific Linux 5 32-bit and 64-bit
- Scientific Linux 6 32-bit and 64-bit
- Ubuntu Linux

- **Upcoming:**
  - Mac OS X
  - Microsoft Windows

SiB

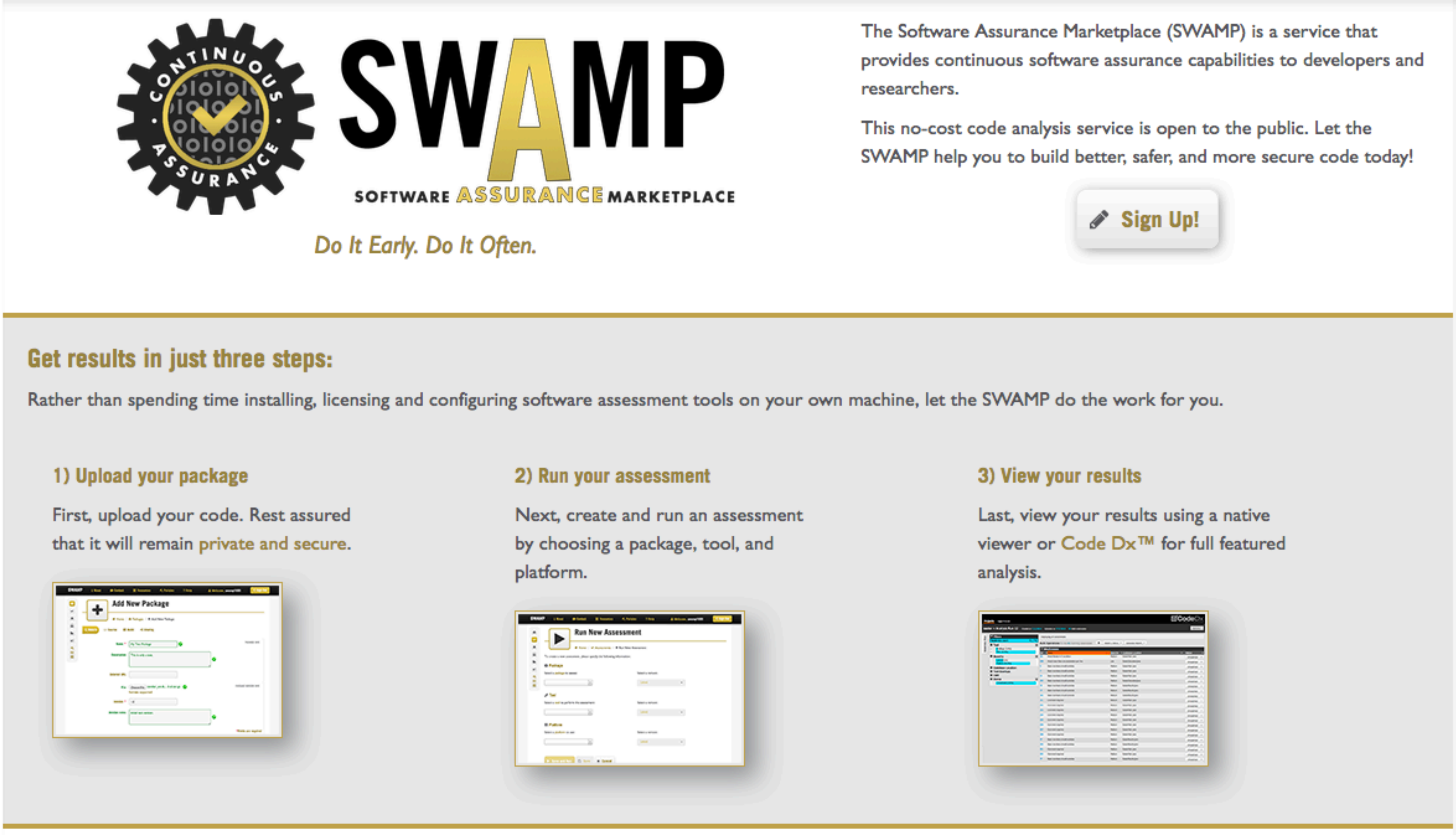
- Ubuntu Linux

- **Upcoming:**
  - Mac OS X
  - Microsoft Windows

SWAMP SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

http://mir-swamp.org/



CONTINUOUS ASSURANCE

SWAMP

SOFTWARE ASSURANCE MARKETPLACE

Do It Early. Do It Often.

The Software Assurance Marketplace (SWAMP) is a service that provides continuous software assurance capabilities to developers and researchers.

This no-cost code analysis service is open to the public. Let the SWAMP help you to build better, safer, and more secure code today!

Sign Up!

Get results in just three steps:

Rather than spending time installing, licensing and configuring software assessment tools on your own machine, let the SWAMP do the work for you.

1) Upload your package

First, upload your code. Rest assured that it will remain private and secure.

2) Run your assessment

Next, create and run an assessment by choosing a package, tool, and platform.

3) View your results

Last, view your results using a native viewer or Code Dx™ for full featured analysis.

The rest of this session…

- Get a SWAMP Account
- Identify and Acquire Interesting Packages
- Move the Package to the SWAMP
- Run an Assessment
- View Results

https://tinyurl.com/swampdemo

- SWAMP Website: https://continuousassurance.org/
- SiB Info: https://continuousassurance.org/swamp-in-a-box/
- Von's full slide set: http://www.vonwelch.com/pres/SWAMP-Regenstrief-Sep-2014.pdf
- Bart's and Elisa's full slide set: https://static1.squarespace.com/static/5047a5a6e4b0dcecada15549/t/54071f4ce4b00e19c7ef11c9/1409752908265/Miller-Heymann-NSF-2014.pdf
- SWAMP-in-a-Box git repo https://github.com/mirswamp/deployment