Naval Surface Warfare Center Dahlgren Division

Software Assurance

Presented by

James Kelchner

Software Assurance Technical Lead

2 May 2024

Agenda

- Software Assurance (SwA) Overview
- General Principles of SwA
- SwA in the Software Development Life Cycle (SDLC)
- SwA Activities and Processes
- Day-to-Day Activities
- Conclusion

Software Assurance Overview

Software Assurance (SwA) is the level of confidence that software functions as intended and is free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.

- Ensures software is securely designed, developed & tested
- Identifies if underlying software dependencies are free of known vulnerabilities
- Integrates with DevSecOps/software pipeline & automation (supports secure development, testing and architecture for urgent changes against new threats)
- Helps Developers avoid inserting new software vulnerabilities and finding & fixing existing ones in the codebase
- Helps Program Managers drive towards building a secure system

Software assurance allows programs to locate potential vulnerabilities and attack vectors

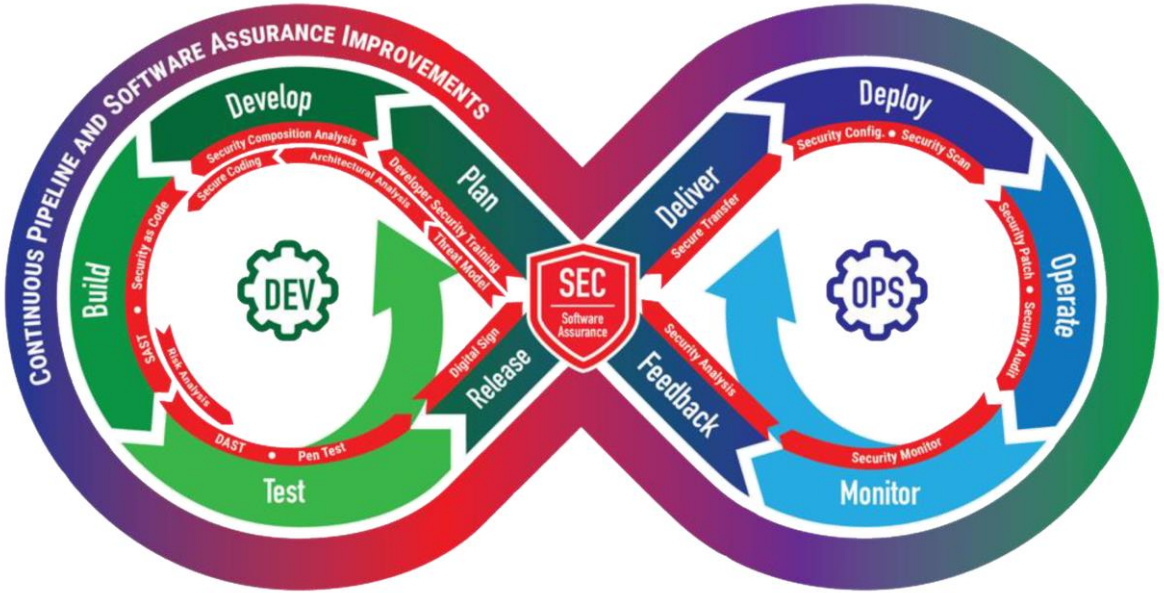
General Principles of SwA

- Practice secure coding
- Use multiple SwA activities and tools
- Understand risks to drive appropriate assurance decisions to mitigate, remediate, or accept
- Align risk concerns across all stakeholders and all interconnected technology elements
- Practice zero trust of dependencies until proven trustworthy
- Expect attacks
- Use independent SwA providers to supplement developer SwA activities

SwA requires effective coordination and participation among all stakeholders

SwA in the Software Life Cycle

- Start where you are and plan for the future
- Start small, start early, and leverage SwA SMEs across the life cycle

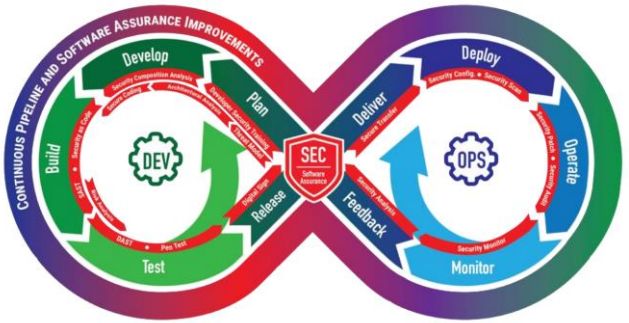


Source: https://insights.sei.cmu.edu/

SwA Activities and Processes

Activities and processes of SwA:

- Static Application Security Testing (SAST) – Build Phase
- Software Bill of Materials (SBOM) – Develop and Release Phases
- Software Composition Analysis (SCA) – Develop Phase
- Architectural Analysis – Plan phase
- Threat Modeling – Plan phase
- Dynamic Application Security Testing (DAST) – Test Phase
- Fuzzing – Test Phase
- Binary Analysis – Test Phase
- Interactive Application Security Testing (IAST) – Test, Operate, Monitor, Feedback Phases



Day to Day of a SwA SME

- Provide SwA direction across programs
- Oversee the development and collection of SwA guidance for a DoD working group
- Support System Security Engineering efforts
- DevSecOps support
- Tool analyses
- Software assessments
- Training development
- Collaborate with other federal agencies

Conclusion

- SwA needs to be applied throughout the lifecycle to ensure the level of confidence that software functions as intended and is free of vulnerabilities
- SwA best practices
  - Secure coding practices
  - Use multiple SwA activities and tools
  - Use independent SwA subject matter expert to supplement developer SwA activities
- Start where you are and keep learning!

Security Should Be Baked In, NOT Bolted On