The Need for a StrongApplication Security Practice

An organization’s application security program is established to introduce and enforce controls at various touchpoints along the SDLC. To identity early weaknesses, the team can save itself from expensive bug fixes and refactors that add in cost as the application matures. While vendors are quick to promote tools to answer all of an organization’s needs, only a combination of **tooling**, **process** and most importantly, **people**, can guarantee a robust program.

Tooling

While it’s true that many issues cannot be prevented by tooling alone, tooling does go a long way to help identify issues. The following are the different types of tooling that we have in place:

- Static Code Analysis
- Source Composition Analysis
- Dynamic Analysis
- Container Scanning

Process

It’s the process that details the controls an organization will elect to utilize in each phase of the SDLC. Even at the start of a new project, activities such as secure design reviews and threat modeling, a shift to the left, help to establish the basis of a secure system.

As we move to the right and coding begins, code reviews become critical in identifying issues before they are introduced.

People

Without people and a mindset change, it’s very difficult to impact change with process and tools alone. As an investment strategy, security training provides a great catalyst to reduce the skills gap promoting a more security-conscious development team.

People include:

- Persons in the OWASP Foundation, a public community that identifies security risks and provides specific guidance for developers to avoid these risks and solve security related problems.
- Vendors of our security tools.
- Corporate subject matter experts from the Information Security Office (ISO), the Infrastructure Team, the Dev Ops Team, the App Dev Architecture Team, and developers.
- All orporate software development partners and consultants.
- *Any technical or non-technical resource at a company who sees a security or data privacy issue with any application or web site.*

Workshops are conducted for awareness and knowledge on the following:

- OWASP Foundation based App Security Policies.
- Secure code reviews
- Rugged software development
- Unit testing