Security Development Lifecycle (SDL)

The Microsoft SDL is an ISO 27034 aligned set of security development practices which are technology agnostic and grouped along with phases of the traditional software development life cycle (SDLC). Experience at Microsoft and multiple industry adopters has shown that integration with the SDLC process leads to greater security gains than practices implemented piecemeal or ad-hoc.

Casaba's SDL Expertise

As a member of the premier Microsoft SDL Pro Network, a collection of less than 24 service, training, and product firms from around the world, Casaba has been recognized as an industry leader with demonstrated capability within all phases of the SDL.

Casaba has worked with organizations to build and augment SDL programs, including the basics of advising and managing security compliance through all phases of the SDLC. Beyond the basics, Casaba has launched more mature aspects of an SDL program, including internal cybersecurity teams, red teams, application penetration testing teams, and bug bounty programs.

Why SDL?

Organizations who have reached an Advanced or Dynamic SDL maturity level have experienced the strategic value it provides in helping them protect customers, innovate efficiently, and stay ahead of competitors. At this level, a fully integrated SDL program has proven ROI for adopters which:

- Manages compliance with standards such as HIPAA and PCIDSS
- Simplifies the onboarding process for developers
- Scales security practices across divisions
- Moves security practices from a reactive to a proactive position
- Quantifies risk and achievements
- Enables visibility for executive leadership

What to Expect

To build your SDL program and maturity roadmap, Casaba will leverage the industry hallmark Microsoft SDL as the program model, building out details specific to your requirements. We will also leverage the Building Security In Maturity Model (BSIMM) scientific study as a measuring stick, for its real-world SDL-program data across 78 organizations.

Building a sophisticated SDL from ground zero requires significant investment, but can be done in phases targeting increasing maturity levels. At the earliest maturity level, 'Standardized' in the graphic below, you can expect a working program which has graduated one or more pilot applications.

Casaba is sensitive to time constraints in your organization, and will require at least one primary point of contact as well as commitments from key stakeholders and individual contributors.

The Casaba Approach

Casaba works as your integrated partner providing leadership and support in the development, deployment, staffing and management of end-to-end SDL programs. We work closely with your management and technical teams to understand your business goals and engineering processes and build an SDL program that meets your current and unique needs. Our approach is to work face-to-face with your company's leadership, and in the field with your development staff, through the following four major phases:

Assess

We begin by understanding your organization and goals by working closely with your CIO or CISO and key stakeholders. Through breakout discussions with subject matter experts, we will perform a maturity assessment to establish a knowledge of the current state of security in your SDLC, relating to the following areas: training, policy, capability, requirements, design, implementation, verification, release, and response.

Identify and Create

Informed on your organization's current and desired positions within the SDL maturity model, we work to create the requirements and capabilities for your SDL program, including training requirements, bug bars, quality gates, and more. A bulk of the recommendations and guidance are created during this phase, when we work closely with our point of contact and key stakeholders to determine many of the important details for your SDL program to be a success and provide the desired metrics for management visibility.

Evaluate and Plan

In this pivotal phase we shift to determining what needs to be done to implement the capabilities as outlined. We also prepare an SDL advisory team with defined roles, and select the application pilots which will be used to evaluate the SDL implementation.

Deploy

In culmination of previous work, we execute the SDL program by guiding a select group of application pilots through the established requirements and processes. This stage is expected to require the most time from your development staff and the most field work from Casaba. To start, development staff should receive training on threat modeling and SDL basics. Following this, Casaba and members from the selected SDL advisory team will guide the pilots through application threat modeling, security testing, and bug triage.

About Casaba

Casaba is a strongly integrated team of security pioneers with a reputation for relentlessly researching, developing, and implementing innovative solutions to the most difficult security problems. We are prepared to assist in every phase of security consulting and auditing, and we are fully bonded and insured by Lloyds of London.

Get Started

Contact us today for a free consultation and security review:

- Phone: 1-888-869-6708
- Email: info@casaba.com
- Web: www.casaba.com