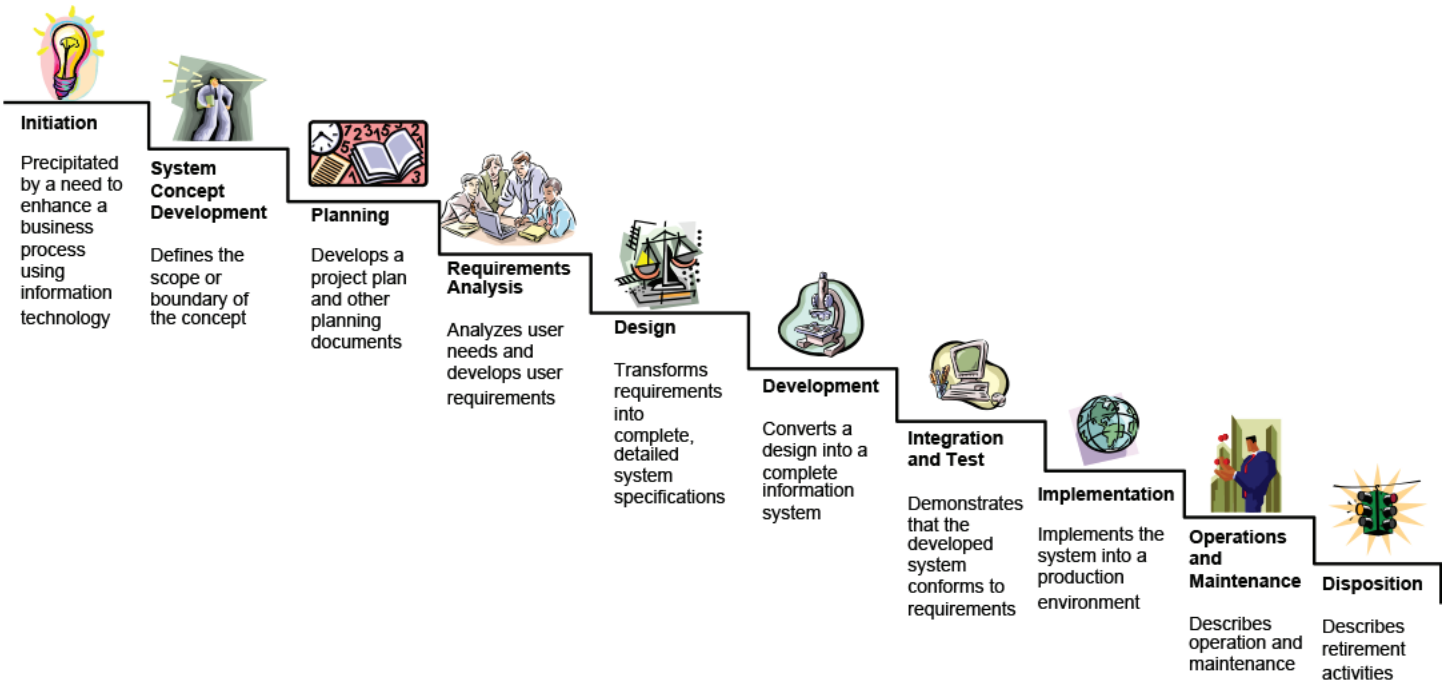
Secure Development Life-Cycle Security Services (SDLC-SS)

Overview

Secure Development Life-Cycle Security Services (SDLC-SS) offers an organization the opportunity to influence product security earlier in the development process.



By addressing security earlier in the life cycle, significant savings may be realized to avoid re-architecting security features into already deployed solutions. Emagined Security's consultants have extensive experience all areas of the SDLC. For simplification, services have been categorized into the following categories: Define, Design, Development, Deploy and Maintain.

Benefits

This unique solution is designed to provide clients the opportunity to implement security controls and reviews during all phases of a products design, implementation and deployment. In today's rapid, design and deployment business model, security is often an afterthought and compromises are exponentially more expensive to address. By injecting security earlier in the development and deployment process, Emagined Security seeks to minimize attack surfaces and reduce long-term costs associated with vulnerabilities, compromises and reputation loss.

Description of Service

Emagined Security's SDLC-SS can enter product development at any stage.

Define

During the Define phase, Emagined Security can assist with the following services:

- Concept Development: Emagined Security works with companies to develop new secure business propositions.
- Requirements Development: Emagined Security helps create solution requirements so designs can meet business and technical requirements.
- Development Planning: Emagined Security can manage the entire lifecycle of a company's solution creation including project management activities and the creation of project documentation.
- Business Comparisons: Emagined Security provides an opportunity to evaluate how a potential product holds up under competitive scrutiny.

Design

During the Design phase, Emagined Security can assist with the following services:

- Security Foundation Analysis: Emagined Security examines the underlying process of development, deployment and maintenance. Emagined Security assists in developing a secure business process for implementation of the project.
- Architecture & Design Development: Emagined Security assists with initial architecture and design development with an eye toward security. This solution assists technology research and seeks to advise the client based on the best available solution, while taking into account the business environment.
- Architecture & Design Review: Emagined Security analyzes architecture and designs already in place. Emagined Security can assist in identifying controls and design problems before the issues reach full implementation.
- Threat Modeling: Emagined Security examines the product in its deployed environment to determine who the products adversaries may be and where they can potentially attack the product. This allows Emagined Security's clients to better focus resources and design efforts.

- Design Documentation: Emagined Security provides clients the necessary information to ensure project continuity while provided needed documentation. This documentation typically is used to design trade-off and the associated business decisions.

Development

During the Development phase, Emagined Security can assess security in the lab provides advanced knowledge of vulnerabilities before exposure to end-users.

- Static Code Analysis: Emagined Security examines the current build for various security issues before researchers and users can discover them.
- Security User Acceptance Testing (UAT): Emagined Security assists in developing test conditions, specifically for security vulnerabilities.

Advanced development testing focuses on providing services while the product is still in development, but may also be employed once the product has been deployed.

- Static & Dynamic Source Analysis: Emagined Security covers both the compiles and raw application source. Static source analysis will provide the most code coverage in a short period of time. Combined with a dynamic scanning results will often weed out most low hanging fruit, enabling more expensive manual testing to focus on business logic and complex attack vectors.
- Reverse Engineering: Emagined Security can reverse engineer code to attempt to find unique penetration test attack vectors.
- Security Research: Emagined Security can perform detailed analysis and reviews of applications to help identify complex vulnerabilities that may be used by Advanced Persistent Threats.
- Physical Penetration Testing: Emagined Security ensures simply opening the door cannot defeat investments in logical attack vectors.

Deploy & Maintain

During the Deploy & Maintain phase, Emagined Security offers a standard line of penetration testing options. Oftentimes businesses do not have the luxury of implementing security from the bottom up and must ensure systems are secure after they have been fully implemented and deployed. These services are typically used to verify that solutions do not have unacceptable vulnerabilities prior to deployment, after significant changes and during periodic reviews.

- Network Penetration Testing: Emagined Security will perform an external penetration test against the Internet architecture (i.e., firewalls, DNS servers, routers, hubs, load balancers, and supporting systems).
- Web Application Penetration Testing: Emagined Security will test the application's security controls to determine if an attack may result in inappropriately viewing, altering, or deleting information.
- Wireless LAN Penetration Testing: Emagined Security will attempt to penetrate a company's wireless LAN infrastructure (War Driving), as well as surrounding network systems.
- Application Penetration Testing: Emagined Security will assess commercial off the shelf (COTS) programs or custom built applications for security vulnerabilities to enables clients to quickly identify, assess and remedy security holes.
- Mobile Penetration Testing: Emagined Security will assess mobile applications written to run on the Apple IOS, Android or Windows mobile platform for security vulnerabilities to enable clients to quickly identify, assess and remedy security holes.

Penetration Testing services are offered at the following levels:

- Level 3 – Ethical Hack: This version includes the Penetration Test and adds attempts to use the exploited vulnerabilities to compromise systems behind the initial targets. This is the most extensive version of the test.
- Level 2 – Penetration Test: This version includes the Vulnerability Assessment and adds exploitations of the vulnerabilities. This is the standard version of the test.
- Level 1 – Vulnerability Assessment: This version includes only scans and validation of vulnerabilities. It is minimal version of the test.
- Level 0 – Vulnerability Scan: This version includes a basic scan to satisfy regulatory requirements utilizing a single vulnerability tool. The associated deliverable is limited to only raw reports from the tool. No analysis on results is performed at this level.