CENSUS
IT Security Works

BUILDING A SECURE SDLC

WHAT IS A SECURE SDLC?

A Software Development Lifecycle (SDLC) represents a series of steps taken during the development of a software product. Although SDLC strategies may vary from organization to organization their ultimate goal is the efficient production of high quality products. A Secure SDLC is a development lifecycle that has been augmented by a special set of processes, whose goal is the development of products meeting high security standards. Secure SDLC methodologies allow for the early mitigation of security risks, by identifying and fixing security vulnerabilities during the early stages of software development. They also introduce best-of-breed proactive defenses in the design and implementation of the software, thus minimizing the released product's exposure to future threats.

CENSUS SERVICES FOR THE REALIZATION OF A SECURE SDLC

CENSUS provides specialized software security services to help businesses build and maintain a Secure Software Development Lifecycle. These services range from consulting and training on Secure SDLC procedures, to security audits on the deliverables of each SDLC phase.

The standards-based Secure SDLC models proposed by CENSUS introduce security processes that run within the boundaries of the already established SDLC phases. In this way, the impact to existing processes and flows is kept minimal and, more importantly, security deliverables become a formal requirement at the end of each SDLC phase (e.g. a security review of the software architecture document will be expected at the end of the software design phase). Experience has shown that this approach is flexible enough to allow its application to both traditional (e.g. Waterfall) and modern (e.g. Agile) development strategies.

PLANNING PHASE

For the Planning phase of projects, CENSUS can provide the necessary training for the implementation of a Secure SDLC. This includes training on SDLC procedures, but also training on security topics related to the technologies that will be used by the development team (e.g. Secure Java Development, Secure Mobile App Development etc.). CENSUS can also provide Vulnerability Research services to examine the security of technologies that are considered for adoption at this phase in the project.

DESIGN PHASE

To gain the most out of a Secure SDLC, a project needs to adhere to the secure-by-design principle. To this effect, CENSUS offers consulting services for the security review of design documents, including the design-level review of new protocols and security controls. CENSUS can also provide assistance on the development of the project security architecture plan and related threat model. The work performed in this phase will stand as a rigorous test to the concepts portrayed in the project design documents and will justify countermeasures that need to be taken in order to minimize the identified risks.

IMPLEMENTATION PHASE

Performing security evaluations of a software's implementation, while the software is being developed, is a key aspect of a Secure SDLC. The CENSUS Source Code Auditing service is designed to help organizations meet this requirement. It offers a thorough security evaluation of a project's code using both static and dynamic analysis techniques. The evaluation can occur either per milestone/sprint or per release candidate.

RELEASE PHASE

Security tests must also be part of the release testing deliverables. CENSUS can examine the production-grade setup of a project through Penetration Testing to identify paths through which an attacker may circumvent the project's security controls and gain unauthorized access to the project's valuable assets (e.g. a database holding user information). During release testing, CENSUS can also provide Bundle Inspection services to check whether the packaged form of the software meets the project's security requirements (e.g. no debugging information has made it into the release package, software integrity protections work as expected).

PRODUCTION PHASE

For teams that maintain software that has been released, CENSUS experts can help in the handling of post-release security issues, by providing issue & fix evaluation services. Incident response services are also available for the investigation of cyber attacks that have targeted production systems and services.

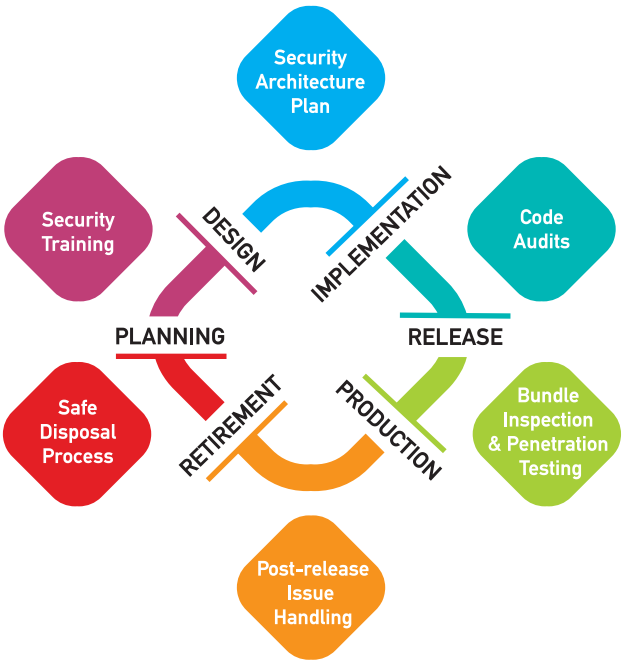
RETIREMENT PHASE

Through security consulting CENSUS can help ensure that the procedures that take place during the project's disposal / upgrade phase (e.g. handling of sensitive data) are compatible with the project's security requirements and are in strict accordance with applicable law and policies.

BENEFITS

Software vendors that adopt a Secure SDLC gain significant benefits, such as:

- The production of high quality software
- The early mitigation of risks
- The mitigation of risks in a cost-effective manner
- The continuous improvement of the development team's security awareness



For more information about the CENSUS Secure SDLC services please visit: **www.census-labs.com**

CENSUS
IT Security Works

Stadiou 33, 10559,
Athens, Greece
T. +30 2110 128 355
F. +30 2310 947 234

I. Gkoura 16, 54352,
Thessaloniki, Greece
T. +30 2310 947 233
F. +30 2310 947 234

E. info@census-labs.com
www.census-labs.com