SECURITY TRAINING SERVICES

Employee training is essential to the success of businesses, as it assists employees in growing their knowledge base and improving their job skills to become more effective in the workplace. It is also beneficial for employers to enhance employee productivity and improve the company culture. Next to that, nowadays organizations face more security threats than ever, making employee security education crucial.

To this end, CENSUS offers Security Training courses that aim to raise the security awareness of personnel regarding cybersecurity threats. CENSUS also offers courses to enable developers and the management in efficiently addressing security defects within an existing systems development lifecycle (SDLC). This allows for the earliest possible treatment of security errors and the development of better, more robust systems. Training courses are delivered by security experts and are based on material coming from best practices, international standards, and field experience from real-world environments.

The CENSUS Security Training services include the following courses:

- Security Awareness Training
- Introduction to Software Security
- Web Application Vulnerabilities
- Mobile App Vulnerabilities (covering Android and iOS apps)
- Implementing a Secure Systems Development Lifecycle
- Secure Development in Java
- Secure Development in C/C++
- Security Tooling for Development Teams
- Security Tooling for QA Teams

The trainings may be requested in an ad-hoc manner or can be grouped together depending on the needs of the organization. CENSUS also delivers tailored training sessions on topics selected by customers.

SECURITY AWARENESS TRAINING

Intended Audience: Organization Staff

The course describes the current cyber threat landscape for organizations, events that may serve as indicators of an ongoing attack, and best practices for building effective defenses against such threats. The course covers key topics such as Social Engineering, Phishing attacks, Sensitive Information handling, Password management, Wi-Fi attacks, Physical and End-point security.

INTRODUCTION TO SOFTWARE SECURITY

Intended Audience: Development Teams

This course introduces the field of software security. It explains the risks related to common software vulnerabilities (e.g., Buffer Overflows, Replay Attacks, etc.) and describes key security controls to address them. Furthermore, it shows how risks can be identified & managed throughout the lifetime of a software project.

WEB APPLICATION VULNERABILITIES

Intended Audience: Developers

The Course provides a detailed study of the types of threats that affect today's web applications, including but not limited to the OWASP Top-10 vulnerabilities list. The course discusses topics such as Code Injection issues, Data Parsing issues, Proxy and Web Cache attacks, Problematic Security Controls, and Supply Chain issues.

MOBILE APP VULNERABILITIES

Intended Audience: Developers

The course presents the most common vulnerabilities, as listed in the OWASP Mobile Top-10, affecting today's mobile app software. Moreover, the course discusses the Security Architectures of the two most common mobile platforms (iOS and Android), and explains key security controls that protect data and system security.

IMPLEMENTING A SECURE SDLC

Intended Audience: Product Managers and Technical Leads

The course explains the process of integrating security audits and processes into an existing Systems Development Lifecycle model. In particular, the fundamentals of a Secure SDLC along with standard methodologies are presented. Following that, a new secure SDLC proposal is made for the client, fitting the client's needs and workflows. The proposal provides a step-by-step guide for the client's path towards security maturity.

SECURE DEVELOPMENT IN JAVA

Intended Audience: Developers

This course covers important security issues that affect applications developed in the Java programming language, including but not limited to Exception Handling, Logical errors, Serialization issues, Injection issues, Race Conditions and Handling of privileged code.

SECURE DEVELOPMENT IN C/C++

Intended Audience: Developers

With the proliferation of C/C++ code as the basic building block of IT infrastructure and the ease by which programming errors can lead to security issues (e.g., remote code execution), it becomes apparent that developers must be able to identify & resolve such bugs, but also be able to measure the related security risks. This course covers critical security bugs found in C/C++ environments (e.g., Memory Corruption, Information/Recourse leaks, File Handling bugs etc.) and presents proactive measures to defend against them.

SECURITY TOOLING FOR DEVELOPMENT TEAMS

Intended Audience: Development Teams

The course describes the software tools available today that can assist development teams in building trustworthy software. The course covers tools for Software Composition Analysis, Supply Chain Risk Management, Static Analysis, Dynamic Analysis, Semantic Code Analysis etc.

SECURITY TOOLING FOR QA TEAMS

Intended Audience: Development Teams

The course describes the software tools available today that can assist Quality Assurance (QA) and Release Engineering teams in identifying security vulnerabilities in release candidate versions of software. The course covers tools for Functional Security Testing, Vulnerability Scanning, Fuzz Testing etc.

For more information about the CENSUS Security Training services please visit:
www.census-labs.com