CSP102 - SECURE SOFTWARE REQUIREMENTS

Course Learning Objectives

This course is part of the Secure Software Practitioner suite of courses. In four modules, we'll explore modern practices for identifying security risks, analyzing operational requirements, getting formal risk acceptance from the business owner, promoting good data governance, classifying data, choosing appropriate data controls, creating policies for data retention and disposal, complying with privacy legislation, getting user consent regarding their personal information, reporting data breaches, anonymizing data, maintaining an up-to-date software requirements specification, tracking software security requirements, and applying security requirements to partners and suppliers.

Description

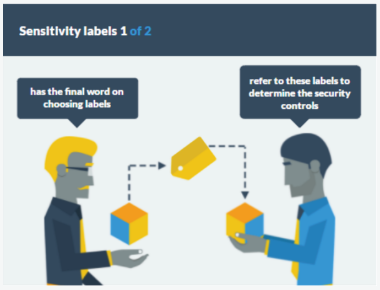
Secure Software Requirements is for anyone involved in the gathering of functional, security or operational requirements, including security professionals, software professionals, architects, product managers, project managers, and program managers.

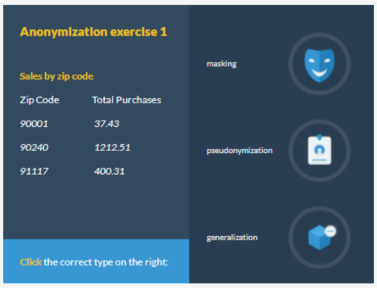
Audience

Software Professionals
Architects
Managers

Time Required

Tailored learning - 80 minutes total (approx.)





CSP102 - SECURE SOFTWARE REQUIREMENTS

Course Outline

1. Gathering Security Requirements

- Shifting security left
- The goal of secure software requirements
- The PNE principle
- PNE techniques
- Use cases
- Misuse cases
- Who writes the security requirements?
- Subject-object matrix
- Operational requirements
- Availability
- Secure deployment
- Assessing risk
- Risk acceptance

2. Classifying Data

- The goal of data classification
- Data classification
- Organizational data roles
- Data owner
- Data custodian
- Additional GDPR roles
- Knowledge check
- Data labeling
- Sensitivity labels
- Impact labels
- Data controls
- Unstructured data
- Unstructured data guidelines
- The data lifecycle
- Data retention
- Data retention requirements
- Data archiving
- Maximum retention times
- Data disposal
- Self-hosted data disposal
- Cloud provider data disposal

3. Identifying Privacy Requirements

- The difference between security and privacy
- Privacy
- Policy decomposition
- Privacy legislation
- Knowledge check
- User consent
- Asking for consent
- The right to be forgotten
- Data breaches
- Breach notification obligations
- Anonymization
- Anonymization scenarios
- Anonymization techniques
- Border crossings
- Treaties

4. Validating Security Requirements

- Validating security requirements
- Maintaining project requirements
- Protecting the SRS
- Tracking security requirements
- Creating an SRTM
- Using an SRTM effectively
- Knowledge check
- Passing security requirements to other parties
- Subcontracting development
- Vendor security posture
- Subcontracting considerations

SecurityCompass