ISTQB Avancé
Tests de sécurité

Vous souhaitez :

- Concevoir et mettre en œuvre une stratégie contre les risques liés à la sécurité
- Définir et implémenter les politiques et procédures de sécurité
- Traiter les menaces sécuritaires tout au long des cycles de développement

Objectif

Préparer le stagiaire au passage de l'examen « Tests de sécurité au niveau avancé » de l'ISTQB

Prérequis

Avoir obtenu la certification ISTQB Fondation et disposer d'au moins 3 ans d'expérience pratique dans le domaine du test logiciel

Public

Ingénieurs des exigences, testeurs fonctionnels, gestionnaires de test, développeurs, spécialistes de l'automatisation des tests, spécialistes des tests de performance, spécialistes de l'environnement de test, spécialistes des tests de sécurité

Méthodes pédagogiques

Supports de formation papier, cahier d'exercices, théorie, exemples, études de cas, QCM, examen blanc

Durée

3 jours (21h) de formation dont un examen de 2h

Les acquis de la formation sont évalués par des QCM, un examen blanc puis l'examen final de certification.
Remise d'une attestation individuelle de fin de formation.

Programme

Jour 1

1. Les bases des tests de sécurité

- 1.1 Risques de sécurité
- 1.2 Politiques et procédures de sécurité de l'information
- 1.3 Audit de sécurité et son rôle dans les tests de sécurité

2. But, objectifs et stratégies des tests de sécurité

- 2.1 Introduction
- 2.2 Le but des tests de sécurité
- 2.3 Le contexte organisationnel
- 2.4 Objectifs des tests de sécurité
- 2.5 La portée et la couverture des objectifs des tests de sécurité
- 2.6 Approches de test de sécurité
- 2.7 Améliorer les pratiques de test de sécurité

3. Processus de test de sécurité

- 3.1 Définition du processus de test de sécurité
- 3.2 Planification des tests de sécurité
- 3.3 Conception d'essai de sécurité
- 3.4 Exécution du test de sécurité
- 3.5 Évaluation de test de sécurité
- 3.6 Maintenance du test de sécurité

Jour 2

4. Tests de sécurité tout au long du cycle de vie du logiciel

- 4.1 Le rôle des tests de sécurité dans un cycle de vie logiciel
- 4.2 Le rôle des tests de sécurité dans les exigences
- 4.3 Le rôle des tests de sécurité dans la conception
- 4.4 Le rôle des tests de sécurité dans les activités de mise en œuvre
- 4.5 Le rôle des tests de sécurité dans les activités de test du système et d'acceptation
- 4.6 Le rôle des tests de sécurité dans la maintenance

5. Test des mécanismes de sécurité

- 5.1 Système de durcissement
- 5.2 Authentification et autorisation
- 5.3 Chiffrement
- 5.4 Pare-feu et zones de réseau
- 5.5 Détection d'intrusion
- 5.6 Analyse de logiciels malveillants
- 5.7 Offuscation de données
- 5.8 Entraînement

Jour 3

6. Facteurs humains dans les tests de sécurité

- 6.1 Comprendre les attaquants
- 6.2 Ingénierie sociale
- 6.3 Sensibilisation à la sécurité

7. Évaluation et rapports des tests de sécurité

- 7.1 Évaluation de test de sécurité
- 7.2 Rapports de test de sécurité

8. Outils de test de sécurité

- 8.1 Types et objectifs des outils de test de sécurité
- 8.2 Sélection d'outil

9. Normes et tendances de l'industrie

- 9.1 Comprendre les normes de test de sécurité
- 9.2 Appliquer les normes de sécurité
- 9.3 Tendances de l'industrie

Modalités de formation et de certification

La durée recommandée pour la formation est de 3 jours. La certification a lieu l'après-midi du dernier jour. La matinée est destinée en partie aux exercices de révision, dont des QCM d'entrainement.

La certification dure 120 minutes, soit 2 heures. Il est nécessaire d'obtenir 65% de bonnes réponses.