

Tests de Logiciels

★ Certifiant

ISTQB Niveau Avancé - Testeur de Sécurité

Formation certifiante ISTQB de niveau avancé dédiée au test de sécurité logicielle : planifier, concevoir, exécuter et évaluer des tests de sécurité selon une approche fondée sur les risques et les standards internationaux.

DURÉE 35 heures	NIVEAU Avancé	FORMAT Présentiel & en ligne
LANGUE Français	CERTIFICAT Certificat Experteam	FORMATEUR Nizar Haddad

Présentation

La formation « ISTQB Niveau Avancé - Testeur de Sécurité », proposée par Expert Team Tunisie (centre de formation IT agréé), prépare les professionnels du test logiciel à se spécialiser dans les tests de sécurité selon le référentiel ISTQB reconnu internationalement. Elle couvre l'ensemble du processus de test de sécurité, depuis l'évaluation des risques et l'analyse des politiques de sécurité jusqu'au test des mécanismes de protection (authentification, cryptage, pare-feu, détection d'intrusion) et à la production de rapports.

Le programme aborde le rôle des tests de sécurité tout au long du cycle de vie du logiciel, la compréhension de la mentalité et des scénarios d'attaque, ainsi que la sélection des outils et l'application des normes de l'industrie. L'objectif est de former des testeurs capables d'évaluer efficacement la robustesse des systèmes face aux menaces actuelles et futures.

La certification obtenue constitue une reconnaissance internationale indépendante de l'expertise en test logiciel avec une spécialisation en sécurité, valorisant fortement le profil des testeurs confirmés, analystes qualité et professionnels de la cybersécurité applicative.

Objectifs pédagogiques

- ✓ Planifier, mettre en œuvre et évaluer des tests de sécurité selon différentes perspectives (politiques, risques, standards, exigences, vulnérabilités)
- ✓ Adapter les activités de tests de sécurité aux différentes phases de développement d'un projet
- ✓ Utiliser efficacement les techniques d'évaluation des risques pour identifier les menaces actuelles et futures
- ✓ Évaluer les suites de test existantes et identifier les tests de sécurité complémentaires nécessaires
- ✓ Analyser les politiques et procédures de sécurité afin d'en déterminer l'efficacité
- ✓ Déterminer les approches de tests de sécurité les plus adaptées à une situation donnée
- ✓ Évaluer l'efficacité des mécanismes de sécurité (authentification, cryptage, pare-feu, détection d'intrusion)
- ✓ Comprendre les méthodologies d'attaque et la mentalité des attaquants pour mieux pallier les failles

Les fondements des tests de sécurité

- Risques de sécurité et rôle de l'évaluation des risques
- Identification des actifs et techniques d'évaluation des risques
- Politiques et procédures de sécurité de l'information
- L'audit de sécurité et son rôle (personnel, processus, technologie)

Buts, objectifs et stratégies des tests de sécurité

- But et contexte organisationnel des tests de sécurité
- Alignement et identification des objectifs de test
- Assurance de l'information vs tests de sécurité
- Portée, couverture et approches des tests de sécurité
- Identification des parties prenantes et amélioration des pratiques

Le processus de test de sécurité

- Définition et alignement du processus de test ISTQB sur le cycle de vie
- Planification des tests de sécurité et éléments clés du plan
- Conception des tests fondée sur les politiques et procédures
- Exécution dans un environnement de test efficace
- Évaluation et maintenance des tests de sécurité

Les tests de sécurité tout au long du cycle de vie du logiciel

- Vue cycle de vie et activités liées à la sécurité
- Tests de sécurité dans les exigences et la conception
- Tests de sécurité en phase d'implémentation (composants et intégration)
- Tests de sécurité en test système et test d'acceptation
- Rôle des tests de sécurité dans la maintenance

Test des mécanismes de sécurité

- Renforcement du système (hardening)
- Authentification et autorisation
- Cryptage et pare-feu / zones de réseau
- Détection des intrusions et analyse des logiciels malveillants
- Obfuscation des données
- Efficacité de la formation à la sécurité

Comprendre les attaquants

- Impact du comportement humain sur les risques de sécurité
- Mentalité des attaquants, motivations et sources d'attaques
- Scénarios d'attaque et ingénierie sociale
- Sensibilisation à la sécurité et moyens de l'accroître

Évaluation des tests de sécurité et rapports

- Évaluation des tests de sécurité
- Confidentialité des résultats
- Contrôles et collecte de données pour le reporting
- Analyse des rapports intermédiaires d'état

Outils, normes et tendances de l'industrie

- Types et objectifs des outils de test de sécurité
- Sélection des outils et évaluation des fournisseurs (dont open source)
- Comprendre et appliquer les normes de tests de sécurité
- Contexte réglementaire/contractuel et tendances de l'industrie

Prérequis

Être titulaire de la certification ISTQB Niveau Fondation et disposer d'au moins 3 ans d'expérience pratique dans le domaine du test logiciel.

Public visé

Testeurs de logiciels confirmés, analystes de test, ingénieurs qualité et professionnels de la cybersécurité applicative souhaitant se spécialiser dans les tests de sécurité.

Prochaines sessions

DATE	VILLE	HORAIRE	FORMATEUR
03/08/2026	En ligne	09h00 - 16h00	Nizar Haddad
07/09/2026	Tunis	09h00 - 16h00	Nizar Haddad

1 450 TND / personne

Acompte de 30% possible à la réservation · Financement sur demande.

Experteam — El Ghazala, Ariana (face au Technopôle La Ghazela)

+216 29 674 204 · contact@expertunisie.com · experteam.itt.tn