ISTQB : Advanced Level – Security Tester

This training is aimed at people directly involved in the design of security tests, their execution and collaboration with the Test Manager.

It has the following objectives:
• Optimize security tests.
• Manage the design and execution of the tests, in line with the activities of the Test Manager
• Perform tests on complex projects.

The Security Tester's mission is to Plan, perform and evaluate security tests from a variety of perspectives – policy-based, risk-based, standards-based, requirements-based and vulnerabilitybased.

Détails

- Code : ISTQBALS
- Durée : 4 jours (28 heures)

Public
- Consultants
- Consultants informatiques
- Developpeurs
- Professionnels de l'IT
- Responsable de la gestion du risque de la sécurité de l'information
- Responsables qualité
- Testeurs

Pré-requis
- Certification at the ISTQB foundation level is required.
- Some practical experience working on software development projects or as a test specialist.

Objectifs
- Analyse the effective use of risk assessment techniques in a given situation to identify current and future security threats and assess their severity levels
- For a given project scenario, identify security test objectives based on functionality, technology attributes and known vulnerabilities
- Analyse a given situation and determine which security testing approaches are most likely to succeed in that situation
- Identify areas where additional or enhanced security testing may be needed
- Demonstrate the attacker mentality by discovering key information about a target, performing actions on a test application in a protected environment that a malicious person would perform, and understand how evidence of the attack could be deleted

Programme

The Basis of Security Testing
- Security Risks. Information Security Policies and Procedures.
- Security Auditing and its Role in Security Testing.

Security Testing Purposes, Goals and Strategies
- The Purpose of Security Testing.
- The Organizational Context.
- Security Testing Objectives.
- TheScope and Coverage of Security Testing Objectives.
- Security Testing Approaches.
- Improving the Security Testing Practices.

Security Testing Processes
- Security Test Process Definition.
- Security Test Planning. Security Test Design.
- Security Test Execution.
- Security Test Evaluation.
- Security Test Maintenance.

Security Testing Throughout the Software Lifecycle
- Role of Security Testing in a Software Lifecycle.
- The Role of Security Testing in Requirements.
- The Role of Security Testing in Design.
- The Role of Security Testing in Implementation Activities
- The Role of Security Testing in System and Acceptance Test Activities.
- The Role of Security Testing in Maintenance.

Testing Security Mechanisms
- System Hardening.
- Authentication and Authorization.
- Encryption.
- Firewalls and Network Zones.
- Intrusion Detection.
- Malware Scanning.
- Data Obfuscation. Training.

Human Factors in Security Testing
- Understanding the Attackers.

- Social Engineering.
- Security Awareness.

- Types and Purposes of Security Testing Tools.
- Tool Selection.

Security Test Evaluation and Reporting

- Security Test Evaluation.
- Security Test Reporting.

Security Testing Tools

Standards and Industry Trends

- Understanding Security Testing Standards.
- Applying Security Standards.
- Industry Trends.

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages