Threat Modeling pour testeurs : anticiper les failles dès la conception avec STRIDE

Lien : https://innov-systems.com/formation/threat-modeling-pour-testeurs-anticiper-les-failles-des-la-conception-avec-stride

DURÉE
5 jours (35h)

RÉFÉRENCE
TLA30

CATÉGORIE
Tests de Sécurité Applicative

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les principes du Threat Modeling appliqué aux tests logiciels
- Maîtriser la méthode STRIDE pour identifier les menaces dès la conception
- Réaliser des Data Flow Diagrams (DFD) pour analyser les architectures applicatives
- Identifier et prioriser les risques de sécurité de manière structurée
- Transformer les menaces identifiées en scénarios de tests de sécurité
- Intégrer le Threat Modeling dans les pratiques Agile, DevSecOps et Secure SDLC
- Automatiser certaines activités de modélisation des menaces
- Vérifier l'efficacité des contre-mesures de sécurité
- Renforcer la collaboration entre les équipes QA, Développement et Cybersécurité
- Réduire les vulnérabilités détectées en phase de production
- Développer une approche proactive de la qualité et de la sécurité logicielle
- Réaliser un projet complet de modélisation des menaces et de validation des exigences de sécurité

POUR QUI ?

- Testeurs logiciels (QA Engineers)
- Ingénieurs Automaticiens de Tests
- SDET (Software Development Engineer in Test)
- Développeurs Full Stack
- Développeurs Backend et Frontend
- DevSecOps Engineers
- Security Engineers
- Architectes logiciels
- Architectes sécurité
- Consultants en cybersécurité
- Chefs de projet techniques
- Toute personne souhaitant intégrer le Threat Modeling et la méthode STRIDE dans les processus de conception, de développement et de validation des applications

Innov Systems

Programme détaillé

1 / Introduction au Threat Modeling

- Principes fondamentaux du Threat Modeling
- Intégration de la sécurité dans le cycle de développement (Secure SDLC)
- Rôle des testeurs dans l'identification précoce des risques

2 / Les fondamentaux de la méthode STRIDE

- Présentation des six catégories de menaces STRIDE
- Identification des actifs critiques et des surfaces d'attaque
- Cartographie des menaces selon le contexte applicatif

3 / Modélisation de l'architecture applicative

- Création de Data Flow Diagrams (DFD)
- Identification des flux, composants et frontières de confiance
- Analyse des points d'entrée et des dépendances

4 / Identification et analyse des menaces

- Détection des vulnérabilités potentielles
- Priorisation des risques avec DREAD, CVSS et autres méthodes
- Documentation des scénarios d'attaque

5 / Conception de cas de tests orientés sécurité

- Transformation des menaces en scénarios de tests
- Élaboration de tests fonctionnels et non fonctionnels
- Validation des exigences de sécurité

Innov Systems

6 / Intégration du Threat Modeling dans les tests logiciels

- Sécurité dès la conception (Shift Left Security)
- Collaboration entre QA, développeurs et équipes sécurité
- Intégration dans les processus Agile et DevSecOps

7 / Automatisation et outils de Threat Modeling

- Présentation des principaux outils de modélisation des menaces
- Génération automatisée de rapports et de recommandations
- Intégration avec les plateformes CI/CD et DevSecOps

8 / Validation des contre-mesures de sécurité

- Vérification des mécanismes de protection
- Tests de robustesse et de résilience
- Suivi des actions correctives et validation des correctifs

9 / Gouvernance et amélioration continue

- Gestion documentaire et traçabilité des analyses
- Mise à jour des modèles de menaces
- Indicateurs de maturité et suivi des risques

10 / Cas pratiques et projet de bout en bout

- Réalisation d'un Threat Modeling complet avec STRIDE
- Construction d'un plan de tests de sécurité basé sur les risques
- Bonnes pratiques d'intégration du Threat Modeling dans les projets logiciels

Inov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés