Threat Modeling — Analyse et modélisation des menaces applicatives

Lien : https://innov-systems.com/formation/threat-modeling-analyse-et-modelisation-des-menaces-applicatives

DURÉE
4 jours (28h)

RÉFÉRENCE
SI133

CATÉGORIE
Sécurité des Applications

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes du Threat Modeling
- Identifier les menaces applicatives de manière structurée
- Maîtriser les méthodologies STRIDE et équivalentes
- Cartographier les systèmes et flux applicatifs
- Évaluer les risques de sécurité applicative
- Définir des stratégies de mitigation efficaces
- Intégrer la sécurité dès la conception (Security by Design)
- Renforcer les pratiques DevSecOps
- Utiliser des outils de modélisation des menaces
- Réduire les vulnérabilités dans les applications
- Améliorer la posture de sécurité des systèmes
- Étudier des cas concrets de sécurité applicative

POUR QUI ?

- Développeurs logiciels
- Architectes applicatifs
- Ingénieurs cybersécurité
- DevSecOps engineers
- Pentesters / Ethical hackers
- SRE et platform engineers
- Product owners techniques
- Consultants sécurité
- Analystes risques IT
- Chefs de projet IT
- QA engineers
- Toute personne impliquée dans la conception et la sécurité des applications

Innov Systems

Programme détaillé

1 / Introduction au Threat Modeling

- Définition et objectifs de la modélisation des menaces
- Importance dans le cycle de développement sécurisé (SSDLC)
- Cas d’usage en cybersécurité applicative

2 / Principes fondamentaux de la sécurité applicative

- Confidentialité, intégrité, disponibilité (CIA)
- Surface d’attaque et vecteurs d’attaque
- Notions de risque et criticité

3 / Méthodologies de Threat Modeling

- Approche STRIDE (Microsoft)
- DREAD et autres modèles d’évaluation des risques
- Méthodes centrées architecture et données

4 / Cartographie des systèmes et des flux

- Diagrammes de flux de données (DFD)
- Identification des actifs critiques
- Analyse des dépendances système

5 / Identification des menaces

- Types d’attaques applicatives
- Vulnérabilités courantes (OWASP Top 10)
- Scénarios d’attaque réalistes

Innov Systems

6 / Analyse des risques

- Évaluation de la probabilité et de l’impact
- Priorisation des menaces
- Matrices de risque

7 / Stratégies de mitigation

- Mesures de sécurité techniques
- Design sécurisé des applications
- Contrôles préventifs et détectifs

8 / Intégration dans le cycle DevSecOps

- Threat modeling dans CI/CD
- Automatisation des contrôles de sécurité
- Collaboration Dev, Sec et Ops

9 / Outils et cas pratiques

- Microsoft Threat Modeling Tool, OWASP Threat Dragon
- Études de cas réels d’architectures applicatives
- Atelier de modélisation de menaces

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

Innov Systems

Prochaines dates programmées

05 au 08 Jan. 2027	Présentiel - Casablanca
02 au 05 Mars 2027	Présentiel - Casablanca
27 au 30 Avr. 2027	Présentiel - Casablanca
22 au 25 Juin 2027	Présentiel - Casablanca
24 au 27 Août 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

Innov Systems