Cyber Risk Quantification (CRQ) : mesurer et communiquer le risque cyber en valeur financière (FAIR)

Lien : https://innov-systems.com/formation/cyber-risk-quantification-crq-mesurer-et-communiquer-le-risque-cyber-en-valeur-financiere-fair

DURÉE
5 jours (35h)

RÉFÉRENCE
SI99

CATÉGORIE
Analyse des Risques, Audit de Sécurité

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les principes de la quantification du risque cyber
- Maîtriser la méthodologie FAIR
- Construire des modèles de risque cyber financiers
- Transformer les risques techniques en indicateurs financiers
- Améliorer la prise de décision basée sur les risques
- Prioriser les investissements en cybersécurité
- Intégrer la CRQ dans la gouvernance des risques
- Structurer des scénarios de menace réalistes
- Utiliser des données pour quantifier le risque
- Communiquer efficacement le risque cyber aux dirigeants
- Mettre en place une démarche CRQ en entreprise
- Étudier des cas concrets de modélisation du risque cyber

POUR QUI ?

- RSSI / CISO
- Risk managers
- Cybersecurity analysts
- Chief risk officers
- Consultants en cybersécurité
- Architectes sécurité
- Data analysts sécurité
- Auditeurs IT
- Responsables conformité
- Managers IT et sécurité
- Responsables assurance et gestion des risques
- Toute personne impliquée dans la gestion, l’évaluation et la communication du risque cyber

Innov Systems

Programme détaillé

1 / Introduction à la Cyber Risk Quantification (CRQ)

- Passage d’une approche qualitative à quantitative du risque cyber
- Objectifs de la mesure du risque en valeur financière
- Introduction au modèle FAIR (Factor Analysis of Information Risk)

2 / Fondamentaux du modèle FAIR

- Concepts de perte probable et fréquence d’événements
- Décomposition du risque en facteurs mesurables
- Méthodologie de calcul du risque financier

3 / Cartographie des actifs et scénarios de risque

- Identification des actifs critiques
- Construction de scénarios d’attaque réalistes
- Définition des événements de perte

4 / Évaluation des menaces et vulnérabilités

- Probabilité d’occurrence des menaces
- Exposition des systèmes et surfaces d’attaque
- Analyse des contrôles de sécurité existants

5 / Quantification des impacts financiers

- Coûts directs et indirects des incidents cyber
- Impact opérationnel, réputationnel et réglementaire
- Modélisation des pertes potentielles

Innov Systems

6 / Collecte et structuration des données de risque

- Sources de données internes et externes
- Qualité et normalisation des données de sécurité
- Construction de bases de données de risque

7 / Outils et frameworks de CRQ

- Solutions FAIR et plateformes CRQ
- Tableaux de bord et visualisation du risque
- Automatisation des calculs de risque

8 / Intégration de la CRQ dans la gouvernance

- Communication du risque aux dirigeants
- Alignement avec la stratégie d’entreprise
- Intégration dans les comités de risque

9 / Cas d’usage et scénarios avancés

- Simulation de cyberattaques majeures
- Analyse de portefeuille de risques cyber
- Priorisation des investissements sécurité

10 / Mise en œuvre d’un programme CRQ en entreprise

- Étapes de déploiement d’une démarche FAIR
- Industrialisation et amélioration continue
- Retours d’expérience et bonnes pratiques

Innov 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