

Formation ISO/IEC 27035 – Certified Lead Incident Manager

Code : NRE16

Durée : 5 jours

Classe : Présentiel / à distance

Public

- Gestionnaires des incidents de sécurité
- Responsables IT et cybersécurité
- Administrateurs systèmes et réseaux
- Professionnels de la sécurité de l'information

Prérequis

- Connaissances générales en sécurité de l'information
- Notions sur les normes ISO/IEC 27000

Objectifs

- Comprendre les principes de gestion des incidents SI
- Élaborer un plan de réponse aux incidents
- Identifier et analyser les menaces potentielles
- Améliorer les processus de gestion des incidents

Programme détaillé

1- Introduction aux concepts liés à la gestion des incidents de sécurité de l'information et à la norme ISO/IEC 27035

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts fondamentaux de la gestion des incidents
- Gestion des incidents de sécurité de l'information
- Établissement du contexte
- Politiques et procédures

2- Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- Management du risque
- Plan de gestion des incidents
- Équipe de gestion des incidents
- Relations internes et externes
- Assistance technique et autre
- Sensibilisation et formation aux incidents de sécurité de l'information

3- Détection et signalement des incidents liés à la sécurité de l'information

- Tests
- Surveillance des systèmes et des réseaux
- Détecter et alerter
- Collecte d'informations sur les incidents
- Signalement des événements liés à la sécurité de l'information
- Appréciation des événements liés à la sécurité de l'information

4- Surveillance et amélioration continue du processus de gestion des incidents liés à la sécurité de l'information

- Résolution des incidents liés à la sécurité de l'information
- Confinement, éradication et récupération
- Enseignements tirés
- Surveillance, mesure, analyse et évaluation
- Amélioration continue