

ISO 27035 – Foundation

Code : NRE22

Durée : 1 jour

Classe : Présentiel / à distance

Public

- Responsables sécurité (RSSI) et équipes de réponse aux incidents (ISIRT)
- Administrateurs systèmes et réseaux souhaitant maîtriser la gestion des incidents
- Auditeurs et consultants en sécurité de l'information
- Tout professionnel souhaitant acquérir les bases de la norme ISO 27035

Prérequis

- Avoir des notions de base en sécurité de l'information
- Une connaissance de la norme ISO 27001 est un plus
- Aucune certification préalable requise

Objectifs

- Comprendre les concepts et les enjeux de la gestion des incidents de sécurité
- Maîtriser les phases et les objectifs de la norme ISO 27035
- Mettre en place une équipe de réponse aux incidents (ISIRT)
- Détecter, analyser et répondre aux incidents de sécurité
- Appliquer les procédures de réponse immédiate et post-incident
- Identifier les catégories d'incidents et les méthodes de classification
- Comprendre les aspects légaux et réglementaires de la gestion d'incidents

Programme détaillé

1- Introduction à la gestion des incidents de sécurité

- Contexte et enjeux de la gestion des incidents de sécurité
- Lien avec la norme ISO 27035
- Vocabulaire et terminologie de la gestion des incidents

2- Norme ISO 27035

- Concepts fondamentaux de la norme ISO 27035
- Objectifs de la gestion structurée des incidents
- Bienfaits d'une approche structurée
- Phases de la gestion d'incident

3- Planification et préparatifs

- Principales activités d'une équipe de réponse aux incidents (ISIRT)
- Politique de gestion des incidents de sécurité
- Interactions avec d'autres référentiels et politiques
- Modélisation du système de gestion des incidents de sécurité
- Procédures et mise en œuvre de l'ISIRT
- Support technique et opérationnel
- Formation, sensibilisation et tests du système de gestion des incidents

4- Détection et rapport d'activité

- Activités de l'équipe opérationnelle de détection des incidents
- Détection d'événements de sécurité de l'information
- Rapport d'activité sur les événements détectés

5- Appréciation et prise de décision

- Activités de l'équipe opérationnelle d'analyse des incidents
- Analyse immédiate et décision initiale
- Appréciation et confirmation de l'incident de sécurité



ISO 27035 – Foundation

Code : NRE22

Durée : 1 jour

Classe : Présentiel / à distance

6- Réponses

- Principales activités de l'équipe opérationnelle de réponse aux incidents
- Réponse immédiate et réponse a posteriori
- Gestion des situations de crise
- Analyse inforensique et communication
- Escalade, journalisation de l'activité et gestion des changements

7- Mise à profit de l'expérience

- Principales activités d'amélioration de l'ISIRT
- Analyse inforensique approfondie
- Retours d'expérience post-incident
- Identification et amélioration : mesures de sécurité, gestion des risques, revue de direction

8- Mise en pratique

- Déni de service (DoS) et déni de service réparti (DDoS)
- Accès non autorisé
- Code malveillant (malware)
- Usage inapproprié
- Collecte d'informations
- Catégories d'incidents de sécurité
- Méthodes de classification : CVSS-ISO 27035
- Enregistrement des événements de sécurité
- Fiche de déclaration des événements de sécurité

9- Aspects légaux et réglementaires de la gestion d'incidents

- Obligations légales et réglementaires en matière de gestion des incidents
- Conformité et responsabilités juridiques
- Notification des incidents aux autorités compétentes

