Formation « Gestion des incidents de sécurité / ISO27035 »

Réf : ISO27035

La gestion des incidents de sécurité dans un délai court et leur prise en compte dans la gestion des risques et l'amélioration continue sont imposés par l'ISO 27001. Le processus de gestion des incidents de sécurité est un processus fondamental pour le succès d'une bonne organisation de la sécurité des systèmes d'information. Un guide, la norme ISO27035, explicite en détail comme organiser ce processus.

Objectifs

- **Comprendre et savoir mettre en œuvre concrètement dans son SMSI le processus de gestion des incidents de sécurité et une équipe de réponse aux incidents de sécurité (Information Security Incident Response Team : ISIRT)**
- **Comprendre et savoir gérer les interactions du processus de gestion des incidents de sécurité avec les autres processus dans son organisme, par exemple savoir différencier incident informatique et incident de sécurité.**
- **Apprendre à organiser son processus de gestion des incidents de sécurité.**

Durée & horaires

- **1 jour soit 7 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **DSI**
- **Personnes chargées de gérer les incidents de sécurité ;**
- **Personnes chargées de gérer les incidents au sens ITIL/ISO 20000 ;**
- **Responsables de la mise en place d'un SMSI.**

Pré-requis

- **Cette formation ne demande pas de pré-requis particuliers.**

Méthode pédagogique

- **Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.**

Supports

- **Support de cours au format papier en français**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

- Introduction
  - Contexte, Enjeux et ISO27001, Vocabulaire
- Norme ISO 27035
  - Concepts
  - Objectifs
  - Bienfaits de l'approche structurée
  - Phases de la gestion d'incident
- Planification et préparatifs (Planning and preparation)
  - Principales activités d'une équipe de réponse aux incidents de sécurité (ISIRT)
  - Politique de gestion des incidents de sécurité
  - Interactions avec d'autres éférentiels ou d'autres politiques
  - Modélisation du système de gestion des incidents de sécurité
  - Procédures
  - Mise en œuvre de son ISIRT
  - Support technique et opérationnel
  - Formation et sensibilisation
  - Test de sons système de gestion des incidents de sécurité)
- Détection et rapport d'activité (Detection and reporting)
  - Activités de l'équipe opérationnelle de détection des incidents de sécurité de l'information
  - Détection d'évènements
  - Rapport d'activité sur les événements
- Appréciation et prise de décision (Assessment and decision)
  - Activités de l'équipe opérationnelle d'analyse des incidents de sécurité
  - Analyse immédiate et décision initiale
  - Appréciation et confirmation de l'incident
- Réponses (Responses)
  - Principales activités d'une équipe opérationnelle de réponse aux incidents de sécurité
  - Réponse immédiate
  - Réponse à posteriori
  - Situation de crise
  - Analyse Inforensique
  - Communication
  - Escalade
  - Journalisation de l'activité et changement
- Mise à profit de l'expérience ('Lessons Learnt')
  - Principales activités d'amélioration de l'ISIRT
  - Analyse Inforensique approfondie
  - Retours d'expérience
  - Identification et amélioration
- Mise en pratique
  - Documentation
  - Exemple d'incidents de sécurité de l'information
  - Catégories d'incidents de sécurité
  - Méthodes de classement ou de typologie d'incidents de sécurité
  - Enregistrement des évènements de sécurité
  - Fiche de déclaration des évènements de sécurité
- Aspects légaux et réglementaires de la gestion d'incidents