G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

ISO27035 / Gestion des incidents de sécurité

But de la formation

- Mettre en oeuvre et organiser le processus de gestion des incidents de sécurité au sein d'un SMSI
- Comment mettre en place une équipe de réponse aux incidents de sécurité (Information Security Incident Reponse Team : ISIRT)
- Gérer et comprendre les interactions du processus de gestion des incidents de sécurité avec les autres processus de son organisation

Pré-requis

- Cette formation ne demande pas de pré-requis

Type de public

- DSI
- Responsables de la mise en place d'un SMSI
- Responsables sécurité
- Personnes chargées de gérer les incidents de sécurité

Moyens pédagogiques

- Support de cours en français au format papier

Sanction de la formation

- Cette formation n'est pas certifiante
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec échanges interactifs

Durée

7 heures (1 jour).

Programme

Introduction

- Contexte
- Enjeux et ISO 27001
- 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 référentiels ou d'autres politiques
- Modélisation du système de gestion des incidents de sécurité
- Procédures
- Mise en oeuvre de son ISIRT
- Support technique et opérationnel
- Formation et sensibilisation
- Test de son 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'événements
- 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
- de mesures de sécurité
- de la gestion des risques
- de la revue de direction
- du système de gestion des incidents

Mise en pratique

- Documentation
- Exemple d'incidents de sécurité de l'information
- Déni de service (DoS) et déni de service répar (DDoS)
- Accès non autorisé
- Code malfaisant

- Usage inapproprié
- Collecte d'informations
- Catégories d'incidents de sécurité
- Méthodes de classement ou de typologie d'incidents de sécurité
- CVSS
- ISO27035
- Enregistrement des événements de sécurité
- Fiche de déclaration des événements de sécurité

Aspects légaux et réglementaires de la gestion d'incidents