

Gestion des incidents de sécurité

Programme de la formation

Introduction

- Définitions
- Normes ISO
- Illustration d'incidents de sécurité

1. Organisation d'une capacité de gestion des incidents

- SOC & CERT
 - a. Composition et architecture
 - b. Compétences des acteurs
- Mise en place de la gestion des incidents
 - a. Création du processus de gestion d'incidents
 - b. Plans de mise en place
- Communication entre équipes et interdépendances
 - a. Formation et sensibilisation
 - b. Communication des équipes et importance du travail collaboratif

2. Gestion des incidents de sécurité

- Détection et analyse
 - a. Catégories d'incidents
 - b. Indicateurs | Détection | Priorisation
- Confinement, éradication et résilience
 - a. Cellule de crise
 - b. Confinement et stratégies de confinement
 - c. Rassembler les preuves
 - d. Éradiquer et nettoyer
- Communication
 - a. La communication pendant un incident
 - b. Données personnelles

3. Gouvernance et activités post-incident

- Plan et suivi post-incident
- Retours d'expérience
- Knowledge Sharing

Objectifs de formation

- Gérer et comprendre les interactions du processus de gestion des incidents de sécurité avec les autres processus de votre organisation.

Public

- RSSI | DSI
- Consultants sécurité, Chefs de projets
- Toute personne souhaitant acquérir les connaissances techniques

Pré-requis

- Connaître les fondamentaux de la sécurité de l'information

Méthodes pédagogiques

- Apports théoriques et pratiques
- Exercices
- Retours d'expérience

Livrables







- Support de cours en numérique

Langue

- Français

Suivi et Sanction

- Examen non certifiant en ligne
- Attestation de formation

					
Code CYB-A1	Durée 1 jour	Prix Inter 1150€ HT	3 à 10 stagiaires	▪ Inter ▪ Intra	▪ Présentiel ▪ À distance