

## Cybersécurité : Réponse aux incidents

### OBJECTIF DE FORMATION :

À l'issue de cette formation, le stagiaire saura identifier et analyser les attaques et mettre en place une réponse.

### OBJECTIFS PEDAGOGIQUES :

Être capable :

- ✓ Identifier des attaques.
- ✓ Comprendre des attaques.
- ✓ Gérer une réponse adaptée aux incidents.
- ✓ Mettre en place un plan de sécurité sur le long terme.

**DUREE** : 1 jour (7h)

#### DATES :

Sessions inter : Voir calendrier  
Sessions intra : A définir

**HORAIRES** : 9h à 17h

**LIEU** : Sur site ou dans nos locaux (Annecy et Chamonix) ou à distance

**EFFECTIF** : Jusqu'à 8 personnes.

### METHODES PEDAGOGIQUES :

Tour de table de positionnement préalable afin de permettre au formateur de vérifier l'adéquation du parcours de chaque stagiaire et d'adapter son déroulé pédagogique.

Le formateur aborde progressivement tous les points du programme en tenu compte du niveau des participants. Un bilan est effectué en fin de journée pour suivre la progression.

### PUBLIC CONCERNE :

Toute personne souhaitant savoir répondre aux incidents de cybersécurité en entreprise.

**PRE-REQUIS** : Avoir préalablement suivi la formation Cybersécurité : Starter

### MATERIEL :

- Ordinateur portable de stagiaire
- 1 salle de formation équipée Vidéoprojecteur, PC, paperboard
- Supports sur forme numérique

### ENCADREMENT :

La formation est dispensée par des formateurs expérimentés et possédants plusieurs années d'expérience de formations dans ce domaine.

### LE PLUS DE LA FORMATION :

- ✓ Intervenant expérimenté dans le domaine de la cybersécurité.
- ✓ Possibilité de faire la formation en présentiel ou en ligne, toujours avec un formateur.

# OURAGAN FORMATION

Email : [contact@ouragan-formation.fr](mailto:contact@ouragan-formation.fr)

Tél : 06 15 24 50 95



## PROGRAMME :

### Identifier et comprendre des attaques

- Identifier, analyser et hiérarchiser les exigences en matière de continuité des opérations (BC)
- Comprendre les méthodes des attaques cryptanalytiques
- Comprendre et respecter les enquêtes

### Gérer une réponse aux incidents

- Gérer les incidents
- Mettre en œuvre des stratégies de rétablissement
- Mettre en œuvre des processus de reprise après sinistre (DR = Disaster Recovery)
- Mise à l'essai des plans de reprise après sinistre (Disaster Recovery Plans)

### Mettre en place un plan de sécurité sur le long terme.

- Participer à la planification et aux exercices de continuité des activités (Business Continuity)
- Mettre en œuvre et gérer la sécurité physique
- Répondre aux préoccupations en matière de sécurité et de sûreté du personnel
- Mettre en œuvre et gérer les correctifs et les vulnérabilités

## EVALUATION :

Une évaluation à chaud sera conduite et permettra de mesurer le niveau de satisfaction immédiate du participant.

## VALIDATION :

Un certificat de réalisation seront remis au stagiaire à la fin de la formation.

## Bilan de fin de formation

***Pour les personnes en situation de handicap merci de prendre préalablement contact avec nous pour définir les modalités de votre participation à cette action de formation.***

*Mis à jour le 02 janvier 2024*