+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 30/05/2024

S'inscrire

Formation gestion de crise en CyberSécurité

4 jours (28 heures)

PRÉSENTATION

Notre formation exclusive "Gestion de crise en cybersécurité" vous permettra de répondre aux défis de la sécurité informatique. Ransomwares, phishings, injections SQL, les cybercriminels rivalisent s'inventivité pour mettre à mal la protection de votre infrastructure.

Notre programme de cours se composent de quatre parties essentielles pour comprendre et établir un plan de gestion de crise/risque en cybersécurité. Nous débuterons par une introduction à la sécurité informatique où nous reviendrons en détail sur les principaux concepts à maitriser que ce soit pour la protection des réseaux ou des applications.

Ensuite, nous préciserons la notion de "crise" "qu'est-ce qu'une crise ?" et "comment y remédier ?". Vous découvrirez alors les différents types de crises et comment les identifier. Nous mettrons l'emphase sur la création du plan de crise grâce l'évaluation des impacts, des métriques et des responsabilités.

Comme souvent, nous inclurons une partie pratique afin d'appliquer les concepts évoqués précédemment grâce à plusieurs exercices basés sur des scénarios réalistes.

OBJECTIFS

- Identifier les enjeux des risques de cybersécurité
- Comprendre les catégories de la cybersécurité
- Appréhender la typologie des outils de la cybercriminalité
- Connaître les fondamentaux de la gestion de crise
- Élaborer un plan de gestion de crise en cas de cyberattaque

PUBLIC VISÉ

- Chefs de projets sécurité informatiques
- Techniciens SSI

- Auditeurs
- RSSI / CISO
- Ingénieurs ou Administrateurs à haute criticité

Pré-requis

Connaissances de base en cybersécurité.

Programme de notre formation gestion de crise en CyberSécurité

Jour 1 - Les enjeux

- Les enjeux des risques de cybersécurité
  - Panorama des cybermenaces en France
  - Les enjeux
- Doctrine tripartite
  - La confidentialité
  - L'intégrité
  - La disponibilité
- Les catégories de la cybersécurité
  - La sécurité des réseaux
  - La sécurité des applications
  - La sécurité des informations
  - La sécurité opérationnelle
  - La résilience et la continuité des activités
  - L'acculturation et la formation des utilisateurs :
- Les risques
  - Qu'est-ce qu'un risque ?
  - Quelles sont les menaces les plus courantes ?
- La typologie des outils de la cybercriminalité
- Les bonnes pratiques de la cybersécurité

Jour 2 - Les fondamentaux de la gestion de crise

- Comprendre les fondamentaux de la gestion de crise
- Qu'est-ce qu'une crise ?
  - Incident
  - Accident
  - Situation d'urgence
  - Crise
- Qu'est-ce que la gestion de crise ?
  - Détection des incidents
  - Qualification
  - Escalade
  - Invocation du protocole de gestion de crise
- Processus d'invocation du protocole de crise

- Cellules de crise
  - Cellule de crise opérationnelle
  - Cellule de crise décisionnelle

Jour 3 - Le plan de gestion

- Formalisation d’un plan de gestion de crise en cas de cyberattaque
  - Métriques
  - Évaluation des impacts
  - Matrice RACI
  - Rôles et responsabilités
  - Canaux de communication
- Communication
  - Communication interne
  - Communication externe
  - Communication spécifique
- Scénarios de crise
  - Indisponibilité partielle du système d’information
  - Indisponibilité totale du système d’information
  - Perte d’une dépendance (effets de bords exogènes)
- Éléments clefs de rédaction du livrable

Jour 4 - Exercices

- Exercice de rédaction d’un protocole de gestion de crise
  - Travail en équipe à partir d’un scénario fourni
- Exercice de gestion de crise
  - Travail en équipe à partir de l’exercice précédent de rédaction d’un protocole de crise

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.