La cybersécurité pour les dirigeants

d'entreprise de taille moyenne ou intermédiaire

Formation labelisée SecNumedu-FC par l'ANSSI - Réf. 2505

La formation vise à permettre aux dirigeants d'entreprise de s'approprier les enjeux et les clés stratégiques de la sécurité numérique

Certification	• Aucune
Durée	• 1 ½ journée par mois soit 2 jours au total • A raison d'une ½ journée par mois
Inter entreprise	• 2.200 euros H.T
Intra entreprise	• Nous consulter
Taux de satisfaction	• N/A

Pré-requis	• Pré-requis : avoir réalisé le diagnostic de maturité cyber de l'entreprise avec l'outil 'Mon Aide Cyber' disponible via le lien suivant : https://monaide.cyber.gouv.fr • A noter – ADHEL est à même de pouvoir vous aider à réaliser ce pré-requis – contacter nous pour en savoir plus !
Public concerné	• Dirigeants d'entreprise de taille moyenne ou de taille intérmédiaire • Membre du Comité Executif, comité de direction
Nombre de stagiaires	• Minimum 8 et maximum 16
Délai d'accès au public	• 2 semaines à compter de la demande de formation • Pour les formations 'sur-mesure', deux entretiens préliminiaires sont proposés pour définir ensemble la session de formation souhaitée.
Compétences visées	• Etre à même de mesurer le risque numérique • Etre à même d'identifier les risques majeurs pour l'entreprise • Pouvoir identifier les actions prioritaires à metter en place • Savoir répondre aux exigences en termes de sécurité numérique • Savoir réagir en case de crise cyber
Méthode d'évaluation	• Evaluation sous la forme d'un questionnaire. Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant la formation.
Certificat de stage	• Attestation de fin de stage

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/

ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue

Cette certification ne vaut pas agrément de l'État.

Tests de certification	• Aucun
Références bibliographiques & sitographiques utilisés pour ce module de formation	• https://cyber.gouv.fr • https://cyber.gouv.fr/guides-essentiels-et-bonnes-pratiques-de-cybersecurite-par-ou-commencer
Méthodes pédagogiques	• Méthode affirmative connue aussi comme méthode magistrale (le formateur « dit ») • Méthode interrogative favorable aux échanges entre formateur et apprenants (le formateur « fait exprimer ») • Méthode démonstrative où se succèdent démonstrations et exercices de mise en oeuvre (le formateur « fait » et « fait faire »)
Débouché et suite du parcours	• Etre à même d'intégrer la gestion du risque cyber dans la gouvernnce de son organisation. • Etre à même de couvrir son risque cyber. • Réaliser des exercices de gestion de crise avec son équipe
Lieu	• Centre de Paris / Caen / Rouen • Seul le module 1 pourra éventuellement être réalisé en distanciel. Les autres modules se feront obligatoirement en présentiel. • Pour les apprenants réalisant le module 1 en distanciel, il est requis de disposer d'une connexion à internet ainsi que les outils permettant les interactions avec le reste du groupe et les formateurs (caméra, micro).
Nom de l'intervenant	• Expert en cybersécurité ayant une solide expérience
Eléments de biographie de l'intervenant	• Les éléments biographiques seront communiqués lors de l'inscription
Modalités d'accès	• Pour vous inscrire vous pouvez nous contacter à l'adresse suivante : contact@adhel.fr • Ou remplir le questionnaire ci-joint • Nous nous engageons à vous répondre dans les 48H

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/

ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue

Cette certification ne vaut pas agrément de l'État.

Contenu de la formation

KICK OFF : EXERCICE DE MISE EN SITUATION DE CRISE / SIMULATION / SERIOUS GAME - ½ journée soit 4 heures

OBJECTIF : Prendre conscience du risque numérique et connaître les divers modes d'attaques et leurs impacts

Introduction

Objectif : Poser le cadre, éveiller l'attention et mobiliser les participants

0.1. Mettre en situation

Présentation du scénario de simulation (fictif mais inspiré de cas réels)

Constitution des équipes / rôles (CEO, CISO, DRH, DAF, Communication...)

Réalisation de l'exercice de gestion de crise

0.2. Retour d'expérience à chaud

Bilan fictif : pertes estimées, impacts RH, image de marque, confiance

Tour de table : ressentis, surprises, erreurs, réflexes

0.3. Apport pédagogiques

Les spécificités de la gestion de crise cyber

Les différents modes d'attaque et leurs impacts

MODULE 1 MESURER LE RISQUE NUMÉRIQUE – ½ journée soit 4 heures

Objectif : Prendre conscience du risque numérique et connaître les divers modes d'attaques et leurs impacts.

Introduction

Objectif : adapter le cadre de la formation aux attentes des apprenants.

- Recueil des attentes des apprenants
- Règles et programme

1.1. Comprendre son activité numérique

Objectif : Prendre conscience de la dépendance au numérique de l'activité économique.

- Transformation numérique et nouvelle dépendance
- Introduction du concept de valeur métier et de biens Ms
- Cartographier son système d'information et son écosystème

1.2. Le risque numérique : êtes-vous une cible ?

Objectif : Comprendre l'économie de la malveillance numérique et des motivations des attaquants.

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/
ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue
Cette certification ne vaut pas agrément de l'État.

- La valeur de la donnée
- Attaque directe et contagion
- Les nouveaux champs de bataille

1.3. Les grands types de menace

Objectif : Connaître les différentes tactiques, techniques et procédures des attaquants.

- Notions de vulnérabilités et de chemins d'attaque
- Les motivations des attaquants
- Les événements redoutés

1.4. À quels impacts s'attendre ?

Objectif : Mesurer les impacts d'une attaque cyber sur l'activité de l'entreprise.

- Les différents impacts d'une attaque cyber (processus, gouvernance, physiques, financiers, réputationnels…)
- L'évolution des impacts (choc initial, souffle et répliques)

1.5. Construire ses scénarios de risque et définir son seuil d'acceptation

Objectif : Être en capacité de décrire au moins un risque critique dans toutes ses dimensions (valeur et bien support, scénario...).

- Identifier les événements redoutés et quantifier leur vraisemblance
- Identifier les scénarios critiques d'attaques cyber
- Quantifier l'impact de ces scénarios et définir son seuil d'acceptation

Mis à disposition en fin de séance : méthodologie et cadre d'étude du risque numérique

Rendu à la fin de la période d'autonomie : étude d'un risque critique

MODULE 2 S'ORGANISER ET PILOTER – ½ journée`soit 4 heures

OBJECTIF : Être en capacité de mettre en place une organisation adaptée aux risques cyber.

Introduction

- Retour sur l'étude de risque du processus critique sélectionné
- Responsabilités du dirigeant

2.1. Définir un cadre de gouvernance du risque numérique (amélioration continue)

Objectif : Piloter le risque cyber.

- Rôle des RSSI / référents cyber / conseillers cyber
- La politique de sécurité des systèmes d'information (PSSI)

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/
ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue
Cette certification ne vaut pas agrément de l'État.

- Les obligations réglementaires, les référentiels et la conformité (NIS2, RGPD, etc.)

2.2. Développer une culture de sécurité numérique

Objectif : Faire vivre la politique de sécurité numérique dans l'organisation.

- Placer l'humain au centre du jeu
- Former ses collaborateurs

2.3. Définir sa stratégie de sécurité numérique

Objectif : Construire ses objectifs de sécurité en fonction des risques.

- Définition des objectifs de sécurité
- Choix du référentiel
- Priorité à la sécurité ou à la résilience ?

2.4. Mettre en place des polices d'assurance adaptées

Objectif : Partager le risque cyber résiduel.

- Pourquoi assurer le risque cyber ?
- Comment choisir sa police d'assurance ?

Mis à disposition en fin de séance : Plan d'une PSSI et référentiels d'objectifs de sécurité

Rendu à la fin de la période d'autonomie : PSSI (chapitre « Objectifs »)

MODULE 3 BÂTIR SA SÉCURITÉ NUMÉRIQUE ET LA VALORISER - ½ journée soit 4 heures

Objectif : Mettre en place les mesures de sécurité adaptées et faire preuve de résilience en cas d'attaque ou de crise d'origine cyber.

Introduction

- Retour sur les PSSI
- Cadrage des objectifs de la demi-journée

3.1. Bâtir sa protection

Objectif : Construire le volet opérationnel de sa politique de sécurité.

- Construction d'un parcours progressif de sécurisation (du diagnostic initial à la conformité)
- Le choix des mesures de sécurité

3.2. Orienter sa défense

Objectif : Comprendre la nécessité de l'évolution des postures de sécurité.

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/
ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue
Cette certification ne vaut pas agrément de l'État.

• La veille (renseignement sur la menace et les vulnérabilités) : présentation des acteurs et solutions, intégration dans la posture de sécurité

• Anticiper sa réponse : les PRA et PCA

3.3. Faire preuve de résilience en cas de cyberattaque

Objectif : S'approprier les méthodes de gestion de crise d'origine cyber.

• La cellule de crise : composantes et dynamique

• Les relations avec l'écosystème (ACYMA, ANSSI, CERT régionaux ou sectoriels, CSIRT, autorités, assureurs)

• Le recours à des prestataires (PASSI, PAMS, PDIS, PRIS)

• L'entraînement et les exercices

3.4. Homologuer ses services numériques critiques

Objectif : Décrire les processus d'homologation et leur importance.

• Les référentiels de certification et d'homologation

• L'homologation, une expression de l'engagement raisonné du dirigeant

3.5. Valoriser ses investissements en sécurité numérique

Objectif : Souligner l'importance de la confiance numérique au sein de la chaîne de valeur.

- Le retour sur investissement : quantification financière du risque cyber
- Le développement de la confiance numérique : les preuves de confiance

Mis à disposition en fin de séance : référentiel de conformité NIS2

Rendu à la fin de la période d'autonomie : positionnement initial et stratégie de conformité (NIS2)

FIN DU DOCUMENT

CONTACT :

Mél: contact@adhel.fr

Tél. +33 6 60 26 27 48

https://adhel.fr

Organisme de formation certifiée Qualiopi au titre de la formation Qualopi

63 Rue Nationale - 92100 Boulogne Billancourt - SIRET – 88274050900014 - https://adhel.fr/

ADHEL est un organisme de formation enregistré sous le numéro 11922660392, agrée QUALIOPI au titre des actions de formation continue

Cette certification ne vaut pas agrément de l'État.