CONSEIL NATIONAL DES BARREAUX

LES AVOCATS

ECOA

ECOLE DU CENTRE OUEST DES AVOCATS

PROGRAMME RÉCAPITULATIF

QUELLES PRÉVENTION, ATTITUDE ET RÉPLIQUES FACE À UNE ATTAQUE CYBERCRIMINELLE ?

QUELLES PRÉVENTION, ATTITUDE ET RÉPLIQUES FACE À UNE ATTAQUE CYBERCRIMINELLE ?

PROGRAMME RÉCAPITULATIF

Modalités d'accès

Session ouverte du 1er janvier au 31 décembre 2024
Sur la plateforme 360LEARNING
Sur inscription auprès de l'EDA

Tarifs :

125 euros

Contacts / Accessibilité aux personnes handicapées

Référent « handicap » : Madame Delphine VANDEVILLE

Chaque témoignage vidéo fait l'objet d'un sous-titrage et d'une transcription vidéo permettant aux personnes malentendantes ou malvoyantes de suivre le parcours de formation.

Objectifs

À l'issue de ce second parcours, l'avocat apprenant :

- aura progressé dans la maîtrise de sa propre cyber sécurité,
- sera plus à l'aise pour aborder une conversation avec son client et comprendre la situation décrite,
- sera conceptuellement équipé pour affronter une situation de sinistre qui exigerait l'appui d'un binôme technique, tel qu'un expert judiciaire.

Prérequis

Être un professionnel du droit (avocat).
Avoir suivi intégralement le premier parcours de formation.

Thème traité, Spécialisation concernée

Cette formation concerne tous les praticiens (généralistes). Elle pourra notamment permettre aux avocats titulaires de la mention de spécialisation « Droit du numérique et des communications » de déclarer des heures de formation au titre de cette spécialisation.

Niveau

Le niveau d'enseignement, selon le schéma défini par la décision à caractère normatif du CNB, est le suivant (en gras) :

- Tout avocat
- Niveau 1 : débutant (acquisition des fondamentaux)
- **Niveau 2 : intermédiaire (approfondissement des connaissances et des pratiques)**
- Niveau 3 : avancé (s'adressant aux spécialistes et praticiens expérimentés)

Nombre d'heures de formation estimé

6 heures (travaux compris)

Séquences d'apprentissage / méthodes mobilisées / modalités d'évaluation

La formation se décompose en deux parcours indépendants :

- « Mieux connaitre l'écosystème de la cybersécurité » d'une part, et
- « Quelles prévention, attitude, répliques face à une attaque cybercriminelle ? », d'autre part.

Ce second parcours est composé de 11 modules :

- La mise en œuvre de la protection – mesures de protection techniques et organisationnelles (1/2) : solutions & moyens de protection
- La mise en œuvre de la protection – mesures de protection techniques et organisationnelles (2/2) : mesures recommandées pour toutes les entreprises, mécanismes de certification et mesures obligatoires
- La mise en œuvre de la protection : mesures juridiques
- Mise en place d'une cellule de crise, et rôle des parties prenantes
- Les bonnes pratiques de communication à l'écosystème
- Mesures techniques & juridiques
- Obligations consécutives à la survenance d'une attaque
- Le rôle des acteurs institutionnels dans la réaction
- La restauration du système ou des données et la résolution des problèmes
- La réparation du préjudice subi par l'entreprise victime de l'attaque
- Cas pratique

Chaque séquence fait l'objet d'une évaluation des acquis grâce à des quiz de validation (questionnaires à choix multiples et/ou à réponses multiples, mises en situation, etc.). Pour passer à la séquence suivante, 70 % minimum de réussite aux quiz est nécessaire (exercice bloquant jusqu'à l'atteinte d'un pourcentage de réponses satisfaisantes). Ainsi, vous pourrez vérifier si vous avez correctement assimilé les connaissances.

Une synthèse finale interactive finale vous permet de retenir les informations essentielles.

Au total, comptez 30 à 35 minutes par module en moyenne pour le réaliser dans de bonnes conditions d'apprentissage.

Le premier parcours fait l'objet d'une session distincte ouverte du 1er janvier au 31 décembre 2024.

Date de dernière mise à jour des modules : janvier 2024

Personnes ayant conçu et animant la formation

Cette formation a été conçue par la société MAKE U LEARN et par EEEI (Institut européen de l'expertise et de l'expert) pour le compte du Conseil national des barreaux.

Les personnes animant la formation sont les suivantes :

- Myriam Quéméner, magistrate, experte auprès du Conseil de l'Europe en matière de cybercriminalité
- Nicolas Barbazange, expert de justice en informatique près la Cour d'appel de Limoges
- Jean-Sylvain Chavanne, ancien délégué régional de l'ANSSI, expert en conseil en cyberdéfense
- Laurence Clayton, expert de justice en informatique près la Cour d'appel de Versailles
- Nicolas Herzog, avocat au barreau de Paris
- Antoine Laureau, expert de justice en informatique près la Cour d'appel de Versailles
- Christophe Roger, avocat au barreau du Havre
- Perrine Salagnac, avocate au barreau de Paris
- Sophie Soubelet, avocate au barreau de Paris
- Camille Tack, avocate au barreau de Paris

Modalités d'assistance

Le forum d'échanges sur la plateforme 360Learning qui héberge le parcours permet de poser des questions à un référent. Ce dernier répondra dans les meilleurs délais.

Modalités de sanction de la formation

Questionnaire anonyme d'évaluation de la formation

Remise par l'EDA d'une attestation de fin de formation :

- faisant état du nombre d'heures de formation suivies ;
- indiquant que la formation s'est déroulée conformément aux modalités de mise en œuvre arrêtées par le Conseil national des barreaux ;
- spécifiant que les critères de prise en charge 2024 du FIF PL ont été respectés dans la mise en œuvre de la formation.