2020

Programme de formation

L’avocat et la cybersécurité

Side Quest

Une question sur le programme ? Besoin de précisions ? Besoin d’une prise en charge particulière ?
Contactez notre responsable pédagogique : thibault@side-quest.io

Document remis au stagiaire avant son inscription

(Article L 6353-8 du Code du Travail)

Les ressources et contenus de la formation sont régulièrement mises à jour. La date du programme correspond également à la date de dernière mise à jour de la formation. V1 11/2020

side quest

L’avocat et la cybersécurité

Objectifs (professionnels)

A l’issue de la formation, le stagiaire sera capable de :

- ✔ Comprendre la définition et les modalités des cyber attaques dites opportunistes
- ✔ Comprendre la définition et les modalités des cyber attaques dites ciblées
- ✔ Découvrir les grandes tendances de la cybercriminalité
- ✔ Connaître les principales autorités impliquées dans la cybersécurité au niveau national et européen
- ✔ Connaître les grands principes du droit applicables à la cybersécurité
- ✔ Connaître les principes d’hygiène de base pour protéger son cabinet
- ✔ Apprendre les bases de la gestion de crise
- ✔ Comprendre les enjeux de la préservation de la preuve numérique
- ✔ Connaître les domaines dans lesquels l’avocat peut intervenir pour développer une offre de service en matière de cybersécurité

Public

Le public concerné est : tous les avocats inscrits et exerçants sur le territoire Français.

Pré-requis

Les conditions d’accès sont :

- Pré-requis : avoir le statut d’avocat car la formation donne des compétences applicables à la pratique de l’avocat.

- Niveau exigé : Cette formation s’adresse aux niveaux débutants et moyens en matière de cybersécurité.

Durée

Cette formation se déroulera en 5h, en e-learning.

La formation est accessible à tout moment par l’apprenant, une fois régulièrement inscrit. Il peut, à tout moment mettre en pause puis reprendre le parcours. Il dispose d’une durée de trois mois pour terminer la formation.

Dates : La formation est accessible à partir du 02 novembre 2020, pour une durée minimum de 3 ans.

Tarif

Cette formation est dispensée pour un coût de 150€ HT, soit 180€ TTC (TVA 20%).

side quest

Modalités et délais d'accès

L'inscription est réputée acquise lorsque l'apprenant a payé l'intégralité de la formation et a signé la convention.

Moyens pédagogiques, techniques et d'encadrement

Méthodes et outils pédagogiques

Méthodes pédagogiques : Magistrale et Démonstrative.

Outils pédagogiques : Vidéos, Screencast, animations, exercices pratiques, QCM..

Supports pédagogiques : A l'issue de la formation, l'apprenant reçoit un document au format PDF lui permettant d'appliquer au quotidien les savoir transmis.

Prise en compte du handicap : 100% en ligne avec rythme modulable, scriptes à disposition des apprenants si nécessaire, aménagements supplémentaires possibles sur demande avec étude au cas par cas.

Contacter le référent handicap : thibault@side-quest.io

Eléments matériels de la formation

Supports techniques : formation 100% en ligne via la plateforme side-quest, créée avec Learnybox.

Équipements devant être amenés par l'apprenant : l'apprenant doit avoir un ordinateur, tablette ou smartphone ainsi qu'une connexion internet pour accéder au portail de la formation.

Documentation : Liste de ressources complémentaires délivrées au cours de la formation, support pédagogique livré en fin de formation.

Compétences des formateurs

La formation sera assurée par Jean-Sylvain Chavanne diplômé de droit et ingénieur en informatique.

Voir CV.

Formation ouverte ou à distance FOAD

Cette formation est exclusivement prodiguée à distance.

Le stagiaire doit suivre l'ensemble des vidéos en intégralité pour valider la formation, il doit également répondre aux questions intermédiaires (entre les modules) ainsi qu'aux questions en fin de partie. Le temps prévu par partie est indiqué dans le plan ci-dessous.

Des ressources complémentaires sont mises à disposition de l'apprenant, il n'est pas obligatoire de les consulter pour valider la formation.

La formation est réalisée via la plateforme , l'apprenant peut à tout moment solliciter l'équipe pédagogique de side quest pour une assistance technique (dans les limites de nos capacités en ce qui concerne la plateforme) ou pédagogique ou pour toute autre question liée au contenu de la formation (Responsable Thibault Oudotte).

L'apprenant peut nous contacter par email (thibault@side-quet.io), par téléphone (07 66 49 18 76), via notre site internet (side-quest.io) ou encore via les réseaux sociaux. Le délai de réponse maximum est de 48h.

Contenu (🔷 = Quizz)

Introduction :

- ***Présentation de la structuration générale de la formation***
- ***Présentation des modalités d'assistance et d'accompagnement***
- ***Présentation du sujet***

PARTIE 1 : Les cyber attaques opportunistes

- ✔ Comprendre la définition des cyber attaques dites opportunistes
- ✔ Comprendre les modalités des principales cyber attaques dites opportunistes

Capsule 01. Le phishing 🔷
Capsule 02. Les rançongiciels
Capsule 03. Les fuites de données
Capsule 04. La défiguration de site internet 🔷

PARTIE 2 : Les cyber attaques ciblées et la cybercriminalité

- ✔ Comprendre la définition des cyber attaques dites ciblées
- ✔ Comprendre les modalités des principales cyber attaques dites ciblées
- ✔ Comprendre la structuration du Web
- ✔ Découvrir les grandes tendances de la cybercriminalité

Capsule 01. Les attaques ciblées
Capsule 02. Les attaques en déni de service
Capsule 03. Les intrusions physiques
Capsule 04. Les attaques "Man in the middle"
Capsule 05. Les attaques APT 🔷
Capsule 06. Les différentes couches du Web
Capsule 07. Exemple de mode opératoire : TV5 monde
Capsule 08. Typologie des attaquants
Capsule 09. Le coût d'une cyberattaque 🔷

PARTIE 3 : Autorités compétentes

- ✔ Connaître les principales autorités impliquées dans la cybersécurité au niveau national et européen

Capsule 01. *L'organisation française en matière de cybersécurité* 🔹

Capsule 02. *L'ANSSI* 🔹

Capsule 03. *Le maillage territorial de lutte contre la cybercriminalité* 🔹

Capsule 04. *L'organisation européenne en matière de cybersécurité* 🔹

PARTIE 4 : Le contexte réglementaire lié à la cybersécurité

- ✔ Connaître les grands principes du droit applicables à la cybersécurité

Capsule 01. *Le droit pénal*

Capsule 02. *Le RGPD* 🔹

Capsule 03. *Les obligation sectorielles*

Capsule 04. *Les SAIV*

Capsule 05. *Les OSE* 🔹

PARTIE 5 : Principes de base pour protéger son cabinet

- ✔ Connaître les principes d'hygiène de base pour protéger son cabinet
- ✔ Savoir les mettre en place

Capsule 01. *Auditer la surface d'attaque*

Capsule 02. *Gestion des mots de passe* 🔹

Capsule 03. *Les outils juridiques*

Capsule 04. *Les outils techniques*

Capsule 05. *Gérer le nomadisme* 🔹

Capsule 06. *Gestion des échanges par mail*

PARTIE 6 : Les principes de base de la gestion d'une crise cyber

- ✔ Apprendre les bases de la gestion de crise
- ✔ Comprendre les enjeux de la préservation de la preuve numérique

Capsule 01. *La gestion d'une crise numérique*

Capsule 02. *Préserver la preuve numérique*

Capsule 03. *Porter plainte* 🔹

PARTIE 7 : Accompagner son client

- ✔ Connaître les domaines dans lesquels l'avocat peut intervenir pour développer une offre de service en matière de cybersécurité

Capsule unique : Comment accompagner votre client en matière de cybersécurité ?

🔹 **QUIZZ GÉNÉRAL** 🔹

Suivi et évaluation

Exécution de l'action

Les moyens permettant de suivre l'exécution de l'action sont inclus dans la plateforme, ils permettent d'attester le suivi du parcours par l'apprenant ainsi que sa participation aux quizz et exercices.

Modalités d'évaluation des résultats (ou d'acquisition des compétences)

Pour déterminer si l'apprenant a acquis les connaissances fixées dans les objectifs, on se base sur des QCM et des exercices d'application en ligne, avec correction automatique.