

FORMATION RÉFÉRENT CYBERSÉCURITÉ EN TPE/PME

Vous souhaitez vous prémunir des risques liés à la sécurité (piratages, vol d'informations stratégiques, ...) de votre entreprise ?

La Chambre de Commerce et d'Industrie Nice Côte d'Azur vous accompagne pour être en mesure d'initier et de pérenniser au sein de la TPE/PME la démarche de prévention en matière de cybersécurité visant à préserver et protéger son patrimoine immatériel d'actes d'hostilité, dans le respect de la règlementation.

LES POINTS FORTS :

- ✓ Une formation certifiante pour devenir référent cybersécurité
- ✓ Une démarche adaptée aux TPE/PME, tenant compte de leur environnement juridique et technologique
- ✓ Une approche opérationnelle pour passer de l'identification des risques à la construction d'un plan d'action
- ✓ Un diagnostic de votre niveau de sécurité pour mieux cibler les priorités
- ✓ Un plan d'action personnalisé directement transposable dans votre entreprise
- ✓ Une vision globale de la cybersécurité, associant prévention, réglementation et protection du patrimoine immatériel.

INDICATEURS DE SATISFACTION ANNÉE 2024 :

Taux de satisfaction : 100% **Taux de reusite : 100%**

CCI NICE CÔTE D'AZUR

Au cœur de votre histoire

Les objectifs de la formation :

À l'issue de la formation, vous serez en mesure de :

- Identifier les principaux risques cyber auxquels votre entreprise peut être exposée
- Analyser votre environnement juridique et technologique
- Identifier les vulnérabilités et les besoins de sécurisation de votre TPE/PME
- Évaluer le niveau de sécurité de votre entreprise
- Définir les actions prioritaires à mettre en œuvre
- Construire un plan d'action cybersécurité adapté à votre activité
- Initier et pérenniser une démarche de prévention au sein de votre entreprise
- Contribuer à la protection du patrimoine immatériel et des informations stratégiques de votre organisation

Le programme de la formation :

Module 1 :

- Identifier la problématique de cybersécurité propre à l'entreprise en tenant compte de son environnement juridique et technologique
- Décrire l'organisation les enjeux et les objectifs de la cybersécurité
- Identifier les aspects juridiques de la réglementation
- Identifier les obligations et responsabilités du chef d'entreprise sur son SI
- Gérer les risques juridiques
- TP Sécurité WEB, découverte et exploitation de vulnérabilités sur les sites internet (injections SQL, faille XSS,...) et compréhension des contre-mesures.

Module 2 :

- Évaluer le niveau de sécurité de son entreprise
- Décrire l'organisation les enjeux et les objectifs de la cybersécurité
- Identifier les aspects juridiques de la réglementation
- Identifier les obligations et responsabilités du chef d'entreprise sur son SI
- Gérer les risques juridiques
- TP Sécurité WEB, découverte et exploitation de vulnérabilités sur les sites internet (injections SQL, faille XSS,...) et compréhension des contre-mesures.
- Connaître les responsabilités juridiques liées à la gestion d'un SI
- Construire une méthodologie de résilience de l'entreprise
- Traiter et recycler le matériel informatique en fin de vie
- TP Hacking, prise en main d'outils offensifs pour se mettre dans la peau d'un hacker, et exploitation de la faille des EternalBlue pour prendre la main sur une machine vulnérable (Kali Linux, Metasploit,...).

Module 3 :

- Mettre en œuvre la cybersécurité : construire son plan d'action
- Lister les métiers directement impactés par la cybersécurité
- Lister les différents métiers de prestation informatique
- Construire une méthodologie pédagogique pour responsabiliser et diffuser les connaissances et les bonnes pratiques
- Construire une méthodologie d'évaluation du niveau de sécurité
- Actualiser le savoir du référent cyber sécurité
- Classer les formes d'externalisation
- Choisir les prestataires de service

Cible

- Toute personne en charge d'assurer la cybersécurité au sein de son entreprise (soit dirigeant, cadre, référent ou responsable informatique, responsable SI, responsable réseau voire administrateur système /réseau etc.)
- Demandeurs d'emploi

Pré-requis

- Disposer des connaissances de base concernant l'informatique
- Justifier d'un titre ou diplôme de Niveau 5 OU d'une expérience professionnelle de 3 ans minimum
- Remplir un questionnaire de positionnement du stagiaire

Durée

- 35h sur 5 jours
- 9h-17h
- Présentiel

Modalités d'évaluation

Une épreuve écrite (cas de mise en situation) de 3h - 100 points

Moyens et outils pédagogiques

- Un positionnement est effectué en amont de l'action de formation
- Tous les points abordés sont illustrés au travers de mises en situation réelles ou fictives
- Examen de certification prévu en fin de formation

Les livrables

- Support de formation
- Boite outils cybersécurité

Inscription

- Pour mobiliser votre Compte Personnel de Formation (CPF), consultez : *https://www.moncompteformation.gouv.fr/espace-prive/html/#/*
- Autrement contactez-nous à : *intelligence-eco@cote-azur.cci.fr*

Tarif

- Coût total de la formation : 3300 € HT / participant soit 3960€ TTC
- Possibilité de prise en charge par France Travail, CPF, fonds de formation

Intervenants

Consultant formateur, expert dans le domaine en cybersécurité : Société Onyl Rocks

Accessibilité aux personnes en situation de handicap

Informations pratiques

Contactez la CCI Nice Côte d'Azur pour vous prémunir des risques liés à la sécurité : intelligence-eco@cote-azur.cci.fr

Retrouvez toute l'actualité économique, l'agenda et les événements business sur notre site internet : www.cote-azur.cci.fr

20 Bd Carabacel - 06005 Nice | 04 93 13 73 00 | allocci@cote-azur.cci.fr

CPF ENTREPRISE DE FORMATION RESPECTANT LA CHARTE DE DÉONTOLOGIE

Cette offre de formation est éligible à MON COMPTE FORMATION

CCI NICE CÔTE D'AZUR

Au cœur de votre histoire

Septembre 2026