PÔLE FORMATION
DU PAYS D'ARLES

FORMATION CERTIFIANTE, FORMATION CYBERSÉCURITÉ • NUMÉRIQUE

CYBERSÉCURITÉ – ARLES

LIEU	DURÉE	PRIX
4 avenue Victor Hugo 13200 Arles	3 jours / 21 Heures	CPF / OPCO

Objectifs de la formation

- Connaitre et comprendre les enjeux de la cyber sécurité
- Comprendre les enjeux de la cyber sécurité
- Identifier les risques juridiques autour de la cyber sécurité
- Connaitre et comprendre les principaux types d'attaques et leurs conséquences
- Identifier les outils de protection

Ce module de formation permet de présenter les bases de la cyber sécurité. Il permettra de comprendre les problématiques et les enjeux de la sécurité informatique, d'identifier ses différents acteurs, ainsi que de comprendre son organisation. Il sert d'introduction aux modules avancés en Cyber sécurité.

Nature de la formation

Action de formation cybersécurité.

Prérequis

Aucun, avoir suivi le MOOC de l'ANSSI constitue un plus.

ModalitéS pédagogiques

La formation est dispensée sous forme d'ateliers collectifs et individuels.
Formation présentielle (Exposés, cas pratiques, synthèse)

Programme

MODULE OBLIGATOIRE

INTRODUCTION ET ESSENTIELS

S'intégrer au groupe en formation, s'engager sur une charte de bonnes pratiques en formation, s'approprier les objectifs et contours de la formation, appréhender les modalités pédagogiques proposées et les outils mobilisables.

Définitions

- Intelligence économique, sécurité économique globale

Cybersécurité (*Sécurité des SI (prévention) + Cyberdéfense (réaction) + Cybercriminalité (sanction)*
= Cybersécurité)
Les enjeux de la sécurité des SI

- La nouvelle économie de la cybercriminalité

Les déficiences en matière de cybersécurité peuvent engendrer des pertes financières directes ou indirectes (comme lorsqu'un site marchand est rendu indisponible ou lors d'espionnage économique sur des appels d'offres, par exemple).

DATES DE RÉALISATION

Pour plus d'informations, nous consulter.
Prochaines sessions.
04 décembre 2023
05 décembre 2023
06 décembre 2023
07 décembre 2023
D'autres dates sont à venir.

DÉLAI D'ACCÈS

15 jours avant le début de la formation.

MODALITÉ D'ACCESSIBILITÉ POUR LES PERSONNES EN SITUATION DE HANDICAP

Le PFPA est particulièrement sensible à l'intégration des personnes en situation de Handicap. Prenez contact avec notre **Référent Handicap M. MOZOL** (s.mozol@pfpa-formations.com) afin d'étudier les possibilités de compensations et/ou aménagements disponibles.

PUBLICS

Tous chef d'entreprise ou salarié souhaitant se former aux fondamentaux de la cybersécurité.

VALIDATION

Remise du **Diplôme ANSSI** à l'issue de cette formation.

Site internet

- Panorama des menaces selon une typologie

Panel assez large des différentes menaces (attaques intrusives – injection SQL, passive – phishing, destructrices – virus, etc.). Détails sur les Advanced Persistent Threat (APT, Attaque persistante avancée) : rôle des entreprises dans ces attaques.

- Les vulnérabilités (exemples, détermination, veille)

Vulnérabilité : faiblesse d'un bien, que ce soit à la conception, la réalisation, l'installation, la configuration ou l'utilisation.

- Focus sur l'ingénierie sociale

Les propriétés de sécurité.

- Présentation du principe de défense en profondeur

Un logiciel spécialisé dans la cybersécurité n'est pas suffisant. La démarche de cybersécurité s'inscrit dans un processus global de sécurité économique (sécurité bâtimentaire, sécurisation des déplacements, contrôle d'accès, etc.).

- Identification et évaluation des actifs et des objectifs de sécurité

Arriver à identifier précisément le besoin :

Un site internet marchand et un site internet « vitrine » n'ont pas les mêmes besoins en termes de sécurité.

Déterminer les critères (disponibilité, intégrité, confidentialité, preuve / traçabilité) qui permettent d'évaluer le niveau de sécurité des SI.

Aspects juridiques et assurantiels

- Responsabilités

Quelles sont les responsabilités des entreprises qui n'ont pas assez sécurisé leurs SI ? Quels recours sont possibles vers les prestataires ?

Réglementation européenne : analyse de risque obligatoire pour une entreprise dès qu'il y a une déclaration à la Commission nationale de l'informatique et des libertés (CNIL).

- Préservation de la preuve

Que faire en cas d'attaques informatiques ?

Comment préserver la preuve tout en restant opérationnel ? Qui faut-il contacter ?

Le rôle de l'huissier.

- L'offre assurantielle

Le paysage institutionnel de la cybersécurité

- La prévention

Rôle et missions des acteurs étatiques en charge de l'accompagnement des entreprises en matière de cyber.

- Le traitement des cyberattaques et la réponse judiciaire

L'agence nationale de la sécurité des systèmes informatiques (ANSSI), la Direction générale de la sécurité intérieure (DGSI), la Gendarmerie nationale, etc.

- Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers

L'ANSSI, la Direction centrale de la police judiciaire, sous-direction de la lutte contre la cybercriminalité (SDLC-OCLCTIC), la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), la gendarmerie nationale (C3N, NTECH), etc.

- Connaître le système d'information et ses utilisateurs

Faire une cartographie des SI de l'entreprise.

- Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes…)

Connaître la valeur des informations contenues dans son ordinateur pour appliquer les différentes procédures de sécurité en fonction des documents utilisés.

- Maîtriser le réseau de partage de documents (en interne ou sur internet)

Identifier précisément les passerelles qui existent entre internet et le réseau interne pour éviter les failles qui permettront ou faciliteront une intrusion non détectée.

- Mettre à niveau les logiciels

Définir une véritable politique de mise-à-jour des logiciels (qui est en charge ? À quel moment ? etc.).

- Authentifier l'utilisateur

Présentation des différentes méthodes permettant d'authentifier les utilisateurs et ainsi de leur attribuer la méthode qui correspond le mieux aux documents qu'ils utilisent.

Évoquer les bonnes pratiques pour les mots/phrases de passe (conception, fréquences d'utilisation, etc.).

- Nomadisme – Problématiques liées au BYOD (Bring your Own Devices)

Évoquer les risques liés à l'utilisation des terminaux mobiles personnels (PC et/ou Smartphone) dans la chaîne de sécurité de l'entreprise.

Présentation des publications/recommandations

- Guides de l'ANSSI
- Recommandations de la CNIL
- Recommandations de la police et de la gendarmerie
- Club de la Sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF/CESIN), etc.
- Observatoires zonaux de la Sécurité des systèmes d'information (SSI).
    - Les CERTs (*Computer Emergency Response Team*)

Il s'agit ici de sensibiliser les PME à l'importance de la veille sur les différentes documentations

disponibles.

Présentation des différents métiers de l'informatique (infogérance, hébergement, développement,

juriste, etc.)

Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)

Insister sur les messages que le référent en cybersécurité doit transmettre aux utilisateurs finaux des entreprises. Présenter le principe des chartes informatiques que chaque utilisateur doit connaitre.

Maîtriser le rôle de l'image et de la communication dans la cybersécurité

- Surveillance de l'e-réputation
- Communication externe
- Usage des réseaux sociaux, professionnel et personnel
- Méthodologie d'évaluation du niveau de sécurité

Présentation d'un audit de sécurité (réglementation, avantages, coût etc.).

- Actualisation du savoir du référent en cybersécurité

Les découvertes en matière de cybersécurité sont nombreuses, rapides et les méthodes d'attaques évoluent en permanence. Il est donc nécessaire que le référent en cybersécurité connaisse les grandes actualités du domaine.

- Gérer un incident / Procédures judiciaires

Identifier clairement le point de contact dans l'entreprise ainsi que son rôle (lien avec les services de police, résilience du SI de l'entreprise etc.).

CONTACT
Directeur - Sébastien MOZOL.
4, avenue Victor Hugo • 13200 Arles • 04 90 96 01 19 • info@pfpa-formations.com

Site internet