Catalogue de formations Cybersécurité – Sensibilisations

Chaque formation de ce catalogue peut être contextualisée à vos activités et adaptée en fonction du public (RSSI, non informaticiens, utilisateurs n'utilisant pas de poste informatique au quotidien, RH, Comptables…). Conçu de manière modulaire, vous pouvez construire votre formation sur-mesure en choisissant les modules de ce catalogue.

CYBERWINGS ACADEMY

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13

CYBERWINGS ACADEMY

Les menaces du cyber-espace

Cette session vous permettra d'appréhender les différents moyens utilisés par les cybercriminels pour exploiter les vulnérabilités de votre système d'information et compromettre ainsi vos données sensibles.

OBJECTIFS PÉDAGOGIQUES

- Appréhender les principales menaces informatiques.
- Comprendre les modes opératoires des cybercriminels.
- Connaître les bonnes pratiques de protection.

PROGRAMME

Introduction

Les impacts d'une cyber-attaques

La sécurité des SI et les données sensibles

Les différentes étapes d'une attaque

Démonstration de prise d'accès sur un système d'information à travers plusieurs vulnérabilités

Les bons réflexes au quotidien

Détecter un mail de type phishing

Le choix des mots de passe

L'utilisation des réseaux sociaux

Hygiène numérique : protection des données, mises à jour des systèmes, bonnes pratiques sur les réseaux sociaux

Ref : SSI-S-001

Séminaire

2 heures

PUBLIC :

Tout public utilisant les outils numériques de manière pro ou perso

PARTICIPANTS :

De 3 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

Inter-entreprises : à partir de 290 € HT / pers.

Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
19 mai 2025
27 juin 2025
26 septembre 2025
7 novembre 2025

Session maintenue à partir de 3 inscrits

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Les menaces du cyber-espace

Cette session vous permettra d'appréhender les différents moyens utilisés par les cybercriminels pour exploiter les vulnérabilités de votre système d'information et compromettre ainsi vos données sensibles.

OBJECTIFS PÉDAGOGIQUES

- Appréhender les principales menaces informatiques.
- Comprendre les modes opératoires des cybercriminels.
- Connaître les bonnes pratiques de protection.
- Comprendre le contexte juridique

PROGRAMME

Introduction

Les impacts d'une cyber-attaques
La sécurité des SI et les données sensibles

La sécurité informatique : comprendre les menaces et les risques

Système d'information, Cyber-espace, Internet : quels liens ?
Qu'entend-on par sécurité Informatique ?
La gestion des la sécurité par les risques : Menaces, impacts, vulnérabilités
Les objectifs de la sécurité : Confidentialité, disponibilité, intégrité, traçabilité
Qu'est-ce qu'une cyber-attaque ?
La typologie de la cyber-criminalité : différence entre hacker, cyber-criminels, escrocs, opportunistes et menaces étatiques
L'équipe de sécurité du système d'information et les stratégies d'entreprise.

Comprendre le contexte juridique de la sécurité

Données à caractère personnel, données à caractère personnel sensibles, données sensibles et stratégiques
RGPD et rôle de la CNIL
Les acteurs de la sécurité en France

Comprendre l'utilité d'un mot de passe fort

Qu'est-ce que l'authentification ? Pourquoi ce thème est important dans la cyber-sécurité ?
Exemple de cassage de mots de passe
Qu'est-ce qu'un mot de passe fort ?
L'intérêt de la double authentification et les solutions
Les bonnes pratiques et l'utilisation d'un gestionnaire de mot de passe

Protéger vos données

Pourquoi maîtriser vos informations sur l'Internet ?
Qu'est-ce qu'un leak ? Comment réagir face à une fuite de données ?
Exemple d'escroquerie
Qu'est-ce que l'ingénierie sociale ?
L'utilisation de l'IA dans tout çà ?
Introduction au chiffrement et un exemple avec vos solutions métiers
Les sauvegardes
Les bonnes pratiques au quotidien pour protéger vos données et détecter de l'ingénierie sociale

Hygiène numérique

Qu'est-ce qu'un logiciel malveillant ? Qu'est-ce qu'un ransomware ? Utilité des anti-virus
Qu'est-ce que le phishing et comment le détecter ?
Pourquoi mettre à jour son système ?
Pourquoi ne pas faire confiance aux périphériques USB ?
Pourquoi ne pas prêter sa session ?
Que faire en cas de compromission ?
Comment bien naviguer sur Internet (Cookie, navigation privée...) ?
La protection des poste

Nomadisme

Définition de l'IoT et technologies sans fil
Les risques du wifi
Risques de partage de connexions
Risques en mobilité
Bonnes pratiques et utilité du VPN

Conclusion

Bonnes pratiques au quotidien

Ref : SSI-S-001-SPE

Séminaire

1 journée

PUBLIC :

Tout public utilisant les outils numériques de manière pro ou perso

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

Inter-entreprises : à partir de 890 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
19 mai 2025
27 juin 2025
26 septembre 2025
7 novembre 2025
Session maintenue à partir de 3 inscrits

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Protection des données personnelles

Cette formation vous permettra de comprendre la réglementation autour de la protection des données à caractère personnel et d'appliquer dans votre quotidien les règles de bonnes pratiques.

OBJECTIFS PÉDAGOGIQUES

- Comprendre ce qu'est l'identité numérique et les risques liés.
- Connaître les bonnes pratiques à mettre en œuvre au quotidien, dans sa vie personnelle et professionnelle pour protéger ses données.
- Connaître les gestes essentiels en cas de fuite de données.

PROGRAMME

Comprendre le contexte

Qu'est-ce qu'une identité numérique ?

Pourquoi le RGPD ?

Rappel du rôle de la CNIL

Qu'est-ce qu'une donnée à caractère personnel, une donnée sensible selon la CNIL ?

Les bonnes pratiques au quotidien

Comprendre ce qu'est un risque en cybersécurité : Vulnérabilités / Menace / Impacts

Qu'est-ce que l'ingénierie sociale ?

Reconnaître un phishing/vishing vous demandant des données personnelles

La gestion des mots de passe

La veille sur votre identité numérique

Utilisation de l'IA et protection des données

Autres recommandations dans la vie professionnelle : conservation des données, cloisonnement ...

Fuite de donnée, que faire ?

Je suis victime d'une fuite ou d'une attaque sur mon identité numérique : porter plainte / déclaration à la CNIL

Mon entreprise est victime d'une fuite de données : les premiers gestes, gestion des cyber-crises (cellule de crise, plan de communication)

Que dit la loi ?

Ref : SSI-S-002

Séminaire

1/2 journée

PUBLIC :

Tout public utilisant les outils numériques de manière pro

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

Inter-entreprises : à partir de 490 € HT / pers.

Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
20 mai 2025
26 juin 2025
22 septembre 2025
6 novembre 2025

Session maintenue à partir de 3 inscrits

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Ransomware : comment s'en protéger

Cette session vous permettra d'appréhender les différents moyens utilisés par les cybercriminels pour propager les rançongiciels et d'appliquer les bonnes pratiques pour s'en prémunir.

OBJECTIFS PÉDAGOGIQUES

- Comprendre le mode opératoire d'un ransomware
- Connaître les bonnes pratiques pour s'en prémunir
- Connaître les gestes essentiels en cas d'attaque réussie

PROGRAMME

Comprendre ce qu'est un ransomware

Qu'est-ce que le chiffrement ?

Qu'est-ce qu'un logiciel malveillant ?

Ramsomware : mode opératoire, les vulnérabilités exploitées par les ransomwares

Se prémunir des ransomwares

Comprendre ce qu'est un risque en cybersécurité : Vulnérabilités / Menace / Impacts

Cartographie du SI / Inventaire des données numériques dans l'entreprise, classement par sensibilité

Veille (CVE…) et mises à jour : pourquoi, quand, comment ?

Cloisonnement SI (réseau, utilisateur...)

Les bonnes pratiques pour partager un fichier

PCA/PRA et plans de sauvegarde

Antivirus / EDR / Firewall / Proxy / Durcissement des configurations

Que faire en cas de cyber-crise ?

L'importance de la détection

Processus de gestion d'incident (comment je gère un incident, comment je sais si c'est grave ?)

Les premiers gestes

Gestion des cyber-crises (cellule de crise, plan de communication, déclencher mon PCA)

Le rôle de l'ANSSI / porter plainte / déclaration à la CNIL

Payer ou ne pas payer ?

L'assurance cyber

Ref : SSI-S-004

Séminaire

1/2 journées

PUBLIC :

Tout public utilisant les outils numériques de manière pro ou perso

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

Inter-entreprises : à partir de 390 € HT / pers.

Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
20 mai 2025
26 juin 2025
22 septembre 2025
6 novembre 2025

Session maintenue à partir de 3 inscrits

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Le vocabulaire de la cyber-sécurité

Ce séminaire vous proposera un panorama du vocabulaire de la cyber-sécurité en replaçant les termes dans leur contexte.

OBJECTIFS PÉDAGOGIQUES

- Connaître les principales menaces informatiques.
- Comprendre l'utilité des principales solutions de sécurité.

PROGRAMME

Les principaux éléments du vocabulaire de la « cyber »

Qu'est-ce que l'identité numérique ?
DCP et Données sensibles
Menaces / Impacts / Risques / Vulnérabilités
Intégrité, confidentialité, disponibilité, traçabilité
Les principes de « sécurité » en informatique
Le contexte légal

Les menaces

Les phases d'une attaque
Vocabulaire des menaces sur le réseau
Vocabulaire des menaces sur les applications et systèmes
L'ingénierie sociale et son vocabulaire
BYOD, Cloud, télétravail, IoT et les nouveaux vecteurs d'attaques
CVE, CWE, CVSS

Les protections

Protections des données : chiffrement, hachage, signature
Vocabulaire lié à la sécurité des applications
Protection des postes : Antivirus / EDR / Firewall / Durcissement des configurations
Protection du réseau : Firewall / Proxy / SIEM / SOC / NIDS

Ref : SSI-S-005

Séminaire

1/2 journées

PUBLIC :

Tout public désirant s'initier au langage des experts sécurité

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

Inter-entreprises : à partir de 490 € HT / pers.

Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
20 mai 2025
26 juin 2025
22 septembre 2025
6 novembre 2025

Session maintenue à partir de 3 inscrits

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Les fondamentaux de la sécurité numérique en entreprise

Cette formation de 2 jours est conçue en 7 modules indépendants de 2 heures et adaptés à un parcours introductifs aux bonnes pratiques numériques en entreprise pour tous.

OBJECTIFS PÉDAGOGIQUES

- Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles
- Identifier les mesures de protection de l'information et de sécurisation de son poste de travail
- Favoriser la conduite de la politique de sécurité SI de l'entreprise
- Comprendre le contexte juridique et comprendre les mesures liées à ce contexte à appliquer

PROGRAMME

MODULE 1 – Comprendre les menaces et les risques

Système d'information, Cyber-espace, Internet : quels liens et dans quels contextes d'utilisation ?

Qu'entend-on par sécurité Informatique ?

La gestion des la sécurité par les risques : Menaces, impacts, vulnérabilités

Les objectifs de la sécurité : Confidentialité, disponibilité, intégrité, traçabilité

Qu'est-ce qu'une cyber-attaque ?

La typologie de la cyber-criminalité : différence entre hacker, cyber-criminels, escrocs, opportunistes et menaces étatiques

L'équipe de sécurité du système d'information et les stratégies d'entreprise.

MODULE 2 – Comprendre le contexte juridique et normatif de la sécurité

Données à caractère personnel, données à caractère personnel sensibles, données sensibles et stratégiques

RGPD et rôle de la CNIL

Autres lois : NIS2, DORA, CRA …

Les acteurs de la sécurité en France

Liens avec les systèmes de management de la sécurité et plus particulièrement ISO 27001

MODULE 3 – Comprendre l'utilité d'un mot de passe fort

Qu'est-ce que l'authentification ? Pourquoi ce thème est important dans la cyber-sécurité ?

Exemple de cassage de mots de passe

Qu'est-ce qu'un mot de passe fort ?

L'intérêt de la double authentification et les solutions

Les bonnes pratiques et l'utilisation d'un gestionnaire de mot de passe

Ref : SSI-S-009

Séminaire

2 jours, soit 14h

PUBLIC :
Tout public utilisant l'outil numérique

PARTICIPANTS :
De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :
- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :
- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :
À partir de 1590 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :
Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Les fondamentaux de la sécurité numérique en entreprise

Cette formation de 2 jours est conçue en 7 modules indépendants de 2 heures et adaptés à un parcours introductifs aux bonnes pratiques numériques en entreprise pour tous.

PROGRAMME - SUITE

MODULE 4 – Protéger vos données

- Pourquoi maîtriser vos informations sur l'Internet ?
- Qu'est-ce qu'un leak ? Comment réagir face à une fuite de données ?
- Exemple d'escroquerie
- Qu'est-ce que l'ingénierie sociale ?
- L'utilisation de l'IA dans tout çà ? Quelles bonnes pratiques à appliquer ?
- Introduction au chiffrement et un exemple avec 7Zip
- Les sauvegardes
- Les bonnes pratiques au quotidien pour protéger vos données et détecter de l'ingénierie sociale

MODULE 5 – Hygiène numérique

- Qu'est-ce qu'un logiciel malveillant ? Qu'est-ce qu'un ransomware ? Utilité des anti-virus
- Qu'est-ce que le phishing et comment le détecter ?
- Pourquoi mettre à jour son système ?
- Pourquoi ne pas faire confiance aux périphériques USB ?
- Pourquoi ne pas prêter sa session ?
- Que faire en cas de compromission ?
- Comment bien naviguer sur Internet (Cookie, navigation privée…) ?

MODULE 6 – Nomadisme

- Définition de l'IoT et technologies sans fil
- Les risques du wifi
- Risques de partage de connexions
- Risques en mobilité
- Bonnes pratiques

MODULE 7 – Vocabulaire autour de la protection

- Qu'est-ce qu'un pare-feu firewall et quel est son rôle dans l'entreprise ?
- Qu'est-ce qu'un proxy et quel est son rôle dans l'entreprise ?
- Les différents moyens de protection sur votre poste : EPP, EDR, firewall
- L'utilité d'un VPN dans un cadre professionnel et privé

Ref : SSI-S-009

Séminaire

2 jours, soit 14h

PUBLIC :
Tout public utilisant l'outil numérique

PARTICIPANTS :
De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :
À partir de 1590 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :
Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Se préparer à une cybercrise

Ce séminaire vous aidera à appréhender une situation de crise-cyber.

OBJECTIFS PÉDAGOGIQUES

- Savoir définir et mettre en œuvre une procédure de gestion de crise adaptée et personnalisée
- Connaître les référentiels et les autres méthodes

PROGRAMME

Qu'est-ce qu'une cyber-crise ?

Évènement / incident / crise
Particularités de la crise d'origine cyber
Les référentiels

Anticiper l'avènement d'un risque grave

Apprécier le risque cyber
Prévenir l'avènement d'une crise
Sensibiliser et entraîner

Formaliser et tester une procédure de gestion de crise

Les différentes cellules de crise
Définir un BPMN de crise
Outils et méthodes pour une gestion de crise efficace

Gérer une crise cyber

Qualification
Mobilisation
Communication
Résolution

L'amélioration continue de la procédure de gestion de crise

RETEX
Amélioration continue des processus liés à la gestion des risques
Veiller et s'informer sur l'évolution de la menace

Ref : SSI-S-007

Séminaire

1 jour, soit 7 heures

PUBLIC :
Dirigeants, RSSI, RPCA/RPRA

PARTICIPANTS :
De 2 à 6 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations, mise en situation pratique,

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :
À partir de 890 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :
Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

CYBERWINGS ACADEMY

Directive NIS2 : comprendre et se préparer

Ce séminaire vous permettra de comprendre la directive NIS2 qui s'inscrit dans un cadre réglementaire étendu visant à renforcer la sécurité numérique sur le marché européen, particulièrement dans les secteurs fortement tributaires des technologies de l'information.

OBJECTIFS PÉDAGOGIQUES

- Faire un état des lieux de la situation de son entreprise versus les obligations NIS2
- Élaborer un plan d'actions de mise en conformité à NIS2
- Améliorer votre capacité à évaluer et à atténuer les risques cyber

PROGRAMME

État de la Menace et des Impacts Cyber en Europe

Les tendances actuelles en matière de cybermenaces et les attaques récentes.

La directive NIS1 et champ d'application initial

Notion d'incidents significatifs et obligation de sécurité

NIS2 – Contenu de la directive

Périmètre des Entités Concernées : Répartition, Annexe 1 2, Critères de classification des entreprises, (tailles, secteurs et autres critères), Cas particuliers.

Entités essentielles (EE) et Entités Importantes (EI), définition et responsabilités des EE et EI

Exigences spécifiques pour les opérateurs de services numériques de confiance

Récapitulatif des obligations de sécurité renforcées

Gestion des incidents et coopération entre les états membres et l'Enisa

Les nouvelles obligations de déclaration d'incident

Les risques financiers en cas de non-respect

Coopération avec les autorités compétentes et mécanismes de communication

Préparation à la conformité

Étapes pratiques pour se conformer à la NIS2

Ressources et références

Atelier pratique sur un scénario concret lié à la mise en œuvre de la NIS2

Panorama des bonnes pratiques

Ref : SSI-S-008

Séminaire

1 jour, soit 7 heures

PUBLIC :
Dirigeants, RSSI, RPCA/RPRA, DSI

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : Aucun

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations, mise en situation pratique,

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 90 % de bonnes réponses)
- Évaluation de satisfaction de fin de formation
- Attestation de fin de formation précisant les modules acquis et en cours d'acquisition
- Support de cours remis au cours de la session

TARIF :

À partir de 730 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Sur demande

Animation

Nos experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par notre équipe pédagogique tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine.

Comment financer votre formation ?

Vous êtes salarié

Votre formation est financée par votre entreprise ou pas des fonds gérés par les OPCO via :

- le plan de développement des compétences
- les actions collectives ou clé en main
- les dispositifs étatiques en cours
- une dotation sur votre CPF si formation certifiante

Vous êtes travailleur non salarié *

Votre formation peut être financée par :

- les fonds d'assurance formation (FAF)
- votre CPF si formation certifiante
- vos fonds propres

** Dirigeant, président, profession libérale, autoentrepreneur*

Vous êtes demandeur d'emploi

Votre formation peut être financée par :

- l'aide individuelle à la formation (AIF)
- l'aide individuelle régionale vers l'emploi (AIRE)
- votre région
- votre CPF si formation certifiante
- vos fonds propres

Votre démarche est personnelle

Vous êtes salarié mais vous souhaitez financer votre formation sans passer par votre entreprise ?

Vous pouvez utiliser :

- votre CPF si formation certifiante
- vos fonds propres

OPCO opérateurs de compétences · France Travail · MON COMPTE FORMATION · Ministère du Travail, de l'Emploi et de l'Insertion – FNE Formation

Modalités d'accès

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint.

Nos locaux sont accessibles aux Personnes à Mobilité Réduite.
Pour les personnes en situation d'handicap, vous pouvez contacter notre référente handicap au 07 52 05 10 68 ou à l'adresse inclusion@cyberwings.fr.

Nos conseillers sont disponibles pour vous accompagner dans toutes vos démarches. Nous sommes en mesure de mobiliser les expertises, les outils nécessaires pour vous accueillir, vous accompagner et vous former.

Qualiopi processus certifié – RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

CYBERWINGS ACADEMY

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13

Qui sommes-nous ?

Cyberwings Academy

Cyberwings Academy est le fruit de l'évolution du département Formation de l'entité Cyberwings, capitalisant sur plus de 20 années d'expérience dans le hacking éthique et le management de l'information stratégique.

Nos experts

Nos experts qui animent la formation sont des spécialistes des matières abordées. Nous tenons en effet à cette dénomination « d'experts » formateurs dans la mesure où ces hommes et femmes sont avant tout des professionnels passionnés par leur activité, fort d'expériences variées, significatives et mises à profit de nos stagiaires.

Nos thèmes pédagogiques

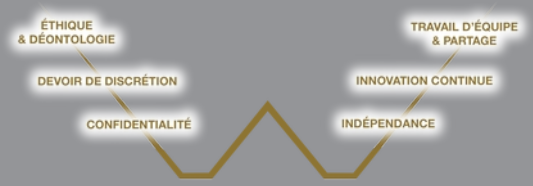
Techniques

- Hacking
- Techniques défensives
- Détection d'intrusions
- Réseaux informatiques
- Linux
- Cryptographie
- Blue / Red team
- Windows expertise
- ...

Non techniques

- Sécurité de l'information
- Secret des affaires
- Données personnelles
- Intelligence économique
- OSINT
- Cyber-stratégies
- Guerre de l'information
- ....

Nos valeurs



Les labels du groupe

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'actions suivantes :
ACTIONS DE FORMATION

CYBERWINGS ACADEMY

Cyberwings Academy – 565 Avenue du Prado, 13008 Marseille - www.cyberwings.academy
RCS Marseille 98413556600011 – **APE** 8559A – Numéro Activité Formation : 93 13 22155 13