Catalogue de formations Cyber-Sécurité – Sécurité Défensive

Ces stages pratiques vous permettent une vision complète de l'état de l'art en matière de sécurité défensive.
Conçus de manière modulaire, vous pouvez construire votre formation sur-mesure en choisissant les modules de ce catalogue.
Toutes ces formations peuvent se réaliser en mode séminaire avec des démonstration à la place des travaux pratiques.

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

Sécu Défensive

Les fondamentaux de la sécurité

Cette session de 5 jours vous permettra d'appréhender les principaux risques sur vos réseaux et systèmes. Elle vous permettra de mettre en œuvre les principales mesures de sécurité.

OBJECTIFS PÉDAGOGIQUES

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Mettre en œuvre les principaux moyens de sécurisation des réseaux

PROGRAMME

Introduction

Le contexte de la cyber-sécurité, les acteurs
Les impacts d'une cyber-attaque
Menaces, vulnérabilités et impacts et analyse de risque
Les différentes étapes d'une attaque

La sécurité réseau

Panorama des principales attaques : MiTM, interception, DoS, attaques sur les DNS, Attaques SNMP ...
La sécurité du LAN : vlans, NAC, architecture 802.1x, fonctionnalités du switch ...
La sécurité externe : Pare-feu et Proxy, Sécurité du Cloud
Sécurité des réseaux sans-fil dont Wi-Fi

La sécurité des échanges et des données

Panorama des principales attaques
Introduction à la cryptographie : chiffrement, PKI, hachage
Échanges sécurisés : VPN, TLS, SSH
Administration sécurisée
IAM, gestion des accès, authentification

La sécurité des postes et serveurs

Panorama des principales attaques, malveillants, vulnérabilités des applications (CVS, CWE, CVSS), quelques vulnérabilités sous environnement Microsoft (AD, Kerberos…), post-exploitation, reverse engineering
Protection des postes : Contrôleurs d'intégrité, Solution antivirale et EPP/EDR, V.D.S
Durcissement : bonnes pratiques Windows et Linux
Introduction à l'Intégration de la Sécurité dans les Projets
La sécurité dans les projets d'IA

Conclusion

Les bonnes pratiques au quotidien

TRAVAUX PRATIQUES

Mise en place d'une architecture sécurisée à partir des thèmes abordés.

Ref : SSI-D-001

Stage Pratique

5 jours, soit 35 heures

PUBLIC :

Informaticiens, équipe DSI

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : bases en système et réseau : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et des TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 2 990 € 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

Sécu Défensive

Les fondamentaux de la sécurité

Ce séminaire de 3 jours vous permettra d'appréhender les principaux risques sur vos réseaux et systèmes. Il vous permettra de comprendre les principales mesures de sécurité à travers de démonstration.

OBJECTIFS PÉDAGOGIQUES

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Connaître les principaux moyens de sécurisation des réseaux

PROGRAMME

Introduction

Le contexte de la cyber-sécurité, les acteurs
Les impacts d'une cyber-attaque
Menaces, vulnérabilités et impacts et analyse de risque
Les différentes étapes d'une attaque

La sécurité réseau

Panorama des principales attaques : MiTM, interception, DoS, attaques sur les DNS, Attaques SNMP ...
La sécurité du LAN : vlans, NAC, architecture 802.1x, fonctionnalités du switch ...
La sécurité externe : Pare-feu et Proxy, Sécurité du Cloud
Sécurité des réseaux sans-fil dont Wi-Fi

La sécurité des échanges et des données

Panorama des principales attaques
Introduction à la cryptographie : chiffrement, PKI, hachage
Échanges sécurisés : VPN, TLS, SSH
Administration sécurisée
IAM, gestion des accès, authentification

La sécurité des postes et serveurs

Panorama des principales attaques, malveillants, vulnérabilités des applications (CVS, CWE, CVSS), quelques vulnérabilités sous environnement Microsoft (AD, Kerberos…), post-exploitation, reverse engineering
Protection des postes : Contrôleurs d'intégrité, Solution antivirale et EPP/EDR, V.D.S
Durcissement : bonnes pratiques Windows et Linux
Introduction à l'Intégration de la Sécurité dans les Projets
La sécurité dans les projets d'IA

Conclusion

Les bonnes pratiques au quotidien

DÉMONSTRATIONS

Le séminaire sera accompagné de démonstrations.

Ref : SSI-D-001-B

Séminaire

3 jours, soit 21 heures

PUBLIC :

Informaticiens, équipes DSI

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : bases en système et réseau : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 2 390 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
Du 7 juillet au 9 juillet 2025
Du 16 au 18 septembre 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

Sécu Défensive

De la protection à la détection

Cette formation de 5 jours vous permettra d'implémenter une architecture permettant de détecter les intrusions. Elle abordera la notion de SOC.

OBJECTIFS PÉDAGOGIQUES

- Comprendre ce qu'est un SOC.
- Comprendre les principales attaques pour mieux les détecter.
- Connaître les bonnes pratiques dans la gestion des LOG.

PROGRAMME

Audit et sécurité au quotidien

Principes de sécurité
Approche normative et analyse de risque
Supervision, audit, test de sécurité

Comprendre les principales attaques réseau

Panorama des attaques : MiTM, ARP Spoofing, DoS …
Sniffing et analyse des trames réseau : wireshark, tshark et autres outils …
Mise en place de moyen de détection simple

L'importance de la détection

Stratégie de sécurisation
La gestion des événements de sécurité et des cyber-crises
Qu'est-ce qu'un SOC ?
Les outils du SOC
Focus sur la détection antivirale sur les postes et les NIDS
Utilisation de la matrice ATT&CK et des IoC
Introduction au forensic

La gestion des Log

Le log management
Les SIEM
Log et contexte réglementaire
Quelques outils : SEC, Syslog, SNMP, Wazuh, ELK

Conclusion

Un exemple d'infrastructure de supervision et les bonnes pratiques

TRAVAUX PRATIQUES

Mise en place d'une architecture de détection à partir des thèmes abordés.

Ref : SSI-D-002

Stage Pratique

5 jours, soit 35 heures

PUBLIC :

Informaticiens, équipe DSI

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : connaître les principales méthodes défensives (avoir réalisé le cours SSI-D-001 avec Cyberwings Academy) ou avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 3 490 € 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

De la protection à la détection

Ce séminaire de 2 jours vous permettra de comprendre l'implémentation d'une architecture permettant de détecter les intrusions. Il abordera la notion de SOC.

OBJECTIFS PÉDAGOGIQUES

- Comprendre ce qu'est un SOC.
- Comprendre les principales attaques pour mieux les détecter.
- Connaître les bonnes pratiques dans la gestion des LOG.

PROGRAMME

Audit et sécurité au quotidien

Principes de sécurité
Approche normative et analyse de risque
Supervision, audit, test de sécurité

Comprendre les principales attaques réseau

Panorama des attaques : MiTM, ARP Spoofing, DoS …
Sniffing et analyse des trames réseau : wireshark, tshark et autres outils …
Mise en place de moyen de détection simple

L'importance de la détection

Stratégie de sécurisation
La gestion des événements de sécurité et des cyber-crises
Qu'est-ce qu'un SOC ?
Les outils du SOC
Focus sur la détection antivirale sur les postes et les NIDS
Utilisation de la matrice ATT&CK et des IoC
Introduction au forensic

La gestion des Log

Le log management
Les SIEM
Log et contexte réglementaire
Quelques outils : SEC, Syslog, SNMP, Wazuh, ELK

Conclusion

Un exemple d'infrastructure de supervision et les bonnes pratiques

DÉMONSTRATIONS

Le séminaire sera accompagné de démonstrations.

Ref : SSI-D-002_B

Séminaire

2 jours, soit 14 heures

PUBLIC :

Informaticiens, équipe DSI

PARTICIPANTS :

De 2 à 12 pers. max
Pré-requis : connaître les principales méthodes défensives (avoir réalisé le cours SSI-D-001 ou SSI-D-001-B avec Cyberwings Academy) ou avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 1 390 € 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

La gouvernance de la cyber-sécurité

Ce séminaire de 3 jours très riche vous présentera l'ensemble des actions et des solutions permettant d'assurer la sécurité de votre SI d'un point de vue gouvernance : de l'analyse des risques à la mise en œuvre optimale de solutions de sécurité.

OBJECTIFS PÉDAGOGIQUES

- Maîtriser le processus de gouvernance de la sécurité
- Utiliser les référentiels métiers et les normes associées de la série ISO 27K
- Connaître le cadre juridique français et européen (LPM, NIS, RGPD, …)

PROGRAMME

Les fondamentaux de la sécurité du système d'information

Actifs processus/information et Actifs en support
La classification DICT/P
Les acteurs incontournables (ANSSI, ENISA, CNIL ...)

Les cadres normatifs et réglementaires

L'approche par la conformité.
Directive NIS/ Loi Programmation Militaire.
La norme ISO 27001 dans une démarche système de management (roue de Deming/PDCA).
La norme ISO 27002, la connaissance minimale indispensable.
Élaborer un Plan d'Assurance Sécurité dans sa relation client/fournisseur.
Focus sur les DCP et le RGPD
L'utilité de la charte d'utilisation du SI

Le processus d'analyse des risques

Identification et classification des risques
Connaître des méthodes pré définies : approche FR/EBIOS RM, approche US/NIST, etc.

Le rôle du RSSI

Le rôle et les responsabilités du RSSI / CISO, la relation avec la DSI.
Les profils d'architectes, intégrateur, auditeurs, pen-testeurs, superviseurs, risk manager, etc.
La gestion de projet au quotidien
Rôle du RSSI dans le SOC
Les projets structurants : PCA/PRA, PKI, IAM …
Le coût de la sécurité

Conclusion

Cas d'étude Ebios RM
Cas d'étude charte utilisateur

Ref : SSI-D-003

Séminaire

3 jours, soit 21 heures

PUBLIC :

Chefs de projet, DSI, RSSI

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 : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 2 390 € HT / pers.
Devis personnalisé : nous consulter

PROCHAINES SESSIONS :

Classe virtuelle :
Du 7 juillet au 9 juillet 2025
Du 16 au 18 septembre 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 bases de la cryptographie

Ce stage pratique de 3 jours présente les différentes techniques cryptographiques ainsi que les principales applications. Les méthodes de chiffrements, le hachage, les algorithmes les plus utilisés ainsi que les méthodes de gestion des clés seront expliqués en détail.

OBJECTIFS PÉDAGOGIQUES

- Maîtriser le vocabulaire associé à la cryptologie : algorithme, hachage, clé
- Connaître les algorithmes les plus utilisés en cryptologie
- Utiliser des outils de chiffrement symétrique et asymétrique

PROGRAMME

Introduction

Protection des données
Qu'est-ce que la cryptographie
Les applications de la cryptographie
Histoire de la cryptographie

Le chiffrement

Chiffrement symétrique vs Chiffrement asymétrique
Quelques algo de chiffrement symétrique : RC4, DES, 3DES, AES, CHACHA20
Quelques algo de chiffrement asymétrique : RSA, ElGamal, courbes elliptiques
L'échange de clé, Diffie-Hellman, EDH
Chiffrement par flux ou par bloc
MAC dans le chiffrement
Introduction à la cryptanalyse

Intégrité et authentification

Principe du hachage
Quelques algorithmes : MD5, SHA (SHA-1, SHA-2 et SHA-3), les fonctions Bcrypt, Scrypt, Argon
HMAC, le sel dans le hachage
Principe des signatures et quelques algorithmes (DSA, ECDSA ...)
Cassage des hash

PKI et certificats

Les certificat X509
Norme PKIX
Architecture, solution technique

Conclusion

Utilité au quotidien de la cryptographie
L'avenir de la cryptographie et la cryptographie post-quantique

TRAVAUX PRATIQUES

Chaque concept sera illustré par un TP ou un cas pratique en démonstration.

Ref : SSI-D-004

Stage Pratique

3 jours, soit 21 heures

PUBLIC :

Informaticiens, équipe DSI

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : bases en système et réseau : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 2 090 € 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

Sécu Défensive

Cryptographie avancée

Ce stage pratique de 4 jours présente les différents concepts de la cryptographie moderne et vous permettra de mieux comprendre l'intérêt de la cryptographie post-quantique.

OBJECTIFS PÉDAGOGIQUES

- Maîtriser les concepts avancés de la cryptographie, y compris les courbes elliptiques, le chiffrement homomorphe et la cryptographie post-quantique.
- Comprendre et appliquer les notions de forward secrecy, post compromise security et les méthodes de multisignatures.
- Utiliser des outils avancés de chiffrement et de signature.
- Analyser et évaluer la sécurité des protocoles cryptographiques modernes.

PROGRAMME

Méthodes de chiffrement et de hachage

Rappel sur les algorithmes de hachage : SHA, BLAKE
Dérivation de clés : HKDF, PBKDF, ChaCha20
Chiffrement hybride : AEAD (ChaCha20-Poly1305)

Méthodes de signature et échange de clés

Rappels des notions de PKI (Public Key Infrastructure), défis et les meilleures pratiques
Rappels sur les signatures numériques, algorithmes et vérification/validation des signatures
Forward Secrecy (FS) et Post Compromise Security (PCS) : Définition, importance, et implémentation
Key Schedules et ratchets : Ratchetting, et Double Ratchet Alrogithm (DRA)
Méthodes de multisignatures et secret sharing : Schnorr, BLS, et SSS
Méthodes d'échanges de clés : PAKE, SPEKE, GKE, MQV
Nouveaux standards : MLS, TreeKEM, GHTree

Les courbes elliptiques

Équations de Weierstrass et d'Edwards
Algorithmes de signatures basés sur les courbes elliptiques (ECDSA et EdDSA)
Chiffrement avec les courbes elliptiques : ECIES
Attaques spécifiques sur les courbes elliptiques

Chiffrement homomorphe et preuves à divulgation nulle de connaissance

Full Homomorphic Encryption (FHE), algorithmes et applications
Partial Homomorphic Encryption (PHE), algorithmes et applications
Définition et importance des ZKP, types et applications

Cryptographie post-quantique

Introduction à la cryptographie post-quantique
Menaces posées par les ordinateurs quantiques
Algorithmes résistants aux attaques quantiques
Nouveaux standards de la NIST
Algorithmes de chiffrement et de signature post-quantique

Étude de cas

Protocole de l'application Signal (synthèse de toute la formation)
Présentation de l'application Signal
Analyse du protocole de Signal

TRAVAUX PRATIQUES

Chaque concept sera illustré par un TP ou un cas pratique en démonstration.

Ref : SSI-D-008

Stage Pratique

4 jours, soit 28 heures

PUBLIC :

Informaticiens, équipe DSI

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : bases en cryptographie : avoir 80 % de bonnes réponses à notre QCM d'entrée ou avoir suivi le cours SSI-D-004.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, travaux pratiques et démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 3 090 € 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

La sécurité des applications Web

Cette formation de 4 jours vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre site web et intégrer les principes de sécurité dans les développements orientés web.

OBJECTIFS PÉDAGOGIQUES

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Mettre en place des mesures de sécurisation simples pour les applications Web

PROGRAMME

Introduction

Les vecteurs d'attaque sur les applications Web
L'OWASP et le TOP 10 de l'OWASP
Rappel de l'utilisé des équipements de sécurité
Réglementation applicables sur les applications Web

Les principales attaques

Présentation des plateformes et outils dvwa, bwapp, burp suite, sqlmap, fimap ...
Exposition de données sensibles
XSS (Cross Site Scripting)
Csrf (cross site request forgery)
Injections SQL, LDAP, PHP, HTML ...
Api non protégée
Références directes non sécurisées à un objet
Mauvaise configuration de sécurité

Les protections

Protections des mots de passe : chiffrement, hachage,
Protection du code par signature
L'utilité du Reverse-Proxy et du WAF
L'Intégration de la sécurité dans les projets

Les bonnes pratiques

Compréhension des différentes protections autour des architectures client-serveur (csp, x-frame, hsts, httponly, secure cookie)
Rappel du fonctionnement de TLS

TRAVAUX PRATIQUES

Chaque concept sera illustré par un TP ou un cas pratique en démonstration.

Ref : SSI-D-005

Stage Pratique

4 jours, soit 28 heures

PUBLIC :

Développeurs Web, chef de projets et administrateurs système

PARTICIPANTS :

De 2 à 6 pers. max
Pré-requis : bases en développement web : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective, mise en situation pratique, démonstrations

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz et TP, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 2 890 € 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

Intégrer la sécurité dans les développements

Ce séminaire de 2 jours vous apprendra les connaissances nécessaire pour renforcer la sécurité de vos développement et mieux appréhender les concepts de DevSecOp et d'ISP.

OBJECTIFS PÉDAGOGIQUES

- Maîtriser les bonnes pratiques de sécurité à toutes les phases de développement
- Intégrer la sécurité dans la méthode agile
- Mettre en place les outils adéquats dans votre cycle de développement
- Promouvoir une culture de sécurité au sein des équipes de développement

PROGRAMME

Introduction

La philosophie Agile
Le framework SCRUM : l'essentiel
La culture DEVOPS : les principes
Objectifs de sécurité : confidentialité, intégrité, disponibilité
Modèles de menaces et analyse de risques liés aux produits

L'intégration de la sécurité dans le processus de développement

Les responsabilités au travers des rôles
Limiter & rembourser la dette sécuritaire et technique
Sécurité dans le Cycle de Vie du Développement Logiciel (SDLC)
Pratiques de Sécurité en Développement Agile
Exigences de sécurité dans les items à développer
Les 3 C
Intégration de la sécurité dans Agile et DevOps (DevSecOps)
Introduction à la Sécurité dans les Pipelines CI/CD
Sécurité du logiciel et de l'architecture
Sécurité des environnements du processus de développement
Programmation sécurisée

Les bonnes pratiques

Analyse statique de code (SAST)
Analyse dynamique de sécurité (DAST)
Tests de sécurité interactifs (IAST)
Composition d'analyse logicielle (SCA)
Configuration des tests de sécurité automatisés
Surveillance continue et feedback loop

Ref : SSI-D-006

Séminaire

2 jours, soit 14 heures

PUBLIC :

Développeurs, Scrum Master Product Owner, chef de projets, équipe cybersécurité

PARTICIPANTS :

De 2 à 8 pers. max
Pré-requis : bases en développement : avoir 80 % de bonnes réponses à notre QCM d'entrée.

MODALITÉS DE DÉROULEMENT :

- Présentiel ou distanciel
- Exposé, interactivité, exercices avec correction collective

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation, QCM finaux(validation des acquis à partir de 80 % 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 1 790 € 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

Management d'équipes en SSI

Ce séminaire de 3 jours vous présentera l'ensemble des bonnes pratiques en management d'équipes contextualisé au domaine d'activité de la cyber-sécurité.

OBJECTIFS PÉDAGOGIQUES

- Maîtriser le processus de mise en place d'action collective dans la gestion des projets des équipes SSI
- Utiliser les référentiels métiers, les cadres juridiques européens et les normes associées de la série ISO 27K pour adapter son management
- Accompagner l'équipe dans les actes de management quotidiens en comprenant les leviers de motivation de l'équipe SSI
- Organiser/animer des réunions utiles et efficaces dans l'activité quotidienne et en cas de cyber-crise

PROGRAMME

Les enjeux

Spécificités pour une équipe SSI
Les défis
Cadres normatifs et réglementaires (Directive NIS2, la norme ISO 27001 dans une démarche système de management)
La charte d'utilisation du SI
Modèles de menaces et analyse de risques
Le management RH d'une DSI au sens Devops et agilité : concept, enjeux, principes
L'importance de la communication et de la collaboration en sécurité des SI

Développer une culture d'équipe positive et inclusive

Sentiment d'appartenance et cohésion d'équipe
Valorisation des talents
Communication ouverte et partage d'informations
Gestion des conflits et des tensions

Le leadership situationnel en SSI

Adaptation du leadership aux différentes situations
Atteinte des objectifs fixés
La gestion de cyber-crise
Déléguer et responsabiliser les collaborateurs
Suivre et évaluer le travail des collaborateurs

Organiser et animer des réunions efficaces

Objectifs, ordre du jour
Animer de manière participative et productive
Les décisions et les actions à mener
Et l'utilisation de l'IA dans tout çà ?

Communiquer efficacement en SSI

Adaptation du discours et vulgarisation de termes techniques par l'exemple
Maîtriser les techniques de communication non verbale

Prévenir les risques psychosociaux

Les défis du management d'une équipe multiculturelle et multidisciplinaire
Identifier les signes de stress et d'épuisement professionnel
Mettre en place des mesures de prévention et de soutien aux collaborateurs
Favoriser un environnement de travail sain et bienveillant

Ref : SSI-D-007

Séminaire

3 jours, soit 21 heures

PUBLIC :

Chefs de projet, DSI, RSSI, directeur de service

PARTICIPANTS :

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

MODALITÉS DE DÉROULEMENT :

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

MÉTHODE/MOYENS MOBILISÉS :

- Validation des acquis : évaluation des acquis tout au long de la formation à travers des Quizz, test d'auto-positionnement en début et fin de formation, QCM final (validation des acquis à partir de 80 % 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 1 990 € 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

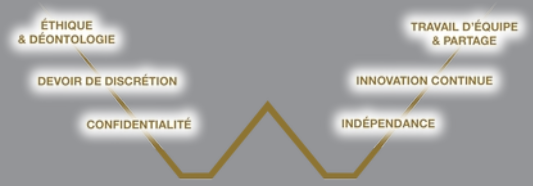
Techniques

- 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