m2i Formation

FORMATION CYBERSECURITE

m2iformation.fr


OFFENSIVE
DEFENSIVE
GOUVERNANCE
EBIOS RM
EGERIE

EDITO

Alors que les volumes de données et les équipements connectés sont l'objet d'une croissance exponentielle, la Cybersécurité est plus que jamais un enjeu stratégique, en lien étroit avec la performance économique des organisations.

Si le gouvernement affiche une volonté de soutenir la montée en puissance des acteurs du numérique et de l'innovation, c'est bien que le défi aujourd'hui est d'absorber la volumétrie tout en perfectionnant la qualité des prestations.

Dans ce contexte, la formation s'inscrit comme une priorité absolue pour susciter les vocations, résoudre le déficit d'experts et renforcer la prise en compte du risque.

C'est pourquoi M2i Formation a développé une offre de formation entièrement dédiée à la Cybersécurité, dont la pédagogie est basée sur la pratique, avec un engagement fort pour l'employabilité et la valorisation des compétences.

Sécurité offensive, sécurité défensive ou gouvernance, n'attendez plus pour découvrir cette offre des compétences les plus demandées et des dernières innovations.

Eligible au CPF

DEVENEZ EXPERT(E)

L'expert(e) Cybersécurité intervient à haut niveau dans l'entreprise.
Il(elle) est en mesure de mener des audits sécurité et de détecter des failles et des faiblesses dans le système d'information de l'entreprise. Il(elle) fait une synthèse des résultats, est capable de mettre des solutions en place, d'organiser l'entreprise autour de ses préconisations.
L'expert(e) Cybersécurité est chargé(e) de mettre en place les protections et d'assurer la surveillance des systèmes informatiques. Il(elle) maîtrise :

- L'organisation des entreprises du point de vue sécurité informatique
- La construction de plans d'affaires visant à organiser la sécurité informatique dans l'entreprise
- La présentation orale de son expertise auprès des décideurs
- La rédaction d'un plan d'action et la présentation de son rapport de fin de mission.

Ses opportunités d'embauches sont considérables dans un monde où la cybersécurité est au cœur des enjeux des organisation.

CYBERSÉCURITÉ

Parcours de 620 heures de formation ponctué par une certification reconnue au Répertoire Spécifique France Compétences

FRANCE compétences
CERTIFICATION
enregistrée au Répertoire spécifique

m2i Formation Diplômante

Contactez nos équipes au
01 44 53 36 30
ou visitez notre site
diplome.m2iformation.fr

SOMMAIRE

#01
Sécurité offensive
- P6 -

#02
Sécurité défensive
- P10 -

#03
Gouvernance & Juridique
- P22 -

#04
Offre éditeurs
- P30 -

#01

SECURITE OFFENSIVE

Sécurité **Offensive**

Fonctionnalités avancées

HIT **SEC-HACK**

Techniques de hacking et contre-mesures - Niveau 1

CPF 5 jours

Cert. M2i Sécurité Pentesting

Expertise / Spécialisation

HIT **SEC-HACK2**

Techniques de hacking et contre-mesures - Niveau 2

CPF 5 jours

Cert. M2i Sécurité Pentesting

SEC-PYT

Python pour tests d'intrusion

3 jours

ESD

NEW **SEC-TESTWI**

Tests d'intrusion sur réseaux Wi-Fi

3 jours

NEW **SEC-TESTAND**

Tests d'intrusion sur Android

2 jours

ESD

NEW **SEC-TESTIOS**

Tests d'intrusion sur iOS

2 jours

CO Cours officiel CPF CPF

HIT

Fonctionnalités avancées

Techniques de hacking et contre-mesures - Niveau 1

[SEC-HACK]

Code CPF
235779

Certification
M2i Sécurité Pentesting

Prix certification
120 €

Public concerné
Décideurs, responsables DSI, responsables sécurité du SI, chefs de projets IT.

Objectifs pédagogiques
- Détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage
- Appliquer des mesures et des règles basiques pour lutter contre le hacking
- Comprendre le mécanisme des principales attaques.

Prérequis
Posséder des bases dans la sécurité des systèmes d'information. Connaître le fonctionnement d'un réseau, maîtriser des connaissances dans la gestion des données et de leur circulation.

Durée
5 jours

Tarif
3300 €HT

Plus de la formation
L'examen de certification (proposé en option) est en français.

Dates
02/03 - 11/05 - 29/06 - 14/09 - 02/11

HIT

Expertise/Spécialisation

Techniques de hacking et contre-mesures - Niveau 2

[SEC-HACK2]

Code CPF
235779

Certification
M2i Sécurité Pentesting

Prix certification
120 €

Public concerné
Etudiants, administrateurs système, consultants en sécurité de l'information.

Objectifs pédagogiques
- Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes
- Comprendre et expérimenter des techniques de hacking avancées
- Appréhender des méthodes offensives dans la pratique.

Prérequis
Avoir des connaissances générales en système, réseau, développement et test d'intrusion.

Durée
5 jours

Tarif
3500 €HT

Plus de la formation
L'examen de certification (proposé en option) est en français.

Dates
30/03 - 25/05 - 06/07 - 28/09 - 23/11

Expertise/Spécialisation

Python pour tests d'intrusion

[SEC-PYT]

Public concerné
Pentesters, développeurs et administrateurs.

Objectifs pédagogiques
- Acquérir les compétences nécessaires en scripting pour créer vos propres outils en Python pour un test d'intrusion.

Prérequis
Avoir des connaissances généralistes en programmation.

Durée
3 jours

Tarif
1980 €HT

Dates
01/04 - 08/06 - 05/10 - 02/12

VOUS SOUHAITEZ UNE ÉVOLUTION DE CARRIÈRE ?

MON COMPTE FORMATION

Misez sur vos droits CPF !

Le Compte Personnel de Formation (CPF) est un droit individuel permettant à chacun de se former tout au long de sa vie en toute autonomie.

LA FORMATION : UN FACTEUR DE COMPÉTITIVITÉ STRATÉGIQUE

Pour l'employeur

- Innovation
- Croissance économique durable
- Agilité et cohésion sociale

Pour l'individu

- Employabilité
- Evolution professionnelle
- Epanouissement personnel

LE CPF : UNE CAGNOTTE DE PLUSIEURS MILLIERS D'EUROS

25 millions
de personnes sont concernées

3240 €
est le montant total que peut atteindre un compte CPF

1040 €
est le montant moyen des droits CPF disponibles

OBJECTIF FORMATION CONTINUE !

500 € / an
pour un salarié à plein temps, dans la limite de 5000 €

800 € / an
pour un salarié peu ou pas qualifié ou en situation de handicap, dans la limite de 8000 €

DIF : LE COMPTE À REBOURS A COMMENCÉ

31 décembre 2020
Date limite pour rapatrier son cumul Droit Individuel à la Formation (DIF) sur son Compte Personnel Formation.

m2i Formation

RDV sur **m2iformation.fr**
et choisissez votre formation
parmi plus de **450 parcours**
éligibles au financement CPF

#02

SECURITE DEFENSIVE

Sécurité **Défensive**

Fondamentaux | Expertise / Spécialisation

Investigation numérique

NEW SEC-INVFOR
Investigation numérique (Computer Forensics)
CPF 5 jours
Cert. M2i Sécurité Inforensic

SEC-INFL
Investigation numérique Linux (Computer Forensics)
3 jours

SEC-INFWEB
Investigation numérique Web (Web Forensics)
2 jours
ESD

SEC-INFW
Investigation numérique Windows (Computer Forensics)
3 jours
ESD

HIT SEC-INFRES
Investigation numérique réseaux (Network Forensics)
3 jours
ESD

SEC-INFAND
Investigation numérique Android (Mobile Forensics)
3 jours

SEC-MALW
Analyse de Malwares - Les fondamentaux
3 jours
ESD

Durcissement Hardening

SEC-DUR
Durcissement des systèmes et réseaux - Hardening
5 jours

HIT SEC-WEC
Durcissement sécurité Windows
4 jours
ESD

SEC-APA
Sécurité des serveurs Web Apache
2 jours

HIT SEC-LEC
Durcissement sécurité Linux
4 jours

SEC-DNS
Sécurité des serveurs de noms (DNS)
2 jours

CO Cours officiel | CPF CPF

Sécurité **Défensive**

Fondamentaux | Expertise / Spécialisation

Sécurité des applications embarquées

Fondamentaux

Sécurité des réseaux et intégration

HIT **WIFI**
Wi-Fi -
Mise en œuvre d'un réseau sécurisé
3 jours

SEC-FIR
Firewall -
Architecture et déploiement
3 jours

SEC-MOB
Sécuriser votre infrastructure mobile
2 jours

SEC-LSF
Sécurité liaison sans fil
3 jours

HIT **SEC-ESS**
Sécurité des systèmes et services réseaux
4 jours

SEC-PKI
PKI -
Mise en œuvre
2 jours

SEC-IDS
Systèmes de détection d'intrusion (IDS)
3 jours

SEC-PREL
Mise en place d'un SIEM
4 jours

SEC-SCA
Cybersécurité des systèmes industriels (SCADA)
3 jours

NEW **SEC-SOC**
Intégration d'un SOC (Security Operation Center)
4 jours

CO Cours officiel CPF CPF

NEW

Fondamentaux

Investigation numérique (Computer Forensics)

[SEC-INVFOR]

Code CPF
236414

Certification
M2i Sécurité Inforensic

Prix certification
120 €

Public concerné
Développeurs, pentesters et consultants en informatique.

Objectifs pédagogiques
- Acquérir des compétences générales sur l'investigation numérique.

Prérequis
Connaissances généralistes en programmation, réseau et système.

Durée
5 jours

Tarif
3300 €HT

Plus de la formation
L'examen de certification (proposé en option) est en français.

Dates
27/01 - 06/04 - 06/07 - 05/10

Expertise/Spécialisation

Investigation numérique Linux (Computer Forensics)

[SEC-INFL]

Public concerné
Administrateurs réseaux et systèmes, RSSI, pentesteurs ou auditeurs.

Objectifs pédagogiques
- Acquérir les connaissances pour réaliser les analyses Forensics sur Linux.

Prérequis
Avoir de bonnes connaissances sur le hacking, la sécurité et Linux.

Durée
3 jours

Tarif
1980 €HT

Dates
17/02 - 11/05 - 24/08 - 02/11

Expertise/Spécialisation

Investigation numérique Web (Web Forensics)

[SEC-INFWEB]

Public concerné
Pentesters et développeurs.

Objectifs pédagogiques
- Analyser de façon méthodique un serveur Web compromis.

Prérequis
Avoir des connaissances en programmation Web, système, Bash et Linux.

Durée
2 jours

Tarif
1320 €HT

Dates
16/03 - 08/06 - 14/09 - 14/12

Expertise/Spécialisation

Investigation numérique Windows (Computer Forensics)

[SEC-INFW]

Public concerné
Administrateurs, analystes SOC et ingénieurs sécurité.

Objectifs pédagogiques
- Réaliser une investigation numérique sur le système d'exploitation Windows.

Prérequis
Avoir des connaissances sur l'OS Windows, TCP/IP, Linux.

Durée
3 jours

Tarif
1980 €HT

Dates
09/03 - 15/06 - 14/09 - 07/12

HIT

Expertise/Spécialisation

Investigation numérique réseaux (Network Forensics)

[SEC-INFRES]

Public concerné
Administrateurs, analystes SOC et ingénieurs sécurité.

Objectifs pédagogiques
- Acquérir les compétences et la méthodologie pour une investigation numérique sur du réseau TCP/IP.

Prérequis
Avoir des connaissances sur l'OS Windows, TCP/IP, Linux.

Durée
3 jours

Tarif
1980 €HT

Dates
23/03 - 15/07 - 19/10 - 07/12

Expertise/Spécialisation

Investigation numérique Android (Mobile Forensics)

[SEC-INFAND]

Public concerné
Administrateurs système et réseau, développeurs, consultants en sécurité.

Objectifs pédagogiques
- Réaliser des analyses Forensic sur Android.

Prérequis
Avoir des connaissances de base en développement d'applications mobiles.

Durée
3 jours

Tarif
2250 €HT

Dates
27/04 - 23/11

Expertise/Spécialisation

Analyse de Malwares - Les fondamentaux

[SEC-MALW]

Public concerné

Pentesters, développeurs, administrateurs et analystes.

Objectifs pédagogiques

- Acquérir des connaissances généralistes sur le fonctionnement des Malwares
- Découvrir une méthodologie d'analyse statique et dynamique
- Créer des charges encodées.

Prérequis

Avoir des connaissances généralistes en programmation, système et réseaux.

Durée

3 jours

Tarif

2250 €HT

Dates

17/02 - 22/06 - 23/11

Fondamentaux

Durcissement des systèmes et réseaux - Hardening

[SEC-DUR]

Public concerné

Administrateurs système et réseau, consultants en sécurité.

Objectifs pédagogiques

- Modifier les systèmes d'exploitation Windows et Linux pour renforcer leur sécurité.

Prérequis

Avoir des connaissances générales sur TCP/IP et la mise en œuvre de services réseaux et systèmes.

Durée

5 jours

Tarif

3500 €HT

Dates

16/03 - 08/06 - 07/09 - 02/11

HIT

Expertise/Spécialisation

Durcissement sécurité Windows

[SEC-WEC]

Public concerné

Administrateurs système et consultants en sécurité de l'information.

Objectifs pédagogiques

- Considérer les menaces courantes pesant sur les systèmes d'information, en vue de l'implémentation de mesures de sécurité adaptées (organisationnelles et techniques).

Prérequis

Avoir des connaissances générales en système et réseau.

Durée

4 jours

Tarif

2400 €HT

Dates

17/02 - 06/04 - 06/07 - 07/10 - 07/12

Expertise/Spécialisation

Sécurité des serveurs Web Apache

[SEC-APA]

Public concerné
Administrateurs système et réseau, consultants en sécurité.

Objectifs pédagogiques
- Sécuriser des serveurs Web Apache et vérifier l'application des mesures de protection.

Prérequis
Avoir des connaissances générales sur TCP/IP et la mise en œuvre de services réseaux et systèmes.

Durée
2 jours

Tarif
1200 €HT

Dates
25/05 - 02/11

HIT

Expertise/Spécialisation

Durcissement sécurité Linux

[SEC-LEC]

Public concerné
Responsables sécurité du SI, chefs de projets informatiques, ingénieurs et administrateurs systèmes.

Objectifs pédagogiques
- Connaître les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent
- Pouvoir optimiser la sécurisation du système.

Prérequis
Etre familiarisé avec le système d'exploitation Linux. Avoir des connaissances de base en sécurité des systèmes d'information.

Durée
4 jours

Tarif
2400 €HT

Dates
10/02 - 20/04 - 20/07 - 19/10 - 14/12

Expertise/Spécialisation

Sécurité des serveurs de noms (DNS)

[SEC-DNS]

Public concerné
Responsables de sécurité, responsables informatique, administrateurs systèmes et sécurité, chefs de projets.

Objectifs pédagogiques
- Acquérir des compétences et connaissances pour sécuriser des serveurs de noms en environnement Linux et Windows.

Prérequis
Avoir des connaissances en administration de systèmes et des notions en sécurité informatique.

Durée
2 jours

Tarif
1400 €HT

Dates
15/06 - 07/12

HIT

Fondamentaux

Sécurité des applications Web

[SEC-SAW]

Public concerné

Pentesters et développeurs.

Objectifs pédagogiques

- Acquérir des compétences en programmation
- Sécuriser efficacement un serveur Web / une application.

Prérequis

Avoir des connaissances généralistes en programmation Web.

Durée

3 jours

Tarif

1800 €HT

Dates

10/02 - 20/04 - 15/06 - 14/09 - 16/11

Expertise/Spécialisation

La sécurité des frameworks JavaScript

[SEC-FRAM]

Public concerné

Pentesters et développeurs.

Objectifs pédagogiques

- Comprendre les vulnérabilités affectant les applications Web
- Développer des applications sécurisées en utilisant les frameworks JavaScript.

Prérequis

Avoir des connaissances en développement d'application en langage JavaScript.

Durée

2 jours

Tarif

1400 €HT

Dates

09/03 - 21/09

NEW

Expertise/Spécialisation

Sécuriser une solution IoT

[SEC-IOT]

Public concerné

Administrateurs système et réseau, consultants en sécurité.

Objectifs pédagogiques

- Comprendre les cybermenaces liées à l'IoT
- Appréhender également les aspects offensifs et défensifs, ainsi que les techniques des infrastructures IoT pour pouvoir développer le Secure by Design demandé par ces systèmes.

Prérequis

Avoir des connaissances générales sur TCP/IP, ainsi que sur la mise en œuvre de services réseaux et systèmes.

Durée

2 jours

Tarif

1400 €HT

Dates

11/05 - 16/11

HIT

Fondamentaux

Wi-Fi - Mise en œuvre d'un réseau sécurisé

[WIFI]

Public concerné
Techniciens réseaux.

Objectifs pédagogiques
- Comprendre les concepts d'un réseau sans fil
- Connaître les matériels sans fil
- Intégrer un réseau sans fil
- Comprendre et mettre en œuvre les mécanismes de sécurité
- Administrer votre réseau sans fil
- Appréhender les techniques de VPN
- Faire évoluer votre réseau sans fil.

Prérequis
Avoir des connaissances sur les réseaux TCP/IP.

Durée
3 jours

Tarif
1800 €HT

Dates
27/01 - 09/03 - 08/06 - 05/10 - 07/12

Fondamentaux

Firewall - Architecture et déploiement

[SEC-FIR]

Public concerné
Tout public.

Objectifs pédagogiques
- Bien connaître et assimiler les fonctionnalités du firewall, l'équipement vital de protection des réseaux
- Maîtriser l'installation et la configuration des firewalls pour mettre en place des architectures sécurisées
- Mettre en place les fonctionnalités d'un UTM (Unified Threat Management)
- Acquérir les méthodologies de «firewalking»
- Installer des protections contre les attaques informatiques.

Prérequis
Avoir de très bonnes connaissances sur les réseaux et la sécurité informatique.

Durée
3 jours

Tarif
1800 €HT

Dates
09/03 - 08/06 - 07/09 - 07/12

Fondamentaux

PKI - Mise en œuvre

[SEC-PKI]

Public concerné
Administrateurs système et réseau, consultants en sécurité.

Objectifs pédagogiques
- Connaître les éléments structurant une PKI
- Appréhender les étapes nécessaires à son implémentation.

Prérequis
Avoir des connaissances générales sur TCP/IP, le chiffrement et la mise en œuvre de services réseaux et systèmes.

Durée
2 jours

Tarif
1200 €HT

Dates
11/05 - 12/10

Fondamentaux

Cybersécurité des systèmes industriels (SCADA)

[SEC-SCA]

Public concerné

Auditeurs, responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS/SCADA (Industrial Control Systems / Supervisory Control and Data Acquisition).

Objectifs pédagogiques

- Connaître le métier et les problématiques
- Dialoguer avec les automaticiens
- Connaître et comprendre les normes et standards propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité.

Prérequis

Avoir de bonnes connaissances générales en informatique et en sécurité des systèmes d'information.

Durée

3 jours

Tarif

2100 €HT

Dates

23/03 - 07/09

Fondamentaux

Sécuriser votre infrastructure mobile

[SEC-MOB]

Public concerné

Responsables sécurité du SI, chefs de projets informatiques, architectes réseaux, ingénieurs, administrateurs.

Objectifs pédagogiques

- Appréhender l'intégration et la sécurisation de la mobilité dans un SI
- Connaître les solutions du marché et posséder les bases pour la sécurisation des terminaux mobiles
- Déployer des solutions pour la sécurité de l'infrastructure mobile
- Découvrir les attaques sur les infrastructures mobiles.

Prérequis

Avoir de bonnes connaissances en réseaux informatiques. Avoir des notions de Cloud et de sécurité.

Durée

2 jours

Tarif

1500 €HT

Dates

23/03 - 22/06 - 21/09 - 14/12

Fondamentaux

Systèmes de détection d'intrusion (IDS)

[SEC-IDS]

Public concerné

Pentesters, étudiants en sécurité informatique, administrateurs système, RSSI et consultants en sécurité de l'information.

Objectifs pédagogiques

- Déployer différents outils de détection d'intrusion.

Prérequis

Avoir des connaissances générales en système, réseau et développement.

Durée

3 jours

Tarif

1800 €HT

Dates

03/06 - 23/11

NEW

Fondamentaux

Intégration d'un SOC (Security Operation Center)

[SEC-SOC]

Public concerné

Etudiants en sécurité informatique, administrateurs système, Pentesters, RSSI (responsables de la sécurité des systèmes d'information) et consultants en sécurité de l'information.

Objectifs pédagogiques

- Comprendre, implémenter et manipuler un SOC (Security Operation Center) dans un environnement complet.

Prérequis

Connaissances générales en système, réseau et développement.

Durée

4 jours

Tarif

3000 €HT

Dates

11/05 - 21/09 - 23/11

Fondamentaux

Sécurité liaison sans fil

[SEC-LSF]

Public concerné

Administrateurs système et réseau, consultants en sécurité.

Objectifs pédagogiques

- Appréhender l'ensemble des éléments de sécurité d'un réseau sans fil
- Maîtriser les principes de leur sécurisation.

Prérequis

Avoir des connaissances générales sur TCP/IP et sur la mise en œuvre de services réseaux et systèmes.

Durée

3 jours

Tarif

2100 €HT

Dates

11/05 - 16/11

Fondamentaux

Mise en place d'un SIEM

[SEC-PREL]

Public concerné

Pentesters, étudiants en sécurité informatique, administrateurs système, responsables sécurité des systèmes d'information (RSSI) et consultants en sécurité de l'information.

Objectifs pédagogiques

- Traiter des incidents et leur management
- Aborder les problématiques liées à la détection d'intrusion, ainsi que leurs limites
- Mettre en place le Prelude SIEM avec implémentation de sondes SNORT et d'agents HIDS dans un réseau existant
- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation.

Prérequis

Avoir des connaissances générales en système, réseau et développement.

Durée

4 jours

Tarif

2400 €HT

Dates

24/02 - 25/05 - 21/09 - 07/12

VALORISEZ VOS COMPÉTENCES

Obtenir une certification ou un diplôme d'Etat valorise l'expérience professionnelle et pose un jalon reconnaissable sur votre parcours. Pour un employeur, c'est l'assurance de compétences maîtrisées, d'une performance opérationnelle immédiate. Pour une entreprise, c'est la valorisation en qualité de ses effectifs et une crédibilité accrue au niveau de ses clients.

M2i a obtenu le référencement de plusieurs certifications auprès de France Compétences.

Nos parcours cumulent de 200 h à 400 h de formation, théorique et pratique, et sont ponctués par un examen d'évaluation des compétences effectives acquises.

Vous pouvez vous aussi, dès à présent, obtenir une preuve officielle de vos compétences professionnelles en rejoignant la grande famille des apprenants certifiés M2i !

FRANCE compétences

m2iformation.fr

#03

GOUVERNANCE & JURIDIQUE

Gouvernance et Juridique

Fonctionnalités avancées

Synthèse

SEMI-SECPCA
PCA PRA pour les décideurs
1 jour

SEMI-ISO
ISO 27000 - Synthèse
1 jour

SEMI-SECMOB
La mobilité sécurisée : les enjeux
1 jour

SEMI-SECCLOUD
La sécurité du Cloud : les enjeux
1 jour

SEMI-SCA
SCADA - Introduction à la sécurité des systèmes industriels
1 jour

SEMI-RGPD
RGPD - Sensibilisation
1 jour

SEC-PEN
Encadrement d'un test d'intrusion
2 jours

SEC-AGI
Développement sécurisé dans les méthodes Agiles
2 jours

SEC-DOPS
Sécurité DevOps pour les managers du SI
3 jours

Audit

NEW **SEC-HYG**
Audit et hygiène de sécurité
2 jours

CO Cours officiel CPF CPF

Gouvernance et Juridique

Fondamentaux | Fonctionnalités avancées

Normes ISO 27005

HIT **ISO-27RM**
ISO 27005 - Risk Manager - Avec certification
CPF 3 jours
Cert. PECB 27005 Risk Manager

Normes ISO 22701

ISO-27GM
ISO 27001 / 27002 - Fondamentaux et gestion des mesures de sécurité
2 jours

HIT **ISO-27LI**
ISO 27001 - Lead Implementer - Avec certification
CPF 5 jours
Cert. PECB 27001 Lead Implementer

HIT **ISO-27LA**
ISO 27001 - Lead Auditor - Avec certification
CPF 5 jours
Cert. PECB 27001 Lead Auditor

Normes ISO 22301

ISO-22LI
ISO 22301 - Lead Implementer - Avec certification
CPF 5 jours
Cert. PECB 22301 Lead Implementer

ISO-22LA
ISO 22301 - Lead Auditor - Avec certification
CPF 5 jours
Cert. PECB 22301 Lead Auditor

SEC-EBIO
Méthode EBIOS 2010 et approche RM 2018
3 jours

NEW **EBIO-RM18**
Méthode EBIOS RM 2018 (Risk Manager) - Avec certification
CPF 2,5 jours
Cert. PECB Certified EBIOS Risk Manager

GES-CRI
Gestion de crise IT / SSI
1 jour

SEC-RSSI
RSSI (Responsable de la Sécurité des SI)
5 jours

CERT-CISSP
Préparation à la certification CISSP
5 jours
Cert. CISSP

CERT-CISA
Préparation à la certification CISA
5 jours
Cert. CISA

CERT-CISM
Préparation à la certification CISM
3 jours
Cert. CISM

DPO-ROLE
DPO - Rôles, missions et obligations
3 jours

HIT **DPO-PECB**
RGPD / GDPR - DPO - Avec certification
CPF 5 jours
Cert. PECB Certified Data Protection Officer

SEC-SANT
Sécurité des données de santé et protection de la vie privée
2 jours

CO Cours officiel | CPF CPF

Fonctionnalités avancées

RGPD - Sensibilisation

[SEMI-RGPD]

Public concerné

Tout type de personnes souhaitant se sensibiliser.

Objectifs pédagogiques

- Comprendre les principes fondamentaux de la nouvelle loi «Informatique et Libertés 2018 (RGPD)».

Prérequis

Aucun.

Durée

1 jour

Tarif

700 €HT

Dates

05/06 - 07/12

Fonctionnalités avancées

Encadrement d'un test d'intrusion

[SEC-PEN]

Public concerné

Administrateurs systèmes, ingénieurs systèmes et réseaux, chefs de projets en sécurité.

Objectifs pédagogiques

- Développer les compétences nécessaires pour mener un test d'intrusion.

Prérequis

Avoir suivi le cours SEC-HACK «Techniques de hacking et contre-mesures - Niveau 1» ou avoir les connaissances équivalentes. Avoir des connaissances de base en réseau TCP/IP ainsi que sur Windows et Linux.

Durée

2 jours

Tarif

1320 €HT

Dates

03/02 - 03/09

Fonctionnalités avancées

Sécurité DevOps pour les managers du SI

[SEC-DOPS]

Public concerné

Pentesters et développeurs.

Objectifs pédagogiques

- Sécuriser efficacement un serveur Web / une application
- Gérer la sécurité au travers d'un projet informatique
- Mettre en place des outils liés à la sécurité applicative et à la gestion des risques applicatifs.

Prérequis

Avoir des connaissances généralistes en programmation Web.

Durée

3 jours

Tarif

2100 €HT

Dates

25/05 - 02/11

NEW Fonctionnalités avancées

Audit et hygiène de sécurité

[SEC-HYG]

Public concerné
Auditeurs, RSSI (Responsables Sécurité des Systèmes d'Information) et responsables SI (Sécurité Informatique).

Objectifs pédagogiques
- Monter un audit SSI (Sécurité des Systèmes d'Information) et d'architecture.

Prérequis
Avoir connaissance des structures composant un système d'information.

Durée
2 jours

Tarif
1700 €HT

Dates
25/05 - 28/09 - 16/11

HIT Fonctionnalités avancées

ISO 27005 - Risk Manager - Avec certification

[ISO-27RM]

Code CPF
235635

Certification
PECB 27005 Risk Manager

Public concerné
Responsables SSI, gestionnaires des risques débutants.

Objectifs pédagogiques
- Acquérir une compréhension globale des concepts, de la norme, des méthodes et des techniques
- Mettre en œuvre une démarche d'appréciation des risques continue et pragmatique
- Maîtriser la norme ISO 27005 : appréciation et analyse des risques du SI.

Prérequis
Des connaissances en sécurité informatique sont recommandées. De plus, pour l'obtention de la certification, il est obligatoire de justifier d'expérience et de souscrire à une adhésion (payante) auprès de PECB.

Durée
3 jours

Tarif
2250 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
22/01 - 16/03 - 27/04 - 15/06 - 28/09 - 04/11 - 02/12

HIT Fonctionnalités avancées

ISO 27001 - Lead Implementer - Avec certification

[ISO-27LI]

Code CPF
236611

Certification
PECB 27001 Lead Implementer

Public concerné
Responsables de la sécurité des systèmes d'information, chefs de projets, DSI, qualiticiens, consultants.

Objectifs pédagogiques
- Mettre en œuvre un système de management de la sécurité de l'information (SMSI)
- Gérer un projet de mise en œuvre de SMSI
- Gérer un SMSI dans le temps
- Utiliser la norme ISO 27001 et les guides associés : ISO 27002, ISO 27004 et ISO 27005
- Gérer les exigences et les risques de sécurité
- Gérer la mise en œuvre d'un plan de traitement des risques
- Améliorer le SMSI et les mesures de sécurité dans le temps grâce aux mécanismes d'amélioration continue.

Prérequis
Connaître les bases de la sécurité des systèmes d'information. Avoir suivi une formation initiale minimum du second cycle ou avoir une expérience professionnelle d'au moins 5 ans dans le domaine des systèmes de management de la sécurité informatique. De plus, pour l'obtention de la certification, il est obligatoire de souscrire à une adhésion (payante) auprès de PECB.

Durée
5 jours

Tarif
3500 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
27/01 - 02/03 - 20/04 - 08/06 - 07/09 - 19/10 - 14/12

HIT

Fonctionnalités avancées

ISO 27001 - Lead Auditor - Avec certification

[ISO-27LA]

Code CPF
235823

Certification
PECB 27001 Lead Auditor

Public concerné
Membres des équipes de contrôle interne, équipes de sécurité, auditeurs externes, qualiticiens, responsables d'audit de SMSI, RSSI, consultants en sécurité des systèmes d'information.

Objectifs pédagogiques
- Disposer de la vision «auditeur» vis-à-vis de la norme ISO 27001
- Intégrer le modèle PDCA (Plan - Do - Check - Act) lors de vos activités d'audit
- Auditer les différentes catégories de mesures de sécurité (annexe A de l'ISO 27001 / ISO 27002)
- Conduire un audit de SMSI et ses entretiens (ISO 19011 / ISO 27001 / ISO 27006).

Prérequis
Avoir lu les normes ISO 27001 et ISO 19011. Avoir suivi une formation initiale minimum du second cycle ou bénéficier d'une expérience professionnelle de 5 ans minimum dans le domaine des systèmes de management de la sécurité ou de la qualité. De plus, pour l'obtention de la certification, il est obligatoire de souscrire à une adhésion (payante) auprès de PECB.

Durée
5 jours

Tarif
3500 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
30/03 - 22/06 - 14/09 - 26/10 - 7/12

NEW

Fonctionnalités avancées

Méthode EBIOS RM 2018 (Risk Manager) - Avec certification

[EBIO-RM18]

Code CPF
236760

Certification
PECB Certified EBIOS Risk Manager

Public concerné
Risk managers, responsables de la sécurité des systèmes d'information (RSSI), consultants SSI.

Objectifs pédagogiques
- Pratiquer la gestion des risques avec la méthode EBIOS Risk Manager.

Prérequis
Avoir de bonnes connaissances en gestion des risques. De plus, pour l'obtention de la certification, il est obligatoire de justifier d'expérience et de souscrire à une adhésion (payante) auprès de PECB.

Durée
2,5 jours

Tarif
1750 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
16/03 - 22/06 - 12/10 - 14/12

Fondamentaux

RSSI (Responsable de la Sécurité des SI)

[SEC-RSSI]

Public concerné
Nouveaux ou futurs RSSI souhaitant se remettre à niveau et échanger. RSSI expérimentés, ingénieurs en sécurité des systèmes d'information, directeurs des systèmes d'information.

Objectifs pédagogiques
- Maîtriser les bases pour la mise en place d'une bonne gouvernance de la sécurité des systèmes d'information
- Connaître les techniques de base indispensables à la fonction de RSSI
- Mettre en œuvre un SMSI en s'appuyant sur la norme ISO 27001
- Connaître l'état du marché de la sécurité informatique
- Maîtriser les méthodes d'appréciation des risques
- Connaître les enjeux de la SSI au sein des organisations
- Maîtriser les stratégies de prise de fonction et des retours d'expériences de RSSI.

Prérequis
Avoir une expérience au sein d'une direction informatique en tant qu'informaticien ou une bonne connaissance générale des systèmes d'information. Avoir des notions de base en sécurité appliquées au système d'information constitue un plus.

Durée
5 jours

Tarif
3600 €HT

Dates
09/03 - 08/06 - 21/09 - 23/11

Fonctionnalités avancées

Préparation à la certification CISSP

[CERT-CISSP]

Certification
CISSP

Public concerné
Toute personne souhaitant obtenir la certification CISSP, par exemple les consultants en sécurité devant démontrer leurs connaissances acquises et enrichir leur CV.

Objectifs pédagogiques
- Maîtriser les concepts fondamentaux de la Sécurité de l'Information
- Passer l'examen CISSP.

Prérequis
Avoir une bonne connaissance des systèmes d'information. La lecture du support de cours officiel de l'ISC (CBK) est fortement recommandée.

Durée
5 jours

Tarif
4100 €HT

Plus de la formation
L'examen de certification est en anglais.

Dates
02/03 - 11/05 - 29/06 - 21/09 - 02/11 - 14/12

Fonctionnalités avancées

Préparation à la certification CISA

[CERT-CISA]

Certification
CISA

Prix certification
835 €

Public concerné
Consultants en organisation, consultants en systèmes d'information, consultants en sécurité, auditeurs, informaticiens, responsables informatique, chefs de projets, urbanistes et managers.

Objectifs pédagogiques
- Pratiquer de l'audit SI
- Maîtriser la gouvernance des SI
- Connaître l'acquisition et l'implantation des SI
- Exploiter et gérer des SI
- Maîtriser l'audit de l'informatique et des opérations, ainsi que l'audit des infrastructures et des réseaux
- Mettre en œuvre la sécurité des actifs informationnels
- Vous familiariser avec le contexte de l'examen (QCM et typologie de questions).

Prérequis
Avoir une connaissance générale de l'informatique, de ses modes d'organisation et de son fonctionnement. Et avoir également connaissance des principes généraux des processus SI et des principes de base de la technologie des SI et des réseaux.

Durée
5 jours

Tarif
3600 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
05/10

Fonctionnalités avancées

DPO - Rôles, missions et obligations

[DPO-ROLE]

Public concerné
CIL, DPO, RSI / RSSI, DSI, directeurs informatiques, directeurs juridiques, directeurs administratifs, auditeurs / contrôleurs internes.

Objectifs pédagogiques
- Identifier et apprécier le risque sur les données personnelles de votre organisation
- Analyser la démarche de la mise en œuvre des mécanismes et des procédures internes
- Bâtir un plan d'actions pour sensibiliser le responsable des traitements aux risques.

Prérequis
Avoir les bases de la direction des systèmes d'information.

Durée
3 jours

Tarif
1980 €HT

Dates
23/03 - 14/09

m2i Formation

Suivez vos actus FORMATION

Offres exclusives

Conseils & astuces pour gérer votre plan de formation

Détail de nos événements

#04

OFFRE EDITEURS

Offre éditeurs

Expertise / Spécialisation

Microsoft

Offre M2i

SEC-AZU
Microsoft Azure - Gestion de la sécurité
2 jours

Offre officielle

MS22744
Windows Server 2016 - Sécurisation de l'infrastructure
CO CPF 5 jours
Cert. 70-744

LogPoint

LOG-TRAIN
LogPoint - Administrateur et utilisateur
CO 3 jours

Check Point

CHK80-N1
Check Point - Certified Security Administrator R80.20
CO 3 jours
Cert. CCSA

→

CHK80-N2
Check Point - Certified Security Engineer R80.20
CO 3 jours
Cert. CCSE

Fortinet

FGT-ADM
Fortinet NSE 4 - FortiGate Security
CO 3 jours
Cert. NSE 4 (v 6.0)

→

FGT-EXP
Fortinet NSE 4 - FortiGate Infrastructure
CO 2 jours
Cert. NSE 4 (v 6.0)

ou

FGT-COMB
Fortinet NSE 4 - FortiGate Security et Infrastructure
CO 5 jours
Cert. NSE 4 (v 6.0)

CO Cours officiel CPF CPF

Offre éditeurs

Fonctionnalités avancées | Expertise / Spécialisation

Red Hat

RH415
Red Hat Security - Linux in Physical, Virtual, and Cloud
CO 4 jours

ou

RH416
Red Hat Security - Linux in Physical, Virtual, and Cloud + examen
CO 4,5 jours
Cert. EX415

Cisco

Certification CCNA Sécurité

IINS
Cisco - Mettre en œuvre la sécurité des réseaux iOS
CO CPF 5 jours
Cert. 210-260

Certification CCNP Sécurité

SISAS
Cisco - Implémentation des solutions Cisco Secure Access
CO CPF 5 jours
Cert. 300-208

→ **SENSS**
Cisco - Implémentation des solutions Cisco Edge Network
CO CPF 5 jours
Cert. 300-206

→ **SIMOS**
Cisco - Implémentation des solutions Cisco Secure Mobility
CO CPF 5 jours
Cert. 300-209

↓ **SITCS**
Cisco - Implémentation de Cisco Threat Control Systems
CO CPF 5 jours
Cert. 300-210

Fonctionnalités avancées

Juniper

JUN-IJOSINT
Juniper IJOS - Junos Operating System Introduction
CO 3 jours

→ **JUN-JSECIN**
Juniper JSEC - Junos Security
CO 5 jours

→ **JUN-AJSEC**
Juniper AJSEC - Junos Security advanced
CO 5 jours

CO Cours officiel CPF CPF

Offre éditeurs

Fonctionnalités avancées

McAfee

MCA-ACC
McAfee Application and Change Control - Administration 8.0
CO 4 jours

MCA-WG
McAfee Web Gateway - Administration
CO 4 jours

MCA-ES
McAfee Endpoint Security 10.x - Administration
CO 5 jours

MCA-VS
McAfee ePolicy Orchestrator - Administration
CO 4 jours

MCA-NSP
McAfee Network Security Platform - Administration
CO 4 jours

ProxySG

NEW **SPSG-AD**
Symantec ProxySG 6.6 - Basic Administration
CO 2 jours

→

NEW **SPSG-ADAV**
Symantec ProxySG 6.6 - Advanced Administration
CO 2 jours
Cert. 250-430

SonicWall

NEW **SNSA**
SonicWall Network Security Administrator
CO 2 jours
Cert. CSSA

EGERIE

NEW **EGERIE-RM**
EGERIE Risk Manager
CO 2 jours

CO Cours officiel CPF CPF

Offre éditeurs

Fondamentaux | Fonctionnalités avancées | Expertise / Spécialisation

Palo Alto Networks

HIT **PAN-EDU210**
Palo Alto Networks - Firewall 9 - Essentials - Configuration et management
CO 5 jours
Cert. PCNSA

PAN-EDU330
Palo Alto Networks - Firewall 9 - Troubleshooting avancé
CO 3 jours

Palo Alto Traps

PAN-EDU281
Palo Alto Networks - Traps - Installation, configuration et gestion
CO 2 jours

PAN-EDU285
Palo Alto Networks - Traps - Déploiement et optimisation
CO 2 jours

PAN-EDU290
Palo Alto Networks - Traps - Cloud Service Operations
CO 2 jours

Stormshield

Protection des réseaux

HIT **STO-CSNA**
Stormshield Network - Administrateur
CO CPF 3 jours
Cert. CSNA

NEW **STO-CSMCE**
Stormshield Management Center - Expert
CO 2 jours
Cert. CSMCE

STO-CSNE
Stormshield Network - Expert
CO CPF 3 jours
Cert. CSNE

STO-CSNTS
Stormshield Network - Troubleshooting and support
CO CPF 4 jours
Cert. CSNTS

Protection des postes

STO-CSEA
Stormshield Endpoint - Administrateur
CO 3 jours
Cert. CSEA

STO-CSEE
Stormshield Endpoint - Expert
CO 2 jours
Cert. CSEE

Protection des données

STO-CSDA
Stormshield Data - Administrateur
CO 2 jours
Cert. CSDA

STO-CSDE
Stormshield Data - Expert
CO 3 jours
Cert. CSDE

CO Cours officiel | CPF CPF

Expertise/Spécialisation

Windows Server 2016 - Sécurisation de l'infrastructure

[MS22744]

Code CPF
235833

Certification
70-744

Prix certification
200 €

Public concerné

Professionnels IT souhaitant administrer des réseaux sous Windows Server 2016 en toute sécurité, avec un accès aux services Cloud ou toute personne souhaitant passer l'examen 70-744.

Objectifs pédagogiques

- Sécuriser Windows Server
- Sécuriser le développement d'applications et une infrastructure de charge utile de serveur
- Gérer les bases de référence de la sécurité
- Configurer et gérer une administration JEA et JIT
- Gérer la sécurité des données
- Configurer le Pare-feu Windows et un pare-feu distribué défini par le logiciel
- Sécuriser le trafic réseau
- Sécuriser votre infrastructure de virtualisation
- Gérer les logiciels malveillants et les menaces
- Configurer un audit avancé
- Gérer les mises à jour logicielles
- Gérer les menaces avec ATA (Advanced Threat Analytics) et Microsoft Operations Management Suite (OMS).

Prérequis

Avoir suivi les cours MS22740 «Windows Server 2016 - Installation, stockage et virtualisation», MS22741 «Windows Server 2016 - Mise en réseau» et MS22742 «Windows Server 2016 - Identité et accès aux données» ou posséder les connaissances équivalentes. Avoir une pratique solide des fondamentaux de la gestion réseau tels que TCP/IP, UDP (User Datagram Protocol), DNS (Domain Name System), Active Directory (AD DS) et d'Hyper-V. Comprendre également les principes de sécurité de Windows Server.

Durée
5 jours

Tarif
2750 €HT

Plus de la formation

L'examen de certification (proposé en option) est disponible en français et en anglais.

Dates
08/06 - 07/12

Expertise/Spécialisation

Check Point - Certified Security Administrator R80.20

[CHK80-N1]

Certification
CCSA

Prix certification
275 €

Public concerné

Administrateurs réseaux, ingénieurs sécurité et réseaux, responsables de la sécurité des SI, ou toute personne visant la certification CCSA.

Objectifs pédagogiques

- Découvrir les technologies Check Point
- Déployer une politique de sécurité et surveiller le trafic
- Comprendre comment gérer les utilisateurs et fournir un accès aux ressources protégées
- Mettre en œuvre la translation d'adresse (NAT) et des VPNs
- Préparer l'examen officiel menant à la certification CCSA.

Prérequis

Avoir des connaissances de base des réseaux, d'Internet, du protocole TCP/IP et sur les systèmes Unix ou Windows Server.

Durée
3 jours

Tarif
2160 €HT

Plus de la formation

L'examen de certification (proposé en option) est en anglais.

Dates
13/01 - 03/02 - 02/03 - 01/04 - 04/05 - 02/06
01/07 - 03/08 - 01/09 - 05/10 - 02/11 - 01/12

Expertise/Spécialisation

Fortinet NSE 4 - FortiGate Security et Infrastructure

[FGT-COMB]

Certification
NSE 4 (v 6.0)

Prix certification
440 €

Public concerné

Toute personne administrant régulièrement un firewall FortiGate ou toute personne souhaitant participer au design des architectures réseaux et sécurité reposant sur des matériels FortiGate.

Objectifs pédagogiques

- Décrire les fonctionnalités des UTM du FortiGate
- Neutraliser les menaces véhiculées au travers des malwares, les applications nocives et limiter les accès aux sites inappropriés
- Contrôler les accès au réseau selon les types de périphériques utilisés
- Authentifier les utilisateurs au travers du portail captif personnalisable
- Mettre en œuvre un VPN SSL et/ou un VPN IPSec, pour l'accès des utilisateurs nomades au réseau de l'entreprise
- Appliquer de la PAT, de la source NAT et de la destination NAT
- Interpréter les logs et générer des rapports
- Utiliser la GUI et la CLI
- Mettre en œuvre la protection anti-intrusion
- Maîtriser l'utilisation des applications au sein de votre réseau
- Configurer de la SD-WAN
- Monitorer le statut de chaque lien de la SD-WAN
- Configurer de la répartition de charge au sein de la SD-WAN
- Déployer un cluster de FortiGate
- Inspecter et sécuriser le trafic réseau sans impacter le routage
- Analyser la table de routage d'un FortiGate
- Diviser un FortiGate physique en plusieurs FortiGates virtuels indépendants, via la mise en œuvre des Virtual Domains
- Etudier et choisir une architecture de VPN IPSec
- Comparer les VPN IPSec en mode Interface (route-based) ou Tunnel (policy-based)
- Implémenter une architecture de VPN IPSec redondée
- Troubleshooter et diagnostiquer des problématiques simples sur le FortiGate
- Mettre en œuvre l'identification utilisateur ou l'authentification transparente dans les environnements Active Directory.

Prérequis

Avoir des notions sur TCP/IP, sur les couches du modèle OSI et sur les concepts de firewall.

Durée
5 jours

Tarif
3700 €HT

Plus de la formation

L'examen de certification (proposé en option) est en anglais.

Dates
20/01 - 03/02 - 24/02 - 09/03 - 23/03 - 20/04 - 06/04
11/05 - 08/06 - 22/06 - 20/07 - 06/07 - 24/08 - 14/09
28/09 - 19/10 - 16/11 - 30/11 - 02/11 - 14/12

Fonctionnalités avancées

Juniper IJOS - Junos Operating System Introduction

[JUN-IJOSINT]

Public concerné

Toute personne en charge de la configuration et de la surveillance des appareils exécutant Junos Software.

Objectifs pédagogiques

- Expliquer les concepts et les opérations de routage de base
- Afficher et décrire les tables de routage et de transfert
- Configurer et surveiller le routage statique
- Configurer et surveiller OSPF (Open Shortest Path First)
- Décrire l'infrastructure de la stratégie de routage et des filtres de pare-feu
- Expliquer l'évaluation de la stratégie de routage et des filtres de pare-feu
- Identifier les instances où vous pouvez appliquer une stratégie de routage
- Rédiger et appliquer une stratégie de routage
- Identifier les instances où vous pouvez utiliser des filtres de pare-feu
- Rédiger et appliquer un filtre de pare-feu
- Décrire le fonctionnement et la configuration de l'algorithme uRPF (Unicast Reverse Path Forwarding)
- Expliquer la fonction et les avantages des classes de services
- Répertorier et expliquer les différents composants des classes de services
- Implémenter et vérifier le bon fonctionnement des classes de services.

Prérequis

Comprendre le modèle OSI et le protocole TCP/IP.

Durée

3 jours

Tarif

2100 €HT

Dates

09/03 - 15/06 - 02/11

Fonctionnalités avancées

McAfee Endpoint Security 10.x - Administration

[MCA-ES]

Public concerné

Administrateurs systèmes, administrateurs réseaux, services SSI, auditeurs ou toute personne concernée par Endpoint Security.

Objectifs pédagogiques

- Mettre en place et administrer le produit McAfee Endpoint Security (ENS)
- Maîtriser McAfee Endpoint Security (qui combine la prévention des menaces, le pare-feu et le contrôle Web afin de réagir immédiatement contre les applications, téléchargements, sites Web et fichiers potentiellement dangereux)
- Manipuler l'interface utilisateur du produit McAfee Endpoint Security, ainsi que d'intégrer cette solution.

Prérequis

Avoir des compétences sur Windows, l'administration système et réseau. Et avoir des connaissances de base sur la sécurité des SI, la syntaxe des lignes de commande, malware / anti-malware, virus / antivirus et les technologies Web.

Durée

5 jours

Tarif

3695 €HT

Plus de la formation

Plus de certification disponible pour le moment.

Dates

03/02 - 23/03 - 11/05 - 06/07 - 14/09 - 02/11 - 07/12

NEW

Fonctionnalités avancées

EGERIE Risk Manager

[EGERIE-RM]

Public concerné

Responsables de la sécurité des systèmes d'information, consultants, experts et gestionnaires des risques.

Objectifs pédagogiques

- Analyser les risques du système d'information avec l'outil EGERIE
- Construire une vision globale des risques projets
- Mieux piloter vos risques.

Prérequis

Avoir une connaissance générale des méthodes d'appréciation des risques telle que la méthode EBIOS.

Durée

2 jours

Date

Formation en intra. Contactez nos agences pour plus d'informations.

HIT — Fonctionnalités avancées

Palo Alto Networks - Firewall 9 - Essentials - Configuration et management

[PAN-EDU210]

Certification
PCNSA

Public concerné
Ingénieurs et administrateurs sécurité, analystes en sécurité, ingénieurs réseaux et membres d'une équipe de support.

Objectifs pédagogiques
- Configurer et gérer les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
- Configurer et gérer GlobalProtect pour protéger des postes clients qui se situent à l'extérieur du réseau
- Configurer et gérer la haute disponibilité des firewalls Palo Alto Networks
- Monitorer le trafic réseau en utilisant les interfaces Web interactives et les rapports intégrés.

Prérequis
Avoir des connaissances de base sur les concepts de la sécurité et des réseaux, incluant routage, switching et adresses IP. Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.

Durée
5 jours

Tarif
3650 €HT

Plus de la formation
L'examen de certification est en anglais.

Dates
20/01 - 24/02 - 23/03 - 20/04 - 25/05 - 15/06
06/07 - 24/08 - 21/09 - 12/10 - 16/11 - 14/12

NEW — Expertise/Spécialisation

Stormshield Management Center - Expert

[STO-CSMCE]

Certification
CSMCE

Public concerné
Responsables informatique, administrateurs réseaux, ou tout technicien en informatique.

Objectifs pédagogiques
- Déployer et maintenir le produit SMC
- Connecter et superviser un grand nombre d'appliances SNS
- Déployer des règles de filtrage et de NAT sur un grand nombre d'appliances SNS
- Mettre en place facilement des tunnels VPN IPsec site à site
- Configurer un grand nombre d'appliances IPsec via des scripts CLI.

Prérequis
Avoir suivi la formation STO-CSNA «Stormshield Network - Administrateur» et avoir réussi l'examen Certified Stormshield Network Administrator (CSNA) dans les 3 ans précédant la formation CSMCE. Avoir de bonnes connaissances TCP/IP. Avoir suivi une formation IP préalable est un plus. Les stagiaires devront se munir d'un PC portable (8Go RAM minimum) avec un système d'exploitation Windows et les droits d'administrateur afin de réaliser les exercices, et disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox.

Durée
2 jours

Tarif
1600 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
25/02

HIT — Fonctionnalités avancées

Stormshield Network - Administrateur

[STO-CSNA]

Code CPF
237154

Certification
CSNA

Public concerné
Responsables informatique, administrateurs réseaux, tout technicien informatique.

Objectifs pédagogiques
- Prendre en main un firewall SNS et connaître son fonctionnement
- Configurer un firewall dans un réseau
- Définir et mettre en œuvre des politiques de filtrage et de routage
- Configurer des proxies
- Configurer des politiques d'authentification
- Mettre en place différents types de réseaux privés virtuels (VPN et VPN SSL).

Prérequis
Avoir de bonnes connaissances en TCP/IP. Avoir suivi une formation IP au préalable est un plus.
Les stagiaires devront se munir d'un PC portable avec un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur afin de réaliser les exercices ; et disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent VMware (VMware player ou VMware workstation).

Durée
3 jours

Tarif
2250 €HT

Plus de la formation
L'examen de certification est disponible en français et en anglais.

Dates
13/01 - 03/03 - 05/05 - 30/06 - 08/09 - 26/10 - 15/12

M2i, PARTENAIRE STRATEGIQUE DE VOTRE CAPITAL HUMAIN

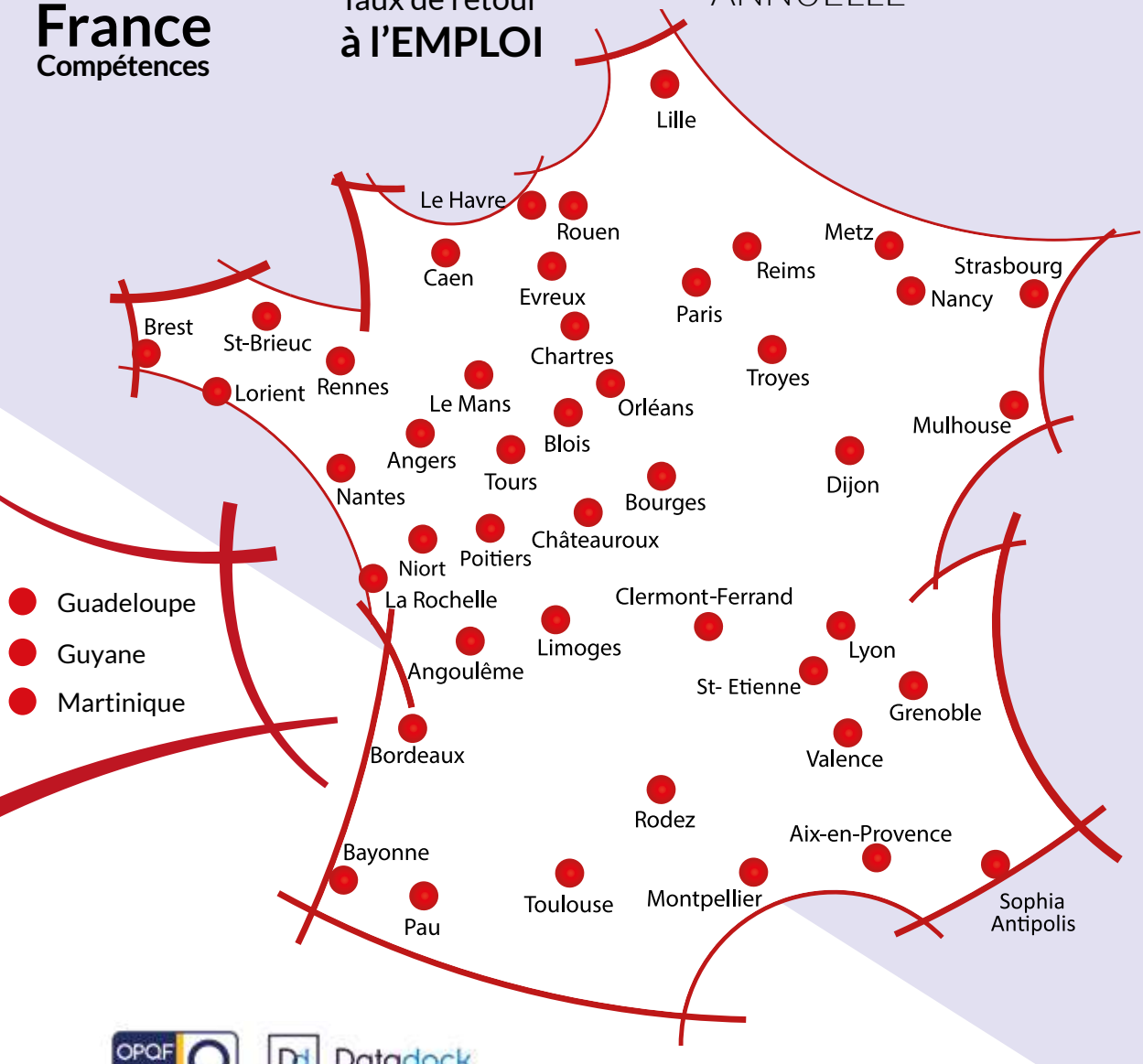
100 000 personnes formées CHAQUE ANNÉE

2400 FORMATIONS & **450** formations éligibles au CPF

Certifications enregistrées au Répertoire Spécifique de **France Compétences**

92% Taux de retour **à l'EMPLOI**

15% DE CROISSANCE ANNUELLE



- Guadeloupe
- Guyane
- Martinique

OPQF Datadock

Retrouvez tous les détails de notre offre sur **m2iformation.fr**

N° Azur 0 810 007 689 - m2iformation.fr - client@m2iformation.fr

TOUS NOS CENTRES A VOTRE ECOUTE

AIX-EN-PROVENCE
Domaine du Tourillon - Bât. B
235 rue Denis Papin
13857 Aix-En-Provence
Tél. : 04 42 39 31 37
aix@m2iformation.fr

ANGERS
152 avenue du Général Patton
49000 Angers
Tél. : 02 47 48 88 48
angers@m2iformation.fr

BLOIS
14 rue des Juifs
41000 Blois
Tél. : 02 54 74 79 34
blois@m2iformation.fr

BORDEAUX
15 bis Allée James Watt - 1er étage
33700 Mérignac
Tél. : 05 57 19 07 60
bordeaux@m2iformation.fr

BOURGES
17 avenue des Prés le Roi
18000 Bourges
Tél. : 02 38 81 13 40
bourges@m2iformation.fr

CAEN
La Folie Couvrechef
11 rue Alfred Kastler
14000 Caen
Tél. : 02 35 19 94 94
caen@m2iformation.fr

CHATEAUROUX
Pépinières d'Entreprises
3 place de la Gare
36015 Châteauroux
Tél. : 02 38 81 13 40
chateauroux@m2iformation.fr

DIJON
Maison Diocésaine
9 bis boulevard Voltaire
21000 Dijon
Tél. : 03 80 72 39 44
dijon@m2iformation.fr

EVREUX
344 rue Jean Monnet
ZAC du Bois des Communes
RDC gauche
27000 Évreux
Tél. : 02 35 60 57 57
evreux@m2iformation.fr

GRENOBLE
Immeuble Le Doyen
22 avenue Doyen Louis Weil
38000 Grenoble
Tél. : 04 76 22 22 20
grenoble@m2iformation.fr

LE HAVRE
28 voie B - Rue des Magasins Généraux
76600 Le Havre
Tél. : 02 35 19 94 94
lehavre@m2iformation.fr

LE MANS
3 avenue Laënnec
72000 Le Mans
Tél. : 02 43 24 89 88
lemans@m2iformation.fr

LILLE
Parc Horizon de la Haute Borne
4 avenue de l'Horizon
59650 Villeneuve-D'Ascq
Tél. : 03 20 19 07 19
lille@m2iformation.fr

LYON
Le Terra Mundi
4 Rue d'Aubigny
69003 Lyon
Tél. : 04 72 68 99 60
lyon@m2iformation.fr

LYON GERLAND
69 Avenue Tony Garnier
Immeuble le Seven
69007 Lyon
Tél. : 04 72 68 99 60
lyon@m2iformation.fr

METZ
Immeuble B6
9 rue Graham Bell
57070 Metz
Tél. : 03 87 75 77 03
metz@m2iformation.fr

MONTPELLIER
55 Rue Euclide
34000 Montpellier
Tél. : 04 67 82 81 80
montpellier@m2iformation.fr

MULHOUSE
Parc d'Activités Ulysse
9 avenue d'Italie
68110 Illzach
Tél. : 03 90 20 66 00
strasbourg@m2iformation.fr

NANCY
4 allée de la Forêt de la Reine
54500 Vandœuvre-Lès-Nancy
Tél. : 03 83 90 58 28
nancy@m2iformation.fr

NANTES
Sillon de Bretagne
1 av. de l'Angevinière
14ème étage aile B
44800 ST HERBLAIN
Tél. : 02 85 52 82 88
nantes@m2iformation.fr

NIORT
12 Avenue Jacques Bujault
79000 Niort
Tél. : 02 47 48 88 48
niort@m2iformation.fr

ORLEANS
12 rue Émile Zola
45000 Orléans
Tél. : 02 38 81 13 40
orleans@m2iformation.fr

PARIS PICPUS
146-148 rue de Picpus
75012 Paris
Tél. : 01 44 53 36 00
paris@m2iformation.fr

PARIS CHAILLOT
17-19 rue de Chaillot
75016 Paris
Tél. : 01 44 53 96 87
paris@m2iformation.fr

PARIS LA DEFENSE
Village 5 - 50 place de l'Ellipse
92000 La Défense
Tél. : 01 49 67 09 50
paris@m2iformation.fr

POITIERS
Centre d'affaires Futuropôle - Téléport 4
1 avenue René Monory
86360 Chasseneuil Du Poitou
Tél. : 05 49 55 13 75
poitiers@m2iformation.fr

REIMS
Maison des Agriculteurs
2 rue Léon Patoux
51664 Reims CEDEX 2
Tél. : 03 26 02 48 45
reims@m2iformation.fr

RENNES
Espace Antrium - ZAC de la Teillais
Rue Jean-Marie David
35740 Pacé
Tél. : 0 810 007 689
rennes@m2iformation.fr

ROUEN
5 rue Jacques Monod
76130 Mont Saint Aignan
Tél. : 02 35 60 57 57
rouen@m2iformation.fr

SAINT-ETIENNE
Centre d'Affaires
35 rue Ponchardier
42100 Saint-Etienne
Tél. : 04 72 68 99 60
saintetienne@m2iformation.fr

SOPHIA-ANTIPOLIS
Marco Polo - Bât. A1
790 avenue du Dr Maurice Donat
06250 Mougins Sophia Antipolis
Tél. : 04 92 28 01 54
sophia@m2iformation.fr

STRASBOURG
Espace Européen de l'Entreprise
Immeuble Le Gallon
11 rue de la Haye
67300 Schiltigheim
Tél. : 03 90 20 66 00
strasbourg@m2iformation.fr

TOURS
26 rue de la Tuilerie
37550 Saint-Avertin
Tél. : 02 47 48 88 48
tours@m2iformation.fr

TROYES
53 rue de la Paix
10000 Troyes
Tél. : 03 25 04 23 48
troyes@m2iformation.fr

VALENCE
C/O 19 Formation
Z.A Briffaut
34 Rue Henri Rey
26000 Valence
Tél. : 04 72 68 99 60
valence@m2iformation.fr

GUADELOUPE
c/o Imm Simkel
3617 Boulevard de Houelbourg
ZI Jarry - 1er étage
97122 Baie-Mauhault
Tél. : 0590 41 41 55
guadeloupe@m2iformation.fr

GUYANE
c/o Route de Montabo
1 Avenue Gustave Charlery
Imm Faic
97300 Cayenne
Tél. : 0590 41 41 55
guyane@m2iformation.fr

MARTINIQUE
c/o Imm Avantage
Lotissement Dillon Stade
11 rue des Arts et Métiers
97200 Fort de France
Tél. : 0590 41 41 55
martinique@m2iformation.fr

m2iformation.fr

N°Azur 0 810 007 689