m2i Formation

FORMATIONS CYBERSÉCURITÉ

CAMPUS CYBER
ACTEUR ENGAGÉ

m2iformation.fr

Dans un monde de plus en plus connecté, où la technologie évolue à une vitesse fulgurante, la cybersécurité est devenue et restera un enjeu incontournable. Chaque jour, de nouvelles menaces émergent, mettant en péril la sécurité des données personnelles et professionnelles. Les cyberattaques se multiplient et se sophistiquent, ciblant aussi bien les grandes entreprises que les petites structures et les particuliers.

La cybersécurité ne se limite pas à la simple protection des systèmes informatiques. Elle englobe une multitude de domaines, allant de la gestion des risques à la protection des données, en passant par la réponse aux incidents et la conformité réglementaire. C'est un domaine en constante évolution, où chaque nouvelle technologie apporte son lot de défis et d'opportunités.

Face à cette réalité, il est impératif de comprendre que la cybersécurité n'est pas seulement une question de technologie, mais aussi de vigilance et de formation continue.
Pour rester compétitif et protéger efficacement ses actifs, il est essentiel de se tenir informé des dernières avancées et de développer des compétences pointues en matière de cybersécurité.

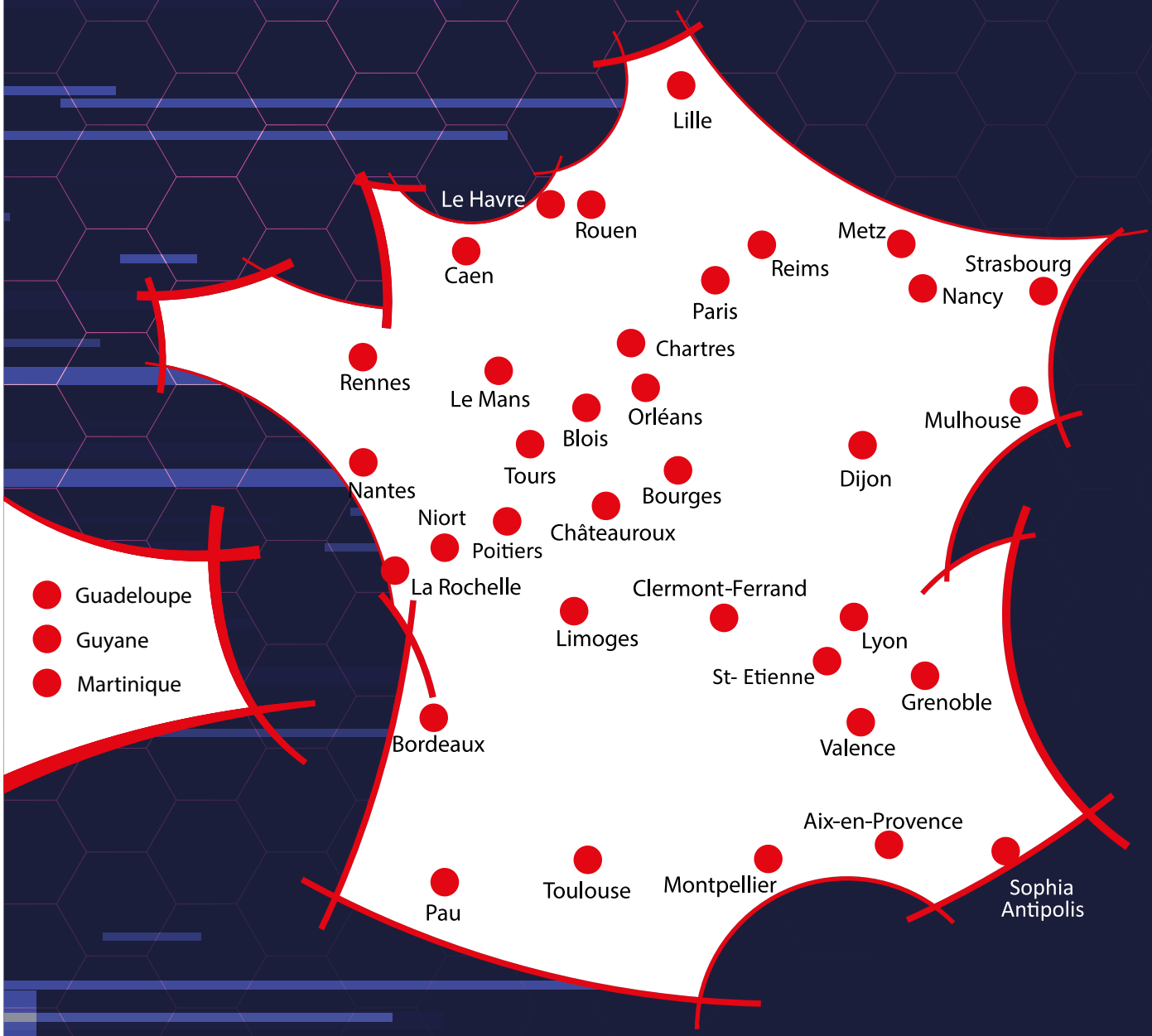
Nos formations en cybersécurité sont conçues pour répondre à ces besoins. Elles offrent une approche pratique et théorique, permettant à chacun de renforcer ses connaissances et de se préparer aux défis actuels et futurs. Que vous soyez un professionnel de l'informatique, un dirigeant d'entreprise ou simplement un passionné de technologie, nos programmes vous fourniront les outils nécessaires pour évoluer en toute sécurité dans le monde numérique.

Ensemble, faisons de la cybersécurité une priorité et construisons un avenir numérique plus sûr et plus résilient.

L'équipe M2i Formation

SOMMAIRE

LEADER DE LA FORMATION IT, IA, DIGITAL, MANAGEMENT & SOFT SKILLS EN FRANCE

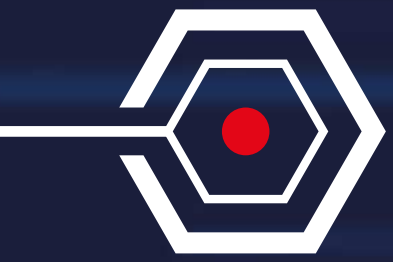


35 centres en France

2500 formateurs experts

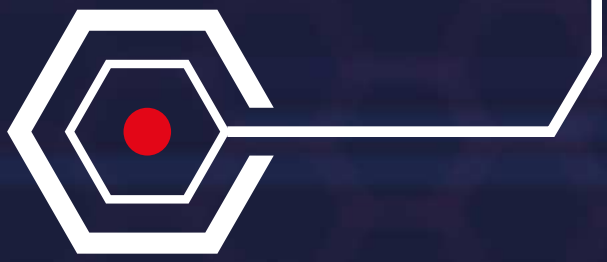
2850 formations

IT, IA, Digital, Management et Soft Skills



01

SÉCURITÉ
OFFENSIVE



Sécurité offensive

Fonctionnalités avancées

PREPA-HACK
Cours préparatoire aux techniques de hacking
2 jours

SEC-HACK — Top Vente
Techniques de hacking - Niveau 1
5 jours

SEC-PYT
Python pour tests d'intrusion
3 jours

SEC-OSINT
OSINT - Investigation en source ouverte - Niveau 1
3 jours

Expertise / Spécialisation

SEC-HACK2 — Top Vente
Techniques de hacking - Niveau 2
5 jours

SEC-OSINT2
OSINT - Investigation en source ouverte - Niveau 2
3 jours

WIFI — Top Vente
Attaque défense Wi-Fi
3 jours

SEC-SAW — Top Vente
Techniques défensives et offensives des applications Web
5 jours

Fonctionnalités avancées

Cours préparatoire aux techniques de hacking

[PREPA-HACK]

PUBLIC CONCERNÉ

Consultants cybersécurité, administrateurs et techniciens réseaux et systèmes, RSSI, DSI, chefs de projets cybersécurité, développeurs, responsables cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Découvrir les notions de base en cybersécurité
- Expliquer le fonctionnement de la virtualisation (VMware)
- Mémoriser les bases d'utilisation des systèmes d'exploitation Windows et Linux
- Mettre en œuvre les bases des protocoles réseaux (modèle OSI, TCP/IP, services, ports, Wireshark...)
- Découvrir la distribution orientée pentest Kali Linux
- Retenir l'essentiel pour suivre la formation SEC-HACK « Techniques de hacking - Niveau 1 ».

PRÉREQUIS

Avoir des connaissances réseaux et système Linux de base.

DURÉE

2 jours (14h)

TARIF

1420 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente

Techniques de hacking - Niveau 1

[SEC-HACK]

PUBLIC CONCERNÉ

Professionnels de la sécurité informatique, administrateurs système et réseau, consultants en sécurité et/ou toute personne souhaitant débuter dans le domaine du hacking éthique et des tests d'intrusion.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les bases du hacking éthique et les concepts fondamentaux de la sécurité des systèmes d'information
- Déterminer les différentes étapes d'un test de pénétration de base
- Utiliser les principaux outils de reconnaissance et de collecte d'information
- Reconnaître les contre-mesures basiques pour protéger un SI.

PRÉREQUIS

Avoir des connaissances de base en réseaux et systèmes d'exploitation et des notions élémentaires de sécurité informatique.

DURÉE

5 jours (35h)

TARIF

3550 €HT

LES PLUS DE LA FORMATION

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande *(coût : 120€)*.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Top Vente

Techniques de hacking - Niveau 2

[SEC-HACK2]

PUBLIC CONCERNÉ

Professionnels de la sécurité informatique ayant une première expérience en pentesting, administrateurs système et réseau souhaitant approfondir leurs connaissances en sécurité, consultants en sécurité avancée.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser des outils de pentesting et des techniques d'exploitation
- Mettre en œuvre des méthodologies et techniques d'attaque réseau plus avancées, incluant l'Active Directory et le social engineering
- Déterminer les contre-mesures avancées pour protéger le SI.

PRÉREQUIS

Avoir suivi la formation SEC-HACK « Techniques de hacking - Niveau 1 » ou avoir les connaissances équivalentes. Savoir maîtriser les concepts de base de la sécurité des réseaux et des systèmes d'information.

DURÉE

5 jours (35h)

TARIF

3800 €HT

LES PLUS DE LA FORMATION

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande *(coût : 120€)*.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Python pour tests d'intrusion

[SEC-PYT]

PUBLIC CONCERNÉ

Professionnels de la sécurité informatique souhaitant utiliser Python (dans leurs activités de tests d'intrusion) et/ou développeurs souhaitant acquérir de nouvelles compétences dans le domaine de la sécurité informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser Python pour réaliser des opérations de base (lecture et écriture de fichiers, interaction avec des sockets et des protocoles réseau...)
- Analyser et interagir avec des systèmes et des réseaux à l'aide de Python
- Exploiter des vulnérabilités et exécuter des commandes sur des systèmes distants à l'aide de Python
- Réaliser des actions de post-exploitation et créer des mécanismes de persistance sur des systèmes compromis à l'aide de Python
- Créer des scripts de tests d'intrusion complets et automatisés à l'aide de Python.

PRÉREQUIS

Avoir des connaissances de base en informatique et en sécurité informatique. Une connaissance préalable en Python est nécessaire, mais une expérience en programmation sera un atout.

DURÉE

3 jours (21h)

TARIF

2010 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

OSINT - Investigation en source ouverte - Niveau 1

[SEC-OSINT]

PUBLIC CONCERNÉ

Enquêteurs en source ouverte, journalistes, responsables de la veille stratégique ou toute personne souhaitant se perfectionner en matière d'investigation en source ouverte.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts de base de l'investigation en source ouverte
- Mettre en œuvre les techniques et les outils d'investigation en source ouverte
- Collecter, trier et analyser des données en source ouverte de manière efficace et éthique
- Mener une investigation en source ouverte de manière autonome et produire des rapports de qualité.

PRÉREQUIS

Avoir des connaissances de base en informatique et en utilisation de logiciels de traitement de données. Savoir utiliser Internet (navigation, recherche avancée) et avoir de bonnes capacités de rédaction et de communication.

DURÉE

3 jours (21h)

TARIF

2550 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

OSINT - Investigation en source ouverte - Niveau 2

[SEC-OSINT2]

PUBLIC CONCERNÉ

Analystes de renseignement cherchant à étendre leurs méthodes d'investigation, enquêteurs privés désireux d'explorer des sources d'informations plus avancées ou tout professionnel de la sécurité souhaitant perfectionner ses compétences en OSINT.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Développer vos compétences en OSINT de manière approfondie en explorant des techniques avancées
- Découvrir des outils puissants pour l'analyse et la collecte de données
- Renforcer votre capacité à mener des investigations approfondies en ligne.

PRÉREQUIS

Avoir suivi la formation SEC-OSINT « OSINT - Investigation en source ouverte - Niveau 1 » ou avoir les connaissances équivalentes. Avoir une expérience avec les techniques d'investigation en source ouverte de base et maîtriser les recherches d'informations en ligne.

DURÉE

3 jours (21h)

TARIF

2850 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Top Vente

Attaque défense Wi-Fi

[WIFI]

PUBLIC CONCERNÉ

Professionnels de la sécurité informatique souhaitant améliorer leurs compétences en matière de sécurité Wi-Fi, administrateurs réseau ou toute personne souhaitant comprendre les risques liés aux réseaux Wi-Fi et les méthodes pour les protéger.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les types de réseaux Wi-Fi et les protocoles de sécurité courants
- Identifier les vulnérabilités courantes dans les réseaux Wi-Fi
- Mettre en pratique les méthodes d'attaque et de défense Wi-Fi
- Acquérir les compétences nécessaires pour configurer la sécurité sur un réseau Wi-Fi et détecter les intrusions.

PRÉREQUIS

Avoir des connaissances de base des réseaux informatiques et des systèmes d'exploitation Windows ou Linux.

DURÉE

3 jours (21h)

TARIF

2010 €HT

LES PLUS DE LA FORMATION

Les exercices incluront des activités pratiques telles que la configuration de la sécurité sur un réseau Wi-Fi, la détection d'intrusion, la mise en place de contre-mesures pour se protéger contre les attaques Wi-Fi, la réalisation de scénarios d'attaque / défense.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Top Vente

Techniques défensives et offensives des applications Web

[SEC-SAW]

PUBLIC CONCERNÉ

Développeurs, ingénieurs DevOps, pentesters et RSSI en sécurité applicative.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Intégrer la sécurité dès le début du cycle de développement (DevSecOps)
- Analyser les attaques pour identifier les vecteurs et les méthodes utilisés
- Identifier les principales menaces et vulnérabilités auxquelles les applications Web sont exposées
- Décrire les différentes techniques d'attaques utilisées par les pirates
- Appliquer des pratiques de codage sécurisé pour prévenir les vulnérabilités courantes
- Utiliser des frameworks et des bibliothèques de sécurité pour renforcer la protection des applications
- Implémenter des mécanismes d'authentification et de gestion des sessions sécurisées
- Mettre en place des contrôles d'accès pour protéger les données sensibles
- Effectuer des audits de sécurité réguliers pour identifier les vulnérabilités
- Effectuer des tests pour confirmer les vulnérabilités
- Assurer la conformité avec les réglementations et les normes de sécurité (comme RGPD, OWASP Level 2, PCI-DSS...)
- Encourager la collaboration entre les équipes de développement et de sécurité pour intégrer la sécurité dès le début du cycle de développement
- Promouvoir une culture de sécurité au sein de l'organisation en sensibilisant les employés aux bonnes pratiques de sécurité.

PRÉREQUIS

Avoir des connaissances généralistes en programmation Web.

DURÉE

5 jours (35h)

TARIF

3800 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

02

SÉCURITÉ DÉFENSIVE

Sécurité défensive

Initiation / Fondamentaux

Expertise / Spécialisation

SEC-CTI
Cyber Threat Intelligence - Niveau 1
3 jours

SEC-CTI2
Cyber Threat Intelligence - Niveau 2
3 jours

Investigation numérique

SEC-INVFOR
Investigation numérique (Computer Forensics)
5 jours

SEC-INFRES
Investigation numérique des réseaux
3 jours

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

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

SEC-MALW
Analyse de Malwares - Les fondamentaux
2 jours

SEC-MALW2
Analyse de Malwares - Niveau avancé
3 jours

Durcissement Hardening

SEC-ESS Top Vente
Sécurité des systèmes et services réseaux
4 jours

SEC-CLI
Sécurité du poste client Windows
2 jours

SEC-AD
Sécurité de l'Active Directory
3 jours

SEC-LEC
Durcissement sécurité Linux
5 jours

DVO-DSOE Top Vente
DevSecOps Foundation
2 jours (16h00)
Cert. DevSecOps Foundation

Sécurité défensive

Expertise / Spécialisation

SEC-PHP
Sécurité applicative avec PHP
3 jours

SEC-RESTAPI
REST API -
Bonnes pratiques et sécurité
3 jours

SEC-JAV
Sécurité applicative Java
3 jours

SEC-SAW Top Vente
Techniques défensives et offensives des applications Web
5 jours

SEC-NET
C# -
Sécurité applicative avec .NET
3 jours

SEC-BYDESIGN Nouveau
Sécurité applicative : intégrer la sécurité dès la conception (Secure by Design)
2 jours

SEC-FRAM
La sécurité du développement Web avec JavaScript
2 jours

Initiation / Fondamentaux

Sécurité des réseaux et intégration

SEC-ANASOC
Parcours Analyste SOC (Security Operation Center)
8 jours

SEC-SOC
Analyste SOC (Security Operation Center)
5 jours

SEC-NESSUS Nouveau
Nessus - Conduite d'un audit de vulnérabilités
3 jours

SEC-ESS Top Vente
Sécurité des systèmes et services réseaux
4 jours

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

SEC-IAM
Gestion des identités et sécurité des accès
4 jours

SEC-FIR
Firewall - Architecture et déploiement
3 jours

SEC-VPN
VPN - Mise en œuvre
3 jours

SEC-PKI
PKI - Mise en œuvre
2 jours

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

Sécurité défensive

Initiation / Fondamentaux

Cyber Threat Intelligence - Niveau 1

[SEC-CTI]

PUBLIC CONCERNÉ

Analystes SOC, responsables de la sécurité des systèmes d'information (RSSI), consultants en cybersécurité et/ou toute personne impliquée dans la collecte et l'analyse des menaces.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts de base de la CTI (Cyber Threat Intelligence)
- Utiliser les termes de la nomenclature de la CTI
- Identifier les différentes menaces et les différents types d'attaques
- Décrire les outils et les méthodes pour vous protéger contre les attaques.

PRÉREQUIS

Avoir des connaissances de base en sécurité des systèmes d'information et être familiarisé avec les concepts de réseau et d'OSINT.

DURÉE

3 jours (21h)

TARIF

2550 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cyber Threat Intelligence - Niveau 2

[SEC-CTI2]

PUBLIC CONCERNÉ

Professionnels de la sécurité informatique, analystes en Cybersécurité, gestionnaires de la sécurité, experts en sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les techniques, tactiques, procédures et infrastructures courantes de la CTI (Cyber Threat Intelligence) de manière approfondie
- Utiliser STIX et TAXII pour représenter les informations sur les menaces
- Développer OpenCTI pour optimiser les flux de travail CTI
- Mettre en place MISP pour collecter, enrichir et partager les informations sur les menaces
- Créer des événements MISP pour documenter les indicateurs de menace
- Intégrer MISP avec d'autres outils de sécurité et collaborer entre organisations
- Appliquer l'automatisation de la CTI avec l'API MISP
- Explorer des études de cas avancées pour une meilleure application des connaissances.

PRÉREQUIS

Avoir suivi le cours SEC-CTI « Cyber Threat Intelligence - Niveau 1 » ou avoir les connaissances équivalentes. Comprendre les concepts fondamentaux de la Cybersécurité et des indicateurs de menace. Etre familié avec MISP, STIX et TAXII à un niveau introductif et avoir une connaissance de base en langage de progammation Python. Avoir également des compétences informatiques de base et être à l'aise avec l'utilisation d'ordinateurs et de logiciels.

DURÉE

3 jours (21h)

TARIF

2850 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Initiation / Fondamentaux

Investigation numérique (Computer Forensics)

[SEC-INVFOR]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs ou auditeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les principes fondamentaux du Forensic des systèmes et des réseaux
- Mettre en pratique les méthodes et outils de collecte de données sous Windows et Linux
- Analyser un système de fichiers Windows et Linux
- Analyser la mémoire et les artefacts du système sous Windows et Linux
- Utiliser les techniques d'acquisition, d'analyse et d'interprétation des données réseau
- Utiliser les outils Windows ou Linux pour la collecte et l'analyse des données réseau
- Appliquer les meilleures pratiques pour sécuriser et documenter les investigations numériques
- Rédiger un rapport et présenter des résultats.

PRÉREQUIS

Avoir de bonnes connaissances sur le hacking, la sécurité, les systèmes Windows et Linux, le modèle OSI et les protocoles TCP/IP.

DURÉE

5 jours (35h)

TARIF

3800 €HT

LES PLUS DE LA FORMATION

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande (*coût : 120€*).

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Investigation numérique des réseaux

[SEC-INFRES]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs ou auditeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts fondamentaux de l'investigation numérique des réseaux
- Identifier les techniques d'acquisition, d'analyse et d'interprétation des données réseau
- Utiliser les outils Windows ou Linux pour la collecte et l'analyse des données réseau
- Appliquer les meilleures pratiques pour sécuriser et documenter les investigations numériques
- Rédiger un rapport et présenter des résultats.

PRÉREQUIS

Avoir de bonnes connaissances sur le hacking, la sécurité, le modèle OSI et les protocoles TCP/IP.

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Investigation numérique Windows (Computer Forensics)

[SEC-INFW]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs et/ou auditeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les principes fondamentaux du Forensic sous Windows
- Décrire les méthodes et outils de collecte de données
- Analyser un système de fichiers
- Analyser la mémoire et les artefacts du système
- Rédiger un rapport et présenter des résultats.

PRÉREQUIS

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

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Investigation numérique Linux (Computer Forensics)

[SEC-INFL]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs ou auditeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les principes fondamentaux du Forensic sous Linux
- Maîtriser les méthodes et outils de collecte de données
- Décrire un système de fichiers
- Décrire la mémoire et les artefacts du système
- Rédiger un rapport et présenter des résultats.

PRÉREQUIS

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

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Initiation / Fondamentaux

Analyse de Malwares - Les fondamentaux

[SEC-MALW]

PUBLIC CONCERNÉ

Professionnels de la Cybersécurité, admnistrateurs système, analystes de menaces, gestionnaires de sécurité, étudiants et toute personne souhaitant se former aux fondamentaux des malwares.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les différents types de malwares et leurs objectifs
- Identifier comment les malwares se propagent et infectent les systèmes
- Définir les techniques d'analyse statique et dynamique des malwares
- Reconnaître les signes d'une éventuelle infection par des malwares.

PRÉREQUIS

Avoir des connaissances de base en Cybersécurité. Etre familié avec les concepts de base des menaces informatiques ainsi qu'avec l'utilisation de systèmes d'exploitation tels que Linux et Windows. Etre à l'aise avec l'utilisation de la ligne de commande pour des tâches basiques et avoir une expérience avec la virtualisation.

DURÉE

2 jours (14h)

TARIF

1700 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Analyse de Malwares - Niveau avancé

[SEC-MALW2]

PUBLIC CONCERNÉ

Professionnels de la Cybersécurité souhaitant approfondir leurs compétences en analyse de malwares et analystes de menaces cherchant à perfectionner leur capacité à analyser des malwares complexes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Exploiter les techniques d'analyse statique et dynamique avancée des malwares
- Reconnaître les outils de débogage et de désassemblage, tels qu'Immunity Debbuger, OllyDbg, GDB, IDA Pro...
- Renforcer les compétences en détection et en réaction aux menaces sophistiquées.

PRÉREQUIS

Avoir suivi le cours SEC-MALW « Analyse de Malwares - Les fondamentaux » ou avoir les connaissances équivalentes. Avoir une expérience avec l'analyse de malwares de base et une connaissance des concepts d'assemblage et d'architecture des systèmes.

DURÉE

3 jours (21h)

TARIF

2850 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Sécurité du poste client Windows

[SEC-CLI]

PUBLIC CONCERNÉ

Administrateurs systèmes, administrateurs SSI.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les enjeux de la sécurité du poste de travail Windows
- Identifier les vulnérabilités et les menaces spécifiques aux postes clients Windows
- Mettre en place des mesures de sécurité adaptées pour protéger les postes de travail Windows
- Appliquer les bonnes pratiques de sécurisation des postes clients Windows
- Configurer et utiliser les outils de sécurité intégrés à Windows
- Mettre en œuvre des stratégies pour renforcer la sécurité
- Gérer efficacement les mises à jour de sécurité sur les postes clients Windows.

PRÉREQUIS

Connaître l'administration de Windows.

DURÉE

2 jours (14h)

TARIF

1340 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Sécurité de l'Active Directory

[SEC-AD]

PUBLIC CONCERNÉ

Architectes et administrateurs systèmes, ingénieurs sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les mécanismes internes Active Directory
- Identifier les fonctionnalités de sécurité
- Concevoir une architecture robuste
- Identifier les attaques et principales exploitations dans un système existant
- Mettre en œuvre les contre-mesures.

PRÉREQUIS

Avoir de bonnes connaissances dans l'administration Windows Server 2012 R2 / 2016 / 2019 ainsi que dans les rôles Active Directory.

DURÉE

3 jours (21h)

TARIF

2130 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Durcissement sécurité Linux

[SEC-LEC]

PUBLIC CONCERNÉ

Responsables sécurité du SI, chefs de projets informatiques, administrateurs systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent
- Optimiser la sécurisation du système.

PRÉREQUIS

Savoir administrer un système d'exploitation Linux. Avoir des connaissances de base en sécurité des systèmes d'information.

DURÉE

5 jours (35h)

TARIF

3350 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Top Vente Cours Officiel

DevSecOps Foundation

[DVO-DSOE]

CERTIFICATION

DevSecOps Foundation

PUBLIC CONCERNÉ

Toute personne impliquée ou intéressée par l'apprentissage des stratégies et l'automatisation DevSecOps, ou impliquée dans les architectures de la chaîne d'outils de livraison continue. Equipes de conformité, Business Managers, personnels de livraison, ingénieurs DevOps, responsables informatiques, professionnels, praticiens et managers de la sécurité informatique, personnels d'entretien et de soutien, fournisseurs de services gérés, chefs de projets et de produits, équipes d'assurance qualité, Release Managers, Scrum Masters, ingénieurs en fiabilité de site, ingénieurs logiciels et/ou testeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer le but, les avantages, les concepts et le vocabulaire de DevSecOps
- Discerner les différences entre les pratiques de sécurité DevOps et les autres approches de sécurité
- Déceler les stratégies et bonnes pratiques de sécurité axées sur l'entreprise
- Définir et appliquer les sciences des données et de la sécurité
- Intégrer les parties prenantes de l'entreprise dans les pratiques DevSecOps
- Améliorer la communication entre les équipes Dev, Sec et Ops
- Expliquer comment les rôles DevSecOps s'intègrent à une culture et une organisation DevOps.

PRÉREQUIS

Avoir une connaissance de base et une compréhension des définitions et principes communs de DevOps.

DURÉE

2 jours (16h)

TARIF

1580 €HT

LES PLUS DE LA FORMATION

Le support de cours est en anglais.

PeopleCert (ex DevOps Institute) recommande fortement ce qui suit pour préparer les candidats à l'examen de certification « DevSecOps Foundation » :

- avoir suivi au moins 16 heures d'enseignement
- consacrer au moins six heures à l'étude personnelle, à la révision de la liste de vocabulaire et des sections pertinentes du manuel du participant et à la passation de l'examen blanc.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Expertise / Spécialisation

Top Vente

Techniques défensives et offensives des applications Web

[SEC-SAW]

PUBLIC CONCERNÉ

Développeurs, ingénieurs DevOps, pentesters et RSSI en sécurité applicative.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Intégrer la sécurité dès le début du cycle de développement (DevSecOps)
- Analyser les attaques pour identifier les vecteurs et les méthodes utilisés
- Identifier les principales menaces et vulnérabilités auxquelles les applications Web sont exposées
- Décrire les différentes techniques d'attaques utilisées par les pirates
- Appliquer des pratiques de codage sécurisé pour prévenir les vulnérabilités courantes
- Utiliser des frameworks et des bibliothèques de sécurité pour renforcer la protection des applications
- Implémenter des mécanismes d'authentification et de gestion des sessions sécurisées
- Mettre en place des contrôles d'accès pour protéger les données sensibles
- Effectuer des audits de sécurité réguliers pour identifier les vulnérabilités
- Effectuer des tests pour confirmer les vulnérabilités
- Assurer la conformité avec les réglementations et les normes de sécurité (comme RGPD, OWASP Level 2, PCI-DSS...)
- Encourager la collaboration entre les équipes de développement et de sécurité pour intégrer la sécurité dès le début du cycle de développement
- Promouvoir une culture de sécurité au sein de l'organisation en sensibilisant les employés aux bonnes pratiques de sécurité.

PRÉREQUIS

Avoir des connaissances généralistes en programmation Web.

DURÉE

5 jours (35h)

TARIF

3800 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Sécurité applicative avec PHP

[SEC-PHP]

PUBLIC CONCERNÉ

Pentesters et développeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Sécuriser un code PHP ou une interface avec du PHP
- Créer des tests visant à éprouver la sécurité des applications Web, notamment sous PHP
- Analyser et organiser la sécurité d'une application Web développée en PHP
- Formuler des exigences de sécurité aux autres corps de métiers.

PRÉREQUIS

Avoir des connaissances généralistes en programmation Web et en langage PHP. Avoir connaissance de la gestion de base d'un serveur Web est un plus.

DURÉE

3 jours (21h)

TARIF

2130 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Sécurité applicative Java

[SEC-JAV]

PUBLIC CONCERNÉ

Pentesters, développeurs impliqués dans des cycles DevSecOps, développeurs déjà formés aux bonnes pratiques du développement sécurisé et souhaitant découvrir les méthodes de protection des contournements potentiels.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître les mécanismes de sécurité du JDK (Java Development Kit)
- Décrire les principales failles de sécurité applicative
- Distinguer la sécurité applicative de la sécurité système et réseau
- Mettre en œuvre les principales stratégies de sécurité en Java
- Utiliser JCE (Java Cryptography Extension)
- Authentifier et autoriser l'accès aux composants Java EE
- Créer des tests visant à éprouver la sécurité des applications
- Formuler des exigences de sécurité aux autres corps de métiers.

PRÉREQUIS

Avoir des connaissances en développement d'applications en langage Java ou langage assimilé, une maîtrise des bonnes pratiques de développement sécurisé, une première sensibilisation à la sécurité du code et du Secure by Design.

DURÉE

3 jours (21h)

TARIF

2010 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

C# - Sécurité applicative avec .NET

[SEC-NET]

PUBLIC CONCERNÉ

Pentesters et développeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître les mécanismes de sécurité de .NET
- Expliquer les principales failles de sécurité applicative
- Mettre en œuvre le Code Access Security et le Role Based Security
- Sécuriser des « Assemblys »
- Authentifier et autoriser l'accès aux applications ASP.NET
- Chiffrer des données avec le Framework .NET
- Créer des tests visant à éprouver la sécurité des applications
- Formuler des exigences de sécurité aux autres corps de métiers.

PRÉREQUIS

Avoir des connaissances en développement d'application en langage .NET ou langage assimilé.

DURÉE

3 jours (21h)

TARIF

2130 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

La sécurité du développement Web avec JavaScript

[SEC-FRAM]

PUBLIC CONCERNÉ

Pentesters et développeurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Ecrire un code participant à la sécurité d'une application Web
- Expliquer les vulnérabilités affectant les applications Web
- Créer des tests visant à éprouver la sécurité des applications Web, notamment en JavaScript
- Développer des applications sécurisées en utilisant JavaScript et ses frameworks
- Formuler des exigences de sécurité aux autres corps de métiers.

PRÉREQUIS

Avoir des connaissances en développement Web et en langage JavaScript.

DURÉE

2 jours (14h)

TARIF

1520 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

REST API - Bonnes pratiques et sécurité

[SEC-RESTAPI]

PUBLIC CONCERNÉ

Développeurs Web Front End et Back End, architectes, chefs de projets techniques.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les bonnes pratiques de conception, de développement et d'architecture des API REST
- Concevoir, déployer et superviser des API
- Identifier les menaces auxquelles s'exposent vos API
- Distinguer les vulnérabilités les plus fréquentes
- Repérer les points faibles d'une API puis la protéger.

PRÉREQUIS

Avoir des connaissances sur HTTP ainsi qu'une bonne culture Web. Avoir quelques connaissances en développement Web (JavaScript / HTML) et sur le fonctionnement de base des API serait un plus.

DURÉE

3 jours (21h)

TARIF

2130 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Expertise / Spécialisation

Nouveau

Sécurité applicative : intégrer la sécurité dès la conception (Secure by Design)

[SEC-BYDESIGN]

PUBLIC CONCERNÉ

Développeurs, ops, testeurs, administrateurs, architectes et/ou toute personne concernée par la sécurité des applications au sens large (application Web, site, Web service...).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Concevoir une application « Secure by Design »
- Appliquer les bonnes pratiques de sécurité à toutes les phases de développement
- Identifier les principales failles de sécurité applicative et anticiper les menaces
- Décrire le déroulement d'une attaque pour mieux la déjouer.

PRÉREQUIS

Pratiquer les langages de développement Web (a minima : HTML, JavaScript, SQL), avoir des connaissances du protocole HTTP et idéalement la connaissance d'un framework front de type Angular, React...

DURÉE

2 jours (14h)

TARIF

1790 €HT

Initiation / Fondamentaux

Parcours Analyste SOC (Security Operation Center)

[SEC-ANASOC]

PUBLIC CONCERNÉ

Etudiant en sécurité informatique, administrateurs système et/ou réseaux, consultants en sécurité de l'information (sécurité offensive, défensive ou organisationnelle) et/ou contractuels des systèmes d'information (développeurs, ingénieurs Big Data, architectes...).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer l'état de l'art du SOC (Security Operation Center)
- Répondre aux besoins des enjeux cybers et des menaces par le métier d'analyste SOC.

PRÉREQUIS

Avoir des connaissances générales en sécurité offensive et défensive et des notions sur le fonctionnement des systèmes d'exploitation. Il est également recommandé d'avoir une capacité de recherche et de restitution (prospecter l'actualité cyber afin d'en comprendre les enjeux).

DURÉE

8 jours (56h)

TARIF

6080 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Initiation / Fondamentaux

Analyste SOC (Security Operation Center)

[SEC-SOC]

PUBLIC CONCERNÉ

Responsables de la Sécurité des Systèmes d'Information (RSSI), Directeurs des Systèmes d'Information, administrateurs systèmes et/ou réseaux, pentesters, consultants en sécurité de l'information et étudiants en sécurité informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire l'état de l'art du SOC (Security Operation Center)
- Organiser les tâches du quotidien dans un SOC
- Organiser et monitorer la collecte et l'analyse de données du SOC
- Répondre aux besoins des enjeux liés à la cybersécurité et des menaces par le métier d'analyste SOC
- Déployer et maintenir un SIEM.

PRÉREQUIS

Avoir des connaissances générales en sécurité offensive et défensive, telles que les techniques de hacking, les modes opératoires adverses, des notions sur les systèmes d'exploitation et les mécanismes de durcissement associés.

DURÉE

5 jours (35h)

TARIF

3800 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Nouveau

Nessus - Conduite d'un audit de vulnérabilités

[SEC-NESSUS]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseaux, analystes en cybersécurité et SOC, consultants en sécurité et auditeurs techniques.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les enjeux et concepts liés à la gestion des vulnérabilités
- Installer, configurer et utiliser Nessus pour détecter des failles de sécurité
- Analyser et interpréter les rapports d'audit générés par Nessus
- Définir un plan de remédiation efficace et suivre la correction des vulnérabilités
- Intégrer Nessus dans un processus de gestion des vulnérabilités.

PRÉREQUIS

Avoir des notions en réseaux et systèmes (Windows / Linux) et être sensibilisé aux concepts de cybersécurité.

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Initiation / Fondamentaux

Top Vente

Sécurité des systèmes et services réseaux

[SEC-ESS]

PUBLIC CONCERNÉ

Responsables de la sécurité des systèmes d'information (RSSI), directeurs des systèmes d'information (DSI), administrateurs système et réseau, techniciens de maintenance système et réseau, consultants en sécurité informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les enjeux de la sécurité des systèmes d'information, ainsi que ses acteurs et ses limites
- Proposer des solutions pour pouvoir faire transiter et stocker des données sur un réseau d'entreprise de façon sécurisée
- Installer et paramétrer un pare-feu approprié au réseau d'une entreprise
- Installer et configurer un proxy
- Mettre en place un filtrage
- Utiliser différents outils permettant de prévenir et détecter une intrusion sur un réseau.

PRÉREQUIS

Avoir des connaissances en réseau et système.

DURÉE

4 jours (28h)

TARIF

2680 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Systèmes de prévention (IPS) et détection (IDS) d'intrusion

[SEC-IDS]

PUBLIC CONCERNÉ

Pentesters, administrateurs système et réseau, analystes SOC, responsables de la sécurité des systèmes d'information (RSSI), consultants en cybersécurité et étudiants en sécurité informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Déployer et maintenir différents outils de prévention et de détection d'intrusion
- Paramétrer et fine-tuner des systèmes de détection et d'alerte
- Organiser et centraliser les alertes pour un SIEM
- Identifier les raisons de déclenchement d'une règle ou d'un faux positif.

PRÉREQUIS

Avoir des connaissances générales en système, réseau et développement.

DURÉE

3 jours (21h)

TARIF

2130 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Gestion des identités et sécurité des accès

[SEC-IAM]

PUBLIC CONCERNÉ

Ingénieurs système, ingénieurs en sécurité, administrateurs système, chefs de projets en sécurité, MOE (maîtres d'œuvre) et/ou MOA (maîtres d'ouvrage).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Renforcer la sécurité et simplifier l'accès aux informations pour les organisations
- Etendre le Single Sign-On (SSO)
- Intégrer une Public Key Infrastructure (PKI)
- Evaluer les services Cloud sur l'authentification à l'intérieur d'un système d'information (SI)
- Mettre en œuvre un système de fédération.

PRÉREQUIS

Avoir des connaissances de base sur la sécurité des systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.

DURÉE

4 jours (28h)

TARIF

3400 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Firewall - Architecture et déploiement

[SEC-FIR]

PUBLIC CONCERNÉ

Professionnels de l'informatique et de la sécurité des réseaux souhaitant acquérir ou approfondir leurs connaissances sur les firewalls.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts de base et les fonctionnalités des firewalls
- Reconnaître l'architecture de réseau et de sécurité, et le rôle des firewalls dans la protection des réseaux
- Configurer et gérer les firewalls de manière efficace
- Déployer et utiliser pfSense pour la sécurité des réseaux.

PRÉREQUIS

Avoir des connaissances de base en réseaux et en sécurité informatique, ainsi que de l'expérience de base avec les systèmes d'exploitation Windows et Linux.

DURÉE

3 jours (21h)

TARIF

2010 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Sécurité défensive

Initiation / Fondamentaux

VPN - Mise en œuvre

[SEC-VPN]

PUBLIC CONCERNÉ

Administrateurs système et réseau, techniciens système et réseau, consultants en sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître les différentes caractéristiques et propriétés des principaux réseaux VPN
- Choisir le type de réseau VPN adapté aux attentes
- Monter un réseau VPN en s'appuyant sur des protocoles courants (SSL / TLS, PPTP, L2TP et IPsec)
- Diagnostiquer et résoudre les problèmes fréquemment rencontrés sur les réseaux VPN.

PRÉREQUIS

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

DURÉE

3 jours (21h)

TARIF

2010 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

PKI - Mise en œuvre

[SEC-PKI]

PUBLIC CONCERNÉ

RSSI, DSI, administrateurs système et réseau, techniciens de maintenance système et réseau, consultants en cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Déterminer et préconiser des pratiques et outils de chiffrement
- Reconnaître les éléments structurant une PKI
- Identifier les étapes nécessaires à son implémentation.

PRÉREQUIS

Avoir des connaissances générales sur le chiffrement et la mise en œuvre de services réseaux et systèmes en entreprise.

DURÉE

2 jours (14h)

TARIF

1420 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Top Vente

Cybersécurité des systèmes industriels (SCADA)

[SEC-SCA]

PUBLIC CONCERNÉ

Responsables de la Sécurité des Systèmes d'Information (RSSI), Directeurs des Systèmes d'Information (DSI), auditeurs, responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS / SCADA (Industrial Control Systems / Supervisory Control And Data Acquisition).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire le métier et les problématiques
- Dialoguer avec les automaticiens
- Identifier et expliquer les normes et standards propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité
- Proposer des mesures de consolidation et de sécurisation en milieu industriel.

PRÉREQUIS

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

DURÉE

3 jours (21h)

TARIF

2280 €^{HT}

Consultez le programme détaillé et les prochaines dates en scannant ce code

03

GOUVERNANCE

Gouvernance

Initiation / Fondamentaux

Fonctionnalités avancées

Synthèse

SEMI-SSI — Top Vente
Etat de l'art de la sécurité des systèmes d'information (SSI)
3 jours

SEMI-ISO
ISO 27000 - Synthèse
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-SECPCA
PCA PRA pour les décideurs
1 jour

SEC-PHISH
Sensibilisation au phishing et à l'ingénierie sociale
1 jour

SEC-RSSI
RSSI (Responsable de la Sécurité des SI) - Rôles et attentes organisationnelles
5 jours

SEC-CYBINTRO
Parcours introductif à la cybersécurité
10 jours

SEC-TECH — Top Vente
Méthodologie de veille pour la cybersécurité
3 jours

Top Vente

Etat de l'art de la sécurité des systèmes d'information (SSI)

[SEMI-SSI]

PUBLIC CONCERNÉ

Directeurs des systèmes d'information ou responsables informatiques, RSSI, chefs de projets sécurité, architectes informatiques.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Présenter les principes et les normes de chaque domaine de la SSI
- Décrire les tendances actuelles au niveau des menaces et des solutions à notre disposition
- Améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'œuvre et la SSI
- Effectuer des choix techniques.

PRÉREQUIS

Avoir une bonne connaissance générale des systèmes d'information.

DURÉE

3 jours (21h)

TARIF

2580 €HT

ISO 27000 - Synthèse

[SEMI-ISO]

PUBLIC CONCERNÉ

Responsables de la sécurité des systèmes d'information (RSSI) et consultants en sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Présenter l'ensemble des normes ISO traitant de la sécurité du SI et de son management.

PRÉREQUIS

Avoir des connaissances générales en sécurité des systèmes d'information.

DURÉE

1 jour (7h)

TARIF

860 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Consultez le programme détaillé et les prochaines dates en scannant ce code

La sécurité du Cloud : les enjeux

[SEMI-SECCLOUD]

PUBLIC CONCERNÉ

Responsables de la sécurité des systèmes d'information (RSSI) et consultants en sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Démontrer les enjeux liés à l'utilisation du Cloud et à sa sécurisation, de manière exhaustive et synthétique.

PRÉREQUIS

Avoir des connaissances générales en sécurité des systèmes d'information.

DURÉE

1 jour (7h)

TARIF

860 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

SCADA - Introduction à la sécurité des systèmes industriels

[SEMI-SCA]

PUBLIC CONCERNÉ

Auditeurs, responsables de sécurité, DSI, managers, automaticiens, consultants, architectes réseaux et systèmes ICS/SCADA, administrateurs réseaux et systèmes ICS/SCADA ou toute autre personne en contact avec ces systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître le métier et les problématiques
- Dialoguer avec les automaticiens
- Identifier et décrire les normes et standards de sécurité propres au monde industriel
- Développer une politique de cybersécurité.

PRÉREQUIS

Avoir de bonnes connaissances générales en informatique.

DURÉE

1 jour (7h)

TARIF

860 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

PCA PRA pour les décideurs

[SEMI-SECPCA]

PUBLIC CONCERNÉ

Responsables de la sécurité des systèmes d'information (RSSI) et consultants en sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître les enjeux et avantages d'un PCA PRA (Plan de Continuité d'Activité / Plan de Reprise d'Activité)
- Démontrer les étapes essentielles à la mise en œuvre d'un PCA PRA de manière exhaustive et synthétique.

PRÉREQUIS

Avoir des connaissances générales en sécurité des systèmes d'information.

DURÉE

1 jour (7h)

TARIF

860 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Sensibilisation au phishing et à l'ingénierie sociale

[SEC-PHISH]

PUBLIC CONCERNÉ

Employés d'entreprises de tous niveaux, utilisateurs fréquents d'Internet et des courriels, gestionnaires et responsables de la sécurité souhaitant renforcer la formation de leurs équipes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Définir les risques associés au phishing et à l'ingénierie sociale
- Reconnaître les signaux d'alerte des attaques de phishing
- Examiner les méthodes d'ingénierie sociale et de manipulation psychologique
- Sensibiliser les utilisateurs à la sécurité.

PRÉREQUIS

Avoir des connaissances de base en informatique et en navigation sur Internet. Etre familier avec les courriels et les réseaux sociaux.

DURÉE

1 jour (7h)

TARIF

850 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

RSSI (Responsable de la Sécurité des SI) - Rôles et attentes organisationnelles

[SEC-RSSI]

PUBLIC CONCERNÉ

Ingénieurs système, ingénieurs en sécurité, administrateurs système, chefs de projets en sécurité, MOE (maîtres d'œuvre) et/ou MOA (maîtres d'ouvrage).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Mettre en place les bases d'une bonne gouvernance de la sécurité des systèmes d'information
- Reconnaître les techniques de base indispensables à la fonction de RSSI
- Expliquer et mettre en œuvre un SMSI en vous appuyant sur la norme ISO 27001
- Exploiter l'état du marché de la sécurité informatique
- Identifier les méthodes d'appréciation des risques ainsi que les enjeux de la SSI au sein des organisations
- Mettre en pratique les stratégies de prise de fonction et des retours d'expérience de RSSI
- Identifier et évaluer les principaux risques juridiques pesant sur un système d'information
- Réduire concrètement les non-conformités juridiques affectant un système d'information.

PRÉREQUIS

Avoir des connaissances de base sur la sécurité des systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.

DURÉE

5 jours (35h)

TARIF

3550 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Parcours introductif à la cybersécurité

[SEC-CYBINTRO]

PUBLIC CONCERNÉ

Etudiants en sécurité informatique, administrateurs système, développeurs, chefs de projets.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

PRÉREQUIS

Avoir des connaissances générales en système et système d'information.

DURÉE

10 jours (70h)

TARIF

7600 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente

Méthodologie de veille pour la cybersécurité

[SEC-TECH]

PUBLIC CONCERNÉ

RSSI (Responsables Sécurité des SI), chefs de projets, responsables cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Faciliter la recherche d'informations pertinentes sur le Web (fonctions avancées de moteurs de recherche, outils de veille, connaissances du Web visible et invisible)
- Construire un référentiel de données pertinentes à partir d'informations recueillies
- Capitaliser les informations du référentiel
- Bien communiquer avec les utilisateurs du référentiel (recueil et diffusion des informations en vue d'améliorer le référentiel).

PRÉREQUIS

Avoir des connaissances de base sur les réseaux et la sécurité.

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

LE GROUPE M2i DISTINGUÉ POUR SON ENGAGEMENT RSE

Le groupe M2i est historiquement très impliqué dans la durabilité de ses activités, avec une maîtrise affirmée de l'impact de celles-ci. Son implication en matière de RSE est reconnue à tous les niveaux de création de valeurs.

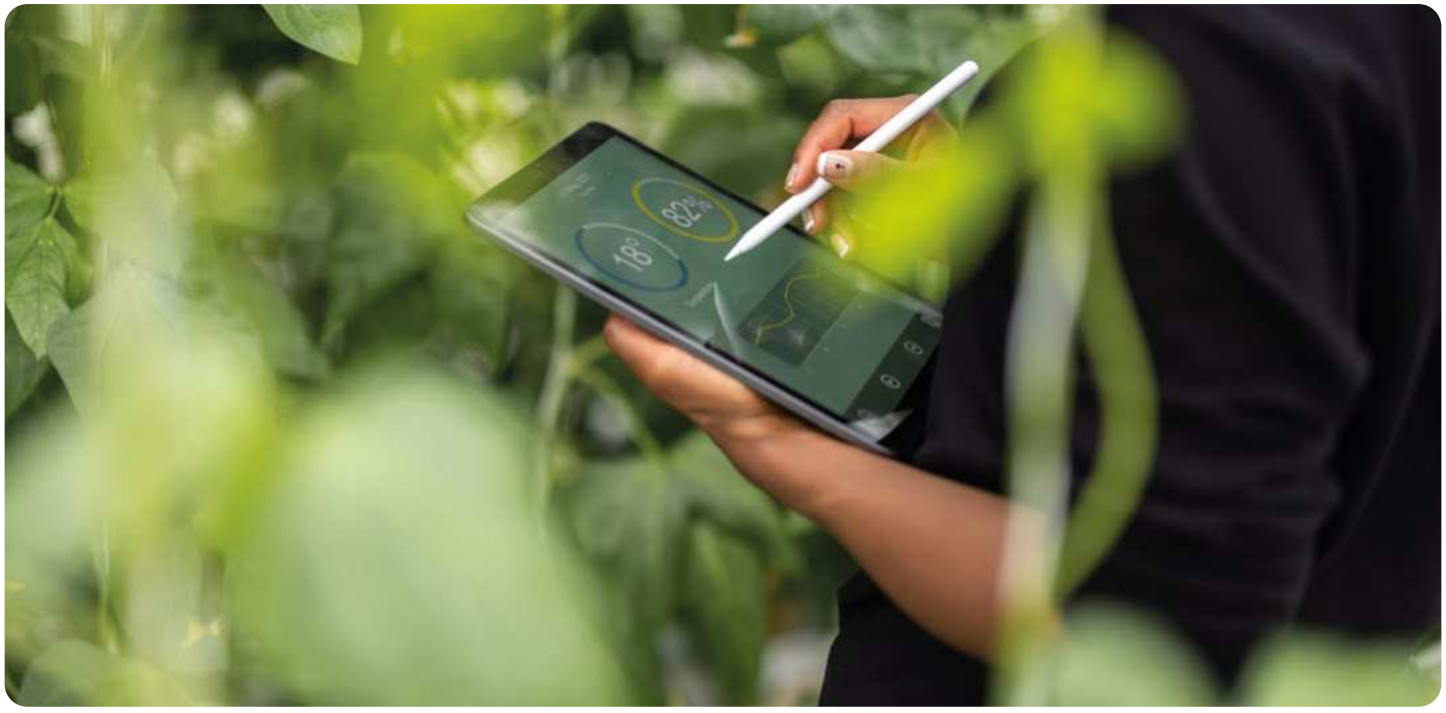
DIVERSITÉ

MIXITÉ

INCLUSION

ÉTHIQUE ET QUALITÉ

PLATEFORMES DE VIGILANCE



La certification qualité a été délivrée au titre des catégories d'actions suivantes : actions de formation (M2i SA, M2i Skills et M2i Scribtel) / actions de formation par apprentissage (M2i Skills et M2i Scribtel).

04

NORMES ET MÉTHODES

Normes et méthodes

Initiation / Fondamentaux

NIS2-ESS — Nouveau
NIS 2 - L'essentiel pour les décideurs
2 jours

SEMI-DORA — Nouveau
DORA - Sensibilisation
1 jour

ISO-27001FND — Nouveau
ISO 27001:2022 - Foundation - Avec certification
2 jours
PECB ISO 27001:2022 Foundation

ISO-27002FND — Nouveau
ISO 27002 - Foundation - Avec certification
2 jours
PECB ISO 27002 Foundation

Fonctionnalités avancées

Norme NIS 2

NIS2-LI — Nouveau
NIS 2 Directive - Lead Implementer - Avec certification
5 jours
Cert. PECB NIS 2 Directive Lead Implementer

Norme DORA

DORA-LM — Nouveau
DORA - Lead Manager - Avec certification
5 jours
Cert. PECB DORA Lead Manager

Norme ISO 27001 / 27002 / 27005 / 27701

ISO-27LI — Top Vente
ISO 27001:2022 - Lead Implementer - Avec certification
5 jours
Cert. PECB 27001 Lead Implementer

ISO-27LA — Top Vente
ISO 27001:2022 - Lead Auditor - Avec certification
5 jours
Cert. PECB 27001 Lead Auditor

ISO-27701LI
ISO 27701 - Lead Implementer - Avec certification
5 jours
Cert. PECB 27701 Lead Implementer

ISO-27RM — Top Vente
ISO 27005 - Risk Manager - Avec certification
3 jours
Cert. PECB 27005 Risk Manager

Norme ISO 22301

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

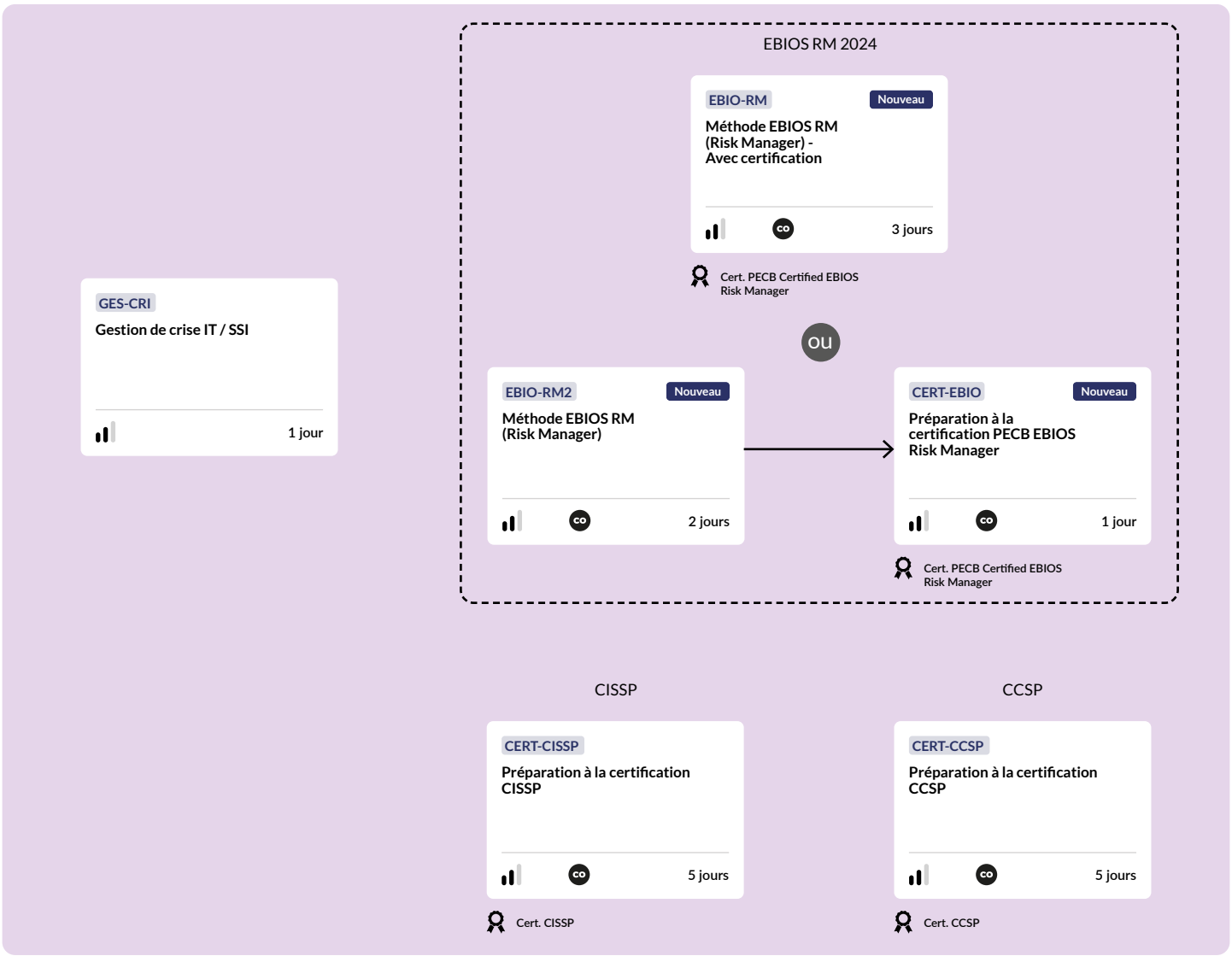
ISO-22LA
ISO 22301 - Lead Auditor - Avec certification
5 jours
Cert. PECB 22301 Lead Auditor

Norme ISO 27032

ISO-27032LCM
ISO 27032 - Lead Cybersecurity Manager - Avec certification
5 jours
Cert. PECB 27032 Lead Cybersecurity Manager

Normes et méthodes

Fonctionnalités avancées



Initiation / Fondamentaux

Nouveau

NIS 2 - L'essentiel pour les décideurs

[NIS2-ESS]

PUBLIC CONCERNÉ

Membres des comités de direction (CEO, CFO, COO...) et responsables des risques, conformité et cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les exigences clés de la Directive NIS 2
- Evaluer son impact sur votre organisation ou vos clients
- Développer une stratégie de mise en conformité
- Vous préparer au mieux aux enjeux stratégiques et opérationnels de la cybersécurité.

PRÉREQUIS

Une bonne compréhension des enjeux globaux de gestion des risques et de conformité, ainsi que la bonne connaissance du cadre réglementaire général applicable à l'entreprise (ex RGPD), sont nécessaires. Avoir une sensibilisation de base aux menaces et principes de cybersécurité et/ou occuper un poste de direction ou de responsabilité stratégique dans l'entreprise seront un plus.

DURÉE

2 jours (14h)

TARIF

1520 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

NIS 2 Directive - Lead Implementer - Avec certification

[NIS2-LI]

CERTIFICATION

PECB NIS 2 Directive Lead Implementer

PUBLIC CONCERNÉ

Professionnels de la cybersécurité cherchant à acquérir une compréhension approfondie des exigences de la directive NIS 2 et à apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes, responsables informatiques et professionnels souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés et améliorer la résilience des systèmes critiques et/ou responsables gouvernementaux et réglementaires chargés de faire appliquer la directive NIS 2.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts fondamentaux de la directive NIS 2 et ses exigences
- Identifier les principes, stratégies, méthodologies et outils nécessaires à la mise en œuvre et à la gestion efficace d'un programme de cybersécurité conformément à la directive NIS 2
- Interpréter et mettre en œuvre les exigences de la directive NIS 2 dans le contexte spécifique d'un organisme
- Initier et planifier la mise en œuvre des exigences de la directive NIS 2, en utilisant la méthodologie de PECB et d'autres bonnes pratiques
- Aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de cybersécurité conformément à la directive NIS 2.

PRÉREQUIS

Avoir une compréhension fondamentale de la cybersécurité.

DURÉE

5 jours (35h)

TARIF

3800 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Nouveau

DORA - Sensibilisation

[SEMI-DORA]

PUBLIC CONCERNÉ

Toute personne souhaitant acquérir des connaissances relatives aux principales exigences du règlement. Responsables de la sécurité de l'information ou équivalent. Consultants, prestataires et tiers intervenant sur les domaines de la gouvernance SSI.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les enjeux et les exigences du règlement
- Identifier les bonnes pratiques de résilience opérationnelle
- Mettre en œuvre un projet de mise en conformité
- Piloter votre mise en conformité avec les parties prenantes.

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

DURÉE

1 jour (7h)

TARIF

700 €HT

LES PLUS DE LA FORMATION

Cours magistral interactif avec des exemples et des travaux pratiques.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

DORA - Lead Manager - Avec certification

[DORA-LM]

CERTIFICATION

PECB DORA Lead Manager

PUBLIC CONCERNÉ

Cadres supérieurs et décideurs des institutions financières, responsables de la conformité et gestionnaires de risques, professionnels des TI, personnels des affaires juridiques et réglementaires, consultants et conseillers spécialisés dans la règlementation financière et la cybersécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer le paysage règlementaire et les exigences en matière de conformité du règlement DORA, se basant sur cinq piliers fondamentaux, parmi lesquels la gestion des risques liés aux TIC, la gestion et la notification des incidents liés aux TIC, les tests de résilience opérationnelle numérique et la gestion des risques liés aux prestataires tiers
- Mettre en œuvre des stratégies et mesures pour améliorer la résilience opérationnelle et atténuer les risques liés aux TIC dans les institutions financières, en se conformant aux exigences de DORA et aux meilleures pratiques du secteur
- Identifier, analyser, évaluer et gérer les risques liés aux TIC qui concernent les entités financières
- Développer et maintenir des cadres robustes de gestion des risques liés aux TIC, des plans de réponse en cas d'incident et des plans de continuité opérationnelle et de reprise après sinistre
- Favoriser la collaboration et la communication avec les principales parties prenantes pour réussir la mise en œuvre et le respect permanent de DORA
- Utiliser des outils et des méthodologies du secteur pour suivre, évaluer et gérer les risques et les vulnérabilités liés aux TIC, améliorant la posture de sécurité globale des institutions financières.

PRÉREQUIS

Avoir une compréhension fondamentale des concepts de la sécurité de l'information et de la cybersécurité et être familiarisé avec les principes de gestion des risques liés aux TIC.

DURÉE

5 jours (35h)

TARIF

3800 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Nouveau Cours Officiel

ISO 27001:2022 - Foundation - Avec certification

[ISO-27001FND]

CERTIFICATION

PECB ISO 27001:2022 Foundation

PUBLIC CONCERNÉ

Toute personne impliquée dans le management de la sécurité de l'information ou souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information et/ou poursuivre une carrière dans le management de la sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les éléments et le fonctionnement d'un système de management de la sécurité de l'information
- Expliquer la corrélation entre la norme ISO/IEC 27001:2022 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres règlementaires
- Décrire les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un système de management de la sécurité de l'information.

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

DURÉE

2 jours (14h)

TARIF

1500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Initiation / Fondamentaux

Nouveau Cours Officiel

ISO 27002 - Foundation - Avec certification

[ISO-27002FND]

CERTIFICATION

PECB ISO 27002 Foundation

PUBLIC CONCERNÉ

Managers et consultants souhaitant en savoir plus sur les mesures de sécurité de l'information de la norme ISO/IEC 27002. Professionnels impliqués ou responsables dans le domaine de gestion de la sécurité de l'information. Toute personne souhaitant acquérir des connaissances sur les principaux processus d'un système de management de la sécurité de l'information et sur les mesures de sécurité de l'information, et/ou toute personne souhaitant poursuivre une carrière dans le domaine de la sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée basés sur la norme ISO/IEC 27002
- Discuter de la corrélation entre les normes ISO/IEC 27001 et ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Interpréter les mesures de sécurité organisationnelles, applicables aux personnes, physiques et technologiques de la norme ISO/IEC 27002 dans le contexte spécifique d'un organisme.

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

DURÉE

2 jours (14h)

TARIF

1500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente Cours Officiel

ISO 27001:2022 - Lead Implementer - Avec certification

[ISO-27LI]

CERTIFICATION

PECB 27001 Lead Implementer

PUBLIC CONCERNÉ

Chefs de projets, consultants, conseillers experts, personnes chargées d'assurer la conformité aux exigences de sécurité de l'information au sein d'un organisme, ou membres d'une équipe de mise en œuvre d'un SMSI.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et le management efficace d'un SMSI (Système de Management de la Sécurité de l'Information)
- Reconnaître la corrélation entre les normes ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Décrire le fonctionnement d'un SMSI et ses processus, conformément à la norme ISO/IEC 27001
- Interpréter et mettre en œuvre les exigences d'ISO/IEC 27001 dans le contexte spécifique d'un organisme
- Aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un SMSI.

PRÉREQUIS

Avoir une bonne connaissance de la norme ISO/IEC 27001 et des connaissances approfondies sur les principes de mise en œuvre. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente Cours Officiel

ISO 27001:2022 - Lead Auditor - Avec certification

[ISO-27LA]

CERTIFICATION

PECB 27001 Lead Auditor

PUBLIC CONCERNÉ

Auditeurs, managers ou consultants souhaitant maîtriser le processus d'audit d'un SMSI, responsables du maintien de la conformité aux exigences du SMSI, experts techniques souhaitant se préparer à un audit du SMSI et/ou conseillers experts en management de sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et les principes fondamentaux d'un SMSI (Système de Management de la Sécurité de l'Information) basé sur ISO 27001
- Interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur
- Evaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO/IEC 27001.

PRÉREQUIS

Avoir une bonne connaissance de la norme ISO/IEC 27001 et avoir des connaissances approfondies sur les principes de l'audit. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

ISO 27701 - Lead Implementer - Avec certification

[ISO-27701LI]

CERTIFICATION

PECB 27701 Lead Implementer

PUBLIC CONCERNÉ

Superviseurs et consultants impliqués dans la confidentialité et la gestion des données, experts-conseils cherchant à maîtriser la mise en œuvre d'un système de management de la protection de la vie privée, responsables des informations personnellement identifiables (IPI) au sein des organisations, responsables de la conformité aux exigences des lois de protection des données, membres de l'équipe PIMS.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Présenter les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS
- Identifier la corrélation entre ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Décrire le fonctionnement d'un PIMS basé sur ISO/CEI 27701 et ses processus principaux
- Interpréter les exigences d'ISO/IEC 27701 dans le contexte spécifique d'une organisation
- Développer l'expertise nécessaire pour aider une organisation à planifier, mettre en œuvre, surveiller et gérer efficacement un PIMS.

PRÉREQUIS

Avoir une compréhension fondamentale de la sécurité de l'information et une connaissance approfondie des principes de mise en œuvre du SMSI. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente Cours Officiel

ISO 27005 - Risk Manager - Avec certification

[ISO-27RM]

CERTIFICATION

PECB 27005 Risk Manager

PUBLIC CONCERNÉ

Responsables ou consultants impliqués dans la sécurité de l'information dans un organisme, responsables de la gestion des risques liés à la sécurité de l'information, membres des équipes de sécurité de l'information, professionnels de l'informatique et responsables de la protection de la vie privée, responsables du maintien de la conformité aux exigences de sécurité de l'information de la norme ISO/IEC 27001 au sein d'un organisme, gestionnaires de projets, consultants ou conseillers experts cherchant à maîtriser la gestion des risques liés à la sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et principes de gestion des risques tels que définis par les normes ISO/IEC 27005 et ISO 31000
- Etablir, maintenir et améliorer un cadre de gestion des risques liés à la sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27005
- Appliquer des processus de gestion des risques liés à la sécurité de l'information sur la base des lignes directrices de la norme ISO/IEC 27005
- Planifier et mettre en place des activités de communication et de consultation sur les risques.

PRÉREQUIS

Avoir des connaissances fondamentales de la norme ISO/IEC 27005 et des connaissances approfondies sur l'appréciation du risque et la sécurité de l'information. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

3 jours (21h)

TARIF

2150 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

ISO 22301 - Lead Implementer - Avec certification

[ISO-22LI]

CERTIFICATION

PECB 22301 Lead Implementer

PUBLIC CONCERNÉ

Responsables ou consultants impliqués dans la continuité d'activité, personnes désireuses de maîtriser la mise en œuvre d'un système de management de la continuité d'activité, personnes chargées d'assurer et de maintenir la conformité aux exigences du SMCA au sein d'un organisme ou toute personne ayant des rôles ou responsabilités liés au SMCA.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) conformément à la norme ISO 22301
- Interpréter les exigences de la norme ISO 22301 pour un SMCA du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMCA conformément à la norme ISO 22301
- Appliquer les bonnes pratiques pour soutenir l'efficacité et l'amélioration continues d'un SMCA conformément à la norme ISO 22301
- Interpréter les exigences pour un audit de certification à la norme ISO 22301.

PRÉREQUIS

Avoir une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de sa mise en œuvre. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

ISO 22301 - Lead Auditor - Avec certification

[ISO-22LA]

CERTIFICATION

PECB 22301 Lead Auditor

PUBLIC CONCERNÉ

Auditeurs souhaitant réaliser et diriger des audits de SMCA, managers ou consultants désirant maîtriser le processus d'audit du SMCA, experts techniques désirant préparer un audit du SMCA, conseillers experts en management de la continuité d'activité ou toute personne responsable du maintien de la conformité aux exigences du SMCA dans un organisme.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et les principes fondamentaux d'un système de management de la continuité d'activité (SMCA) conformément à la norme ISO 22301
- Interpréter les exigences de la norme ISO 22301 pour un SMCA du point de vue d'un auditeur
- Evaluer la conformité du SMCA aux exigences de la norme ISO 22301, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à la norme ISO 22301, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO 22301.

PRÉREQUIS

Avoir une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

ISO 27032 - Lead Cybersecurity Manager - Avec certification

[ISO-27032LCM]

CERTIFICATION

PECB 27032 Lead Cybersecurity Manager

PUBLIC CONCERNÉ

Professionnels de la cybersécurité, experts en sécurité de l'information, professionnels souhaitant gérer un programme de cybersécurité, responsables du développement d'un programme de cybersécurité, spécialistes IT, conseillers spécialisés dans l'IT, professionnels IT souhaitant accroître leurs connaissances et compétences techniques.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Définir de façon approfondie les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST (National Institute of Standards and Technology)
- Décrire l'objectif, le contenu et la corrélation entre l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST ainsi qu'avec d'autres normes et cadres opérationnels
- Identifier les concepts, les approches, les normes, les méthodes et les techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation
- Interpréter les lignes directrices de l'ISO/IEC 27032 dans le contexte spécifique d'une organisation
- Planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST
- Conseiller une organisation sur les bonnes pratiques de gestion de la cybersécurité.

PRÉREQUIS

Avoir une connaissance fondamentale sur la norme ISO/IEC 27032 et des connaissances approfondies sur la cybersécurité. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3500 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Gestion de crise IT / SSI

[GES-CRI]

PUBLIC CONCERNÉ

Responsables des SI, directeurs des SI, dirigeants, RSSI / CISO (responsables de la sécurité des SI).

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les méthodes de cyberattaque utilisées
- Estimer les conséquences que peut avoir une attaque informatique
- Expliquer le rôle des mécanismes de protection informatique
- Vous prémunir d'une attaque informatique
- Décrire le concept de risque cyber.

PRÉREQUIS

Avoir une connaissance technique de base des SI (Systèmes d'Information).

DURÉE

1 jour (7h)

TARIF

760 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Méthode EBIOS RM (Risk Manager) - Avec certification

[EBIO-RM]

CERTIFICATION

PECB Certified EBIOS Risk Manager

PUBLIC CONCERNÉ

Toute personne souhaitant apprendre et comprendre les concepts de base de la gestion des risques et/ou participant à des activités d'évaluation des risques à l'aide de la méthode EBIOS. Managers cherchant à comprendre les techniques permettant de réaliser une évaluation des risques basée sur la méthode EBIOS et/ou managers souhaitant maîtriser les techniques d'analyse et de communication des résultats d'une évaluation des risques basée sur la méthode EBIOS.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et principes de base de la gestion des risques associés à l'utilisation de la méthode EBIOS
- Décrire les activités de la méthode EBIOS afin de suivre la réalisation d'études (pilote, contrôle, recadrage) en tant que maître d'œuvre
- Interpréter et expliquer les résultats d'une étude EBIOS et ses principaux livrables
- Réaliser une étude EBIOS
- Gérer les risques de sécurité des systèmes d'information d'une organisation
- Analyser et communiquer les résultats d'une étude EBIOS.

PRÉREQUIS

Avoir une connaissance fondamentale de la gestion des risques.

DURÉE

3 jours (21h)

TARIF

2550 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Méthode EBIOS RM (Risk Manager)

[EBIO-RM2]

PUBLIC CONCERNÉ

Toute personne souhaitant apprendre et comprendre les concepts de base de la gestion des risques et/ou participant à des activités d'évaluation des risques à l'aide de la méthode EBIOS. Managers cherchant à comprendre les techniques permettant de réaliser une évaluation des risques basée sur la méthode EBIOS et/ou managers souhaitant maîtriser les techniques d'analyse et de communication des résultats d'une évaluation des risques basée sur la méthode EBIOS.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Expliquer les concepts et principes de base de la gestion des risques associés à l'utilisation de la méthode EBIOS
- Décrire les activités de la méthode EBIOS afin de suivre la réalisation d'études (pilote, contrôle, recadrage) en tant que maître d'œuvre
- Interpréter et expliquer les résultats d'une étude EBIOS et ses principaux livrables
- Réaliser une étude EBIOS
- Gérer les risques de sécurité des systèmes d'information d'une organisation
- Analyser et communiquer les résultats d'une étude EBIOS.

PRÉREQUIS

Avoir une connaissance fondamentale de la gestion des risques.

DURÉE

2 jours (14h)

TARIF

1700 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Préparation à la certification PECB EBIOS Risk Manager

[CERT-EBIO]

CERTIFICATION

PECB Certified EBIOS Risk Manager

PUBLIC CONCERNÉ

Toute personne souhaitant apprendre et comprendre les concepts de base de la gestion des risques et/ou participant à des activités d'évaluation des risques à l'aide de la méthode EBIOS. Managers cherchant à comprendre les techniques permettant de réaliser une évaluation des risques basée sur la méthode EBIOS et/ou managers souhaitant maîtriser les techniques d'analyse et de communication des résultats d'une évaluation des risques basée sur la méthode EBIOS.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser la méthode EBIOS Risk Manager
- Réaliser une étude EBIOS
- Analyser et communiquer les résultats d'une étude EBIOS
- Passer la certification EBIOS Risk Manager.

PRÉREQUIS

Avoir suivi la formation EBIO-RM2 « Méthode EBIOS RM (Risk Manager 4.2) » ou avoir les connaissances équivalentes.

DURÉE

1 jour (7h)

TARIF

850 €HT

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Préparation à la certification CISSP

[CERT-CISSP]

CERTIFICATION

CISSP

PUBLIC CONCERNÉ

Directeurs de l'information, responsables de la sécurité de l'information, responsables de la technologie, responsables / agents de la conformité, architectes de l'information, spécialistes / gestionnaires de l'information, consultants en matière de risques liés à l'information, administrateurs de la sécurité, architectes / analystes de la sécurité, consultants en sécurité, directeurs de la sécurité, ingénieurs en systèmes de sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Appliquer les concepts et méthodes fondamentaux liés aux domaines des technologies de l'information et de la sécurité
- Aligner les objectifs opérationnels globaux de l'organisation avec les fonctions et les mises en œuvre de la sécurité
- Protéger les actifs de l'organisation au cours de leur cycle de vie
- Exploiter les concepts, principes, structures et normes utilisés pour concevoir, mettre en œuvre, surveiller et sécuriser les systèmes d'exploitation, les équipements, les réseaux, les applications et les contrôles utilisés pour appliquer divers niveaux de confidentialité, d'intégrité et de disponibilité
- Appliquer les principes de conception de la sécurité pour choisir les mesures d'atténuation appropriées des vulnérabilités présentes dans les types et les architectures de systèmes d'information courants
- Expliquer l'importance de la cryptographie et des services de sécurité qu'elle peut fournir à l'ère du numérique et de l'information
- Evaluer les éléments de sécurité physique par rapport aux besoins des systèmes d'information
- Evaluer les éléments qui composent la sécurité des communications et des réseaux par rapport aux besoins de sécurité de l'information
- Exploiter les concepts et l'architecture qui définissent les systèmes et les protocoles de technologie et de mise en œuvre associés aux couches 1 à 7 du modèle OSI (Open Systems Interconnection) pour répondre aux besoins de sécurité de l'information
- Déterminer les modèles de contrôle d'accès appropriés pour répondre aux besoins de sécurité de l'entreprise
- Appliquer les modèles de contrôle d'accès physique et logique pour répondre aux besoins de sécurité de l'information
- Différencier les principales méthodes de conception et de validation des stratégies de test et d'audit qui répondent aux exigences de sécurité de l'information
- Appliquer les contrôles et contre-mesures de sécurité appropriés pour optimiser la fonction et la capacité de fonctionnement d'une organisation
- Evaluer les risques liés aux systèmes d'information pour les activités opérationnelles d'une organisation
- Déterminer les contrôles appropriés pour atténuer les menaces et les vulnérabilités spécifiques
- Appliquer les concepts de sécurité des systèmes d'information pour atténuer le risque de vulnérabilité des logiciels et des systèmes tout au long du cycle de vie des systèmes
- Passer l'examen CISSP.

PRÉREQUIS

Avoir une bonne connaissance des systèmes d'information ainsi qu'une expérience technique et managériale approfondie pour concevoir, développer et gérer la posture de sécurité globale d'une organisation. La lecture du support de cours officiel de l'ISC (CBK) est fortement recommandée.

DURÉE

5 jours (35h)

TARIF

4100 €HT

LES PLUS DE LA FORMATION

Un minimum de 4 personnes sera nécessaire pour maintenir la session.

De plus, il est très important de noter que pour chaque inscription, un délai de 10 jours (minimum) est imposé par l'éditeur avant d'obtenir les documents pédagogiques (donc pas d'inscription possible à moins de 10 jours).

Le support de cours est en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Préparation à la certification CCSP

[CERT-CCSP]

CERTIFICATION

CCSP

PUBLIC CONCERNÉ

Architectes d'entreprise, architectes / administrateurs / ingénieurs / consultants / responsables de sécurité, ingénieurs / architectes systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les composants physiques et virtuels et identifier les principales technologies des systèmes basés sur le Cloud
- Définir les rôles et les responsabilités des clients, des fournisseurs, des partenaires, des courtiers et des divers professionnels techniques qui prennent en charge les environnements Cloud Computing
- Identifier et expliquer les cinq caractéristiques requises pour répondre à la définition du NIST (National Institute of Standards and Technology) du Cloud Computing
- Différencier les modèles de prestation de services et les frameworks qui sont incorporés dans l'architecture de référence du Cloud Computing
- Discuter des stratégies de sauvegarde des données, de classification des données, de protection de la confidentialité, de conformité avec les organismes de réglementation et de collaboration avec les autorités lors d'enquêtes judiciaires
- Différencier l'analyse forensic dans les Data Centers d'entreprise et les environnements Cloud Computing
- Evaluer et mettre en œuvre les contrôles de sécurité nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité dans le cadre du Cloud Computing
- Identifier et expliquer les six phases du cycle de vie des données
- Expliquer les stratégies de protection des données au repos et des données en mouvement
- Décrire le rôle du cryptage dans la protection des données et les stratégies spécifiques de gestion des clés
- Comparer diverses stratégies Business Continuity et Disaster Recovery basées sur le Cloud et sélectionner une solution appropriée aux besoins spécifiques de l'entreprise
- Comparer les aspects de sécurité du SDLC (Software Development Life Cycle) dans les environnements standard du Data Center et du Cloud Computing
- Décrire comment les solutions de gestion des identités fédérées et des accès atténuent les risques dans les systèmes du Cloud Computing
- Effectuer une analyse des écarts entre les pratiques de référence et les bonnes pratiques du secteur
- Développer des SLA (Service Level Agreements) pour les environnements Cloud Computing
- Réaliser des évaluations de risques des environnements Cloud existants et proposés
- Enoncer les normes professionnelles et éthiques de (ISC)² et de la certification CCSP.

PRÉREQUIS

Avoir un minimum de cinq années cumulées d'expérience professionnelle rémunérée dans le domaine des technologies de l'information, dont trois ans en sécurité de l'information et un an dans un ou plusieurs des six domaines de la norme CCSP CBK, ou être certifié CISSP.

DURÉE

5 jours (35h)

TARIF

4100 €HT

LES PLUS DE LA FORMATION

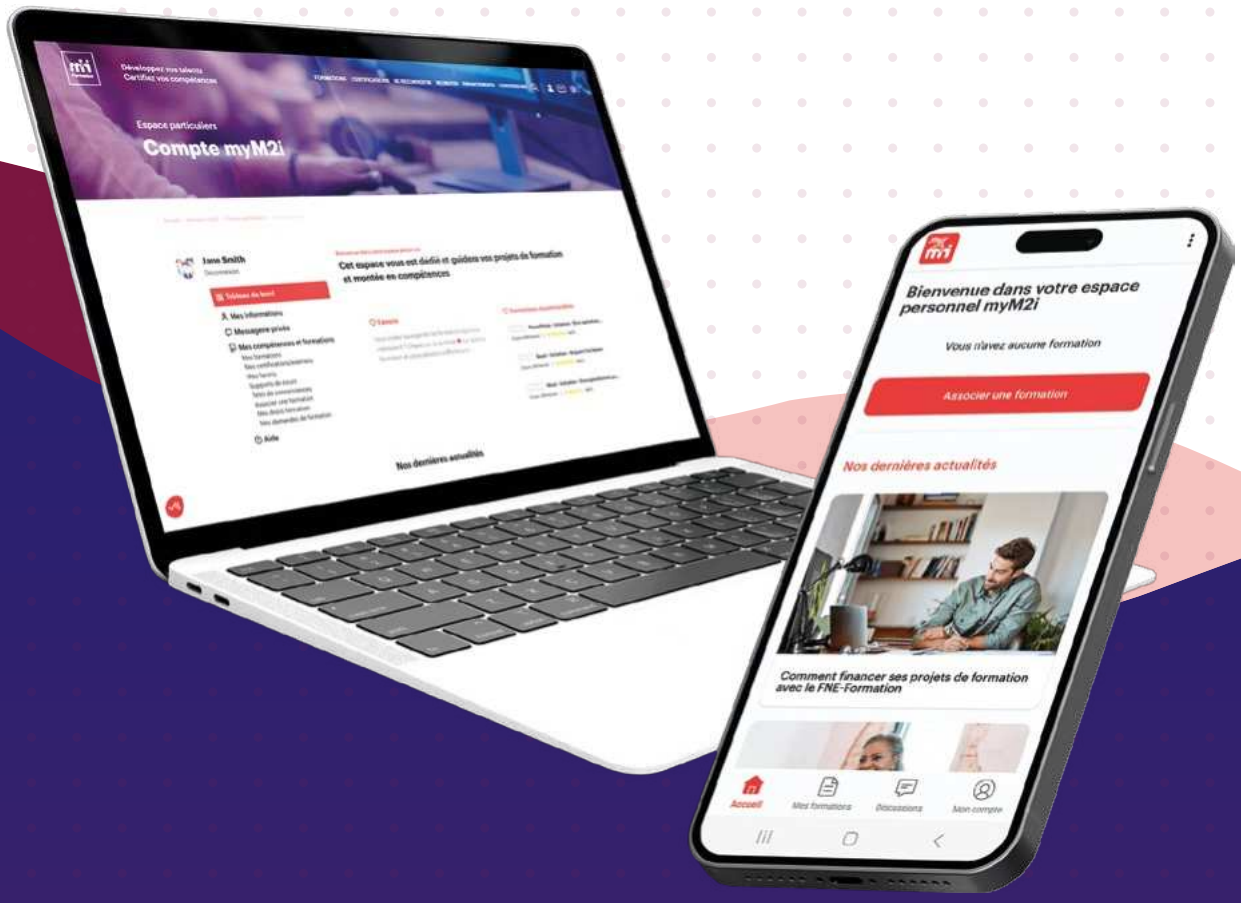
Un minimum de 4 personnes sera nécessaire pour maintenir la session.

De plus, il est très important de noter que pour chaque inscription, un délai de 10 jours (minimum) est imposé par l'éditeur avant d'obtenir les documents pédagogiques (donc pas d'inscription possible à moins de 10 jours).

Le support de cours est en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Téléchargez dès maintenant votre application myM2i !



Immergez-vous dans une expérience de formation interactive et personnalisée.

Télécharger dans l'App Store

DISPONIBLE SUR Google Play

m2iformation.fr

05

JURIDIQUE :
RGPD ET DPO

Juridique : RGPD et DPO

Fonctionnalités avancées

SEMI-RGPD

RGPD -
Sensibilisation

1 jour

RGPD-EURO

RGPD -
Les éléments fondamentaux du texte européen

1 jour

DPO-PECB

RGPD / GDPR -
DPO -
Avec certification

5 jours

Cert. PECB Certified Data Protection Officer

RGPD - Sensibilisation

[SEMI-RGPD]

PUBLIC CONCERNÉ

Toute personne souhaitant se sensibiliser à la RGPD.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

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

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

DURÉE

1 jour (7h)

TARIF

760 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

RGPD - Les éléments fondamentaux du texte européen

[RGPD-EURO]

PUBLIC CONCERNÉ

DPO, responsables de traitement, chefs de projets, RSSI et/ou sous-traitants.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Proposer une vision globale des obligations du RGPD dans la protection des données au regard des ressources humaines et déterminer les informations et les documents nécessaires à la gestion des processus de collecte d'informations personnelles des salariés et des clients de l'entreprise (information, consentement, retrait du consentement...)
- Définir une donnée personnelle et les finalités de traitement, reconnaître les obligations des responsables de traitement (Art. 24, Art. 28) et identifier les études d'impact sur la vie privée
- Expliquer les concepts d'Accountability, de « privacy by default » et « privacy by design » (Art. 25) et d'analyse d'impact sur la vie privée (Art. 35)
- Exploiter la notion de risque et identifier une violation de données personnelles (Art. 32)
- Réagir à une violation de données personnelles (procédure, données à collecter, notion de preuve...).

PRÉREQUIS

Cette formation ne nécessite pas de prérequis.

DURÉE

1 jour (7h)

TARIF

760 €HT

LES PLUS DE LA FORMATION

Principe d'animation de cet atelier :

- La présentation magistrale d'un consultant certifié DPO
- Des exercices de compréhension
- La présentation des Normes Simplifiées de la CNIL comme guide rédactionnel

Support et outils mis à disposition :

- La présentation effectuée par le consultant au format PDF
- L'article 4 du Règlement Européen de Protection des Données personnelles
- Bibliographie Web des documents complémentaires à l'atelier

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

RGPD / GDPR - DPO - Avec certification

[DPO-PECB]

CERTIFICATION

PECB Certified Data Protection Officer

PUBLIC CONCERNÉ

Responsables de projets ou consultants souhaitant préparer et soutenir un organisme dans la mise en œuvre des nouvelles procédures et l'adoption des nouvelles exigences présentées dans le RGPD (en vigueur depuis le 25 mai 2018). DPD (Délégués à la Protection des Données) et cadres supérieurs chargés de la protection des données personnelles d'une entreprise et de la gestion de ses risques. Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité des affaires. Conseillers experts en sécurité des données personnelles, experts techniques et experts de la conformité envisageant un poste de DPD.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire l'histoire de la protection des données personnelles en Europe
- Identifier les concepts et approches nécessaires à l'alignement efficace avec le RGPD (Règlement Général sur la Protection des Données)
- Reconnaître les nouvelles exigences que le RGPD apporte aux organisations de l'UE et aux organisations hors UE et, lorsqu'il est nécessaire, les mettre en œuvre
- Aider un organisme à évaluer la mise en œuvre de ces nouvelles exigences
- Gérer une équipe implémentant le RGPD
- Conseiller les organismes sur la gestion des données personnelles
- Mettre en œuvre l'expertise nécessaire pour l'analyse et la prise de décision dans le contexte de la protection des données personnelles.

PRÉREQUIS

Avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données. De plus, pour l'obtention de la certification, il est obligatoire de justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles ; ou justifier d'une expérience professionnelle d'au moins 2 ans ainsi que d'une formation d'au moins 35 heures en matière de protection des données personnelles (reçue par un organisme de formation). Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (35h)

TARIF

3800 €^{HT}

LES PLUS DE LA FORMATION

Ce cours est animé par un formateur certifié PECB.

Consultez le programme détaillé et les prochaines dates en scannant ce code

06

OFFRE
ÉDITEURS

Offre éditeurs

Expertise / Spécialisation

Microsoft

MSSC900 — Nouveau
Les fondamentaux de Microsoft en matière de sécurité, conformité et identité
1 jour

WS25-SEC — Nouveau
Windows Server 2022 / 2025 - Sécurité - Niveau 1
4 jours

WS25-SEC2 — Nouveau
Windows Server 2022 / 2025 - Sécurité - Niveau 2
5 jours

Cert. Microsoft SC-900

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

MSAZ500
Microsoft Azure - Security Technologies
4 jours

Cert. Microsoft AZ-500

MSSC100 — Nouveau
Architecte en cybersécurité Microsoft
4 jours

Cert. Microsoft SC-100

LogPoint

LOG-ADM
LogPoint - Administrateur
2 jours

Cert. LogPoint Certified Administrator

LOG-UT
LogPoint - Utilisateur
2 jours

Cert. LogPoint Certified User

Check Point

CHK81-ADM
Check Point - Certified Security Administrator R81.x
3 jours

Cert. CCSA

→

CHK81-EXP
Check Point - Certified Security Expert R81.x
3 jours

Cert. CCSE

Red Hat

RH415
Red Hat Security - Linux in Physical, Virtual, and Cloud
5 jours (26h15)

ou

RH416
Red Hat Security - Linux in Physical, Virtual, and Cloud (RH415) + examen (EX415)
5,5 jours (30h15)

Cert. EX415

Fortinet

FGT-ADMIN — Top Vente — Nouveau
Fortinet NSE 4 - FortiGate Administrator
4 jours

\+ ou

FGT-MANAG — Nouveau
Fortinet NSE 5 - FortiManager Administrator
2 jours

FGT-ANALY — Nouveau
Fortinet NSE 6 - FortiAnalyzer Administrator
1 jour

= Fortinet Certified Professional (FCP) Network Security

Offre éditeurs

Fonctionnalités avancées

EGERIE

EGERIE-ISO
EGERIE Risk Manager avec ISO 27005
CO — 2 jours

EGERIE-EBIOS
EGERIE Risk Manager v4 avec EBIOS RM - Avec certification
CO — 2 jours

Cert. EGERIE Risk Manager v4

Trellix Endpoint Forensics (HX)

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

MCA-DLP
Trellix Data Loss Prevention Endpoint - Administration
CO — 4 jours

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

TRELL-EDR Nouveau
Trellix Endpoint Detection and Response (EDR) - Administration
CO — 2 jours

MCA-VS
Trellix ePolicy Orchestrator - Administration
CO — 5 jours

→

TRELL-EPOAV Nouveau
Trellix ePolicy Orchestrator - Advanced Topics
CO — 4 jours

Splunk

SPLUNK-ESS
Splunk - Les essentiels
3 jours

→

SPLUNK-AV Nouveau
Splunk - Niveau avancé
3 jours

SonicWall

SNSA
SonicWall Network Security Administrator
CO — 2 jours

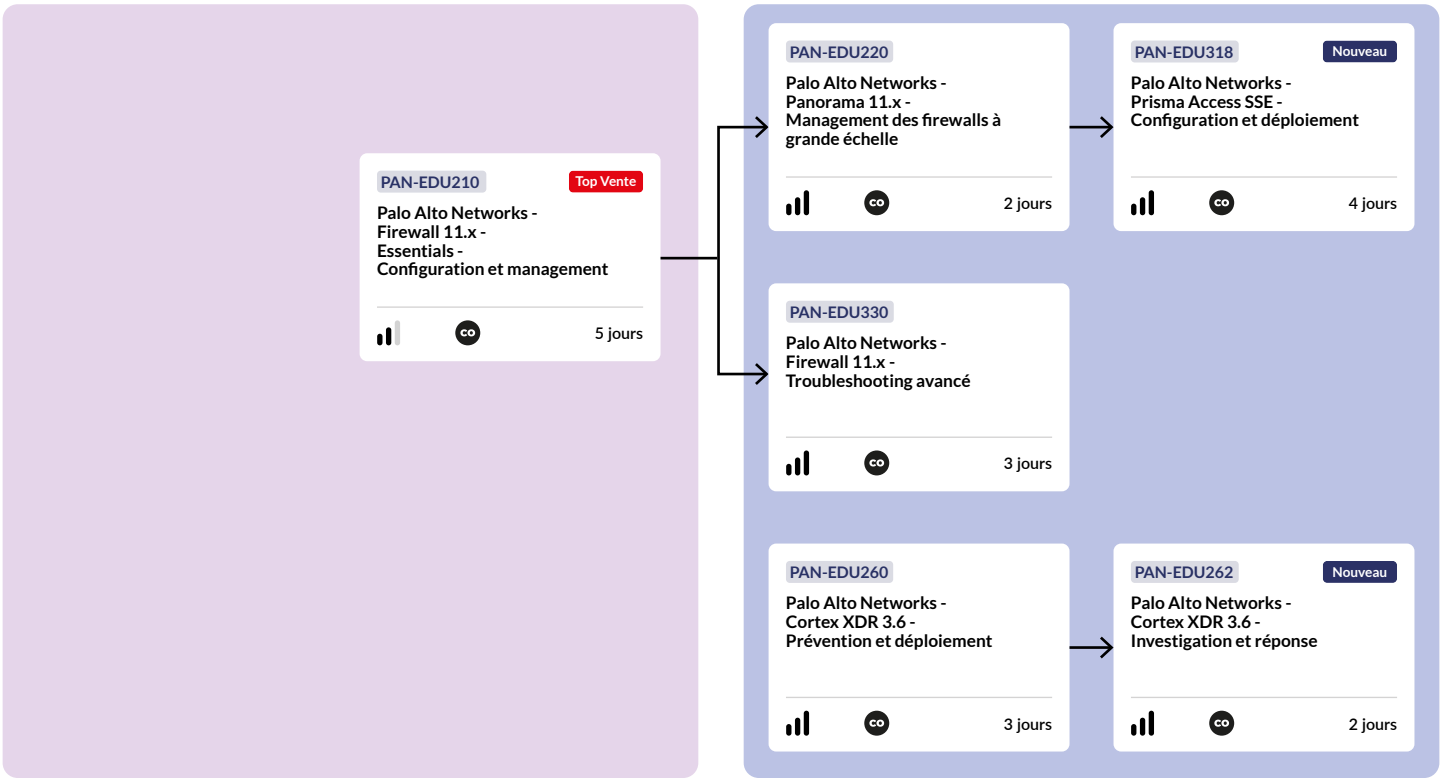
Cert. CSSA

Offre éditeurs

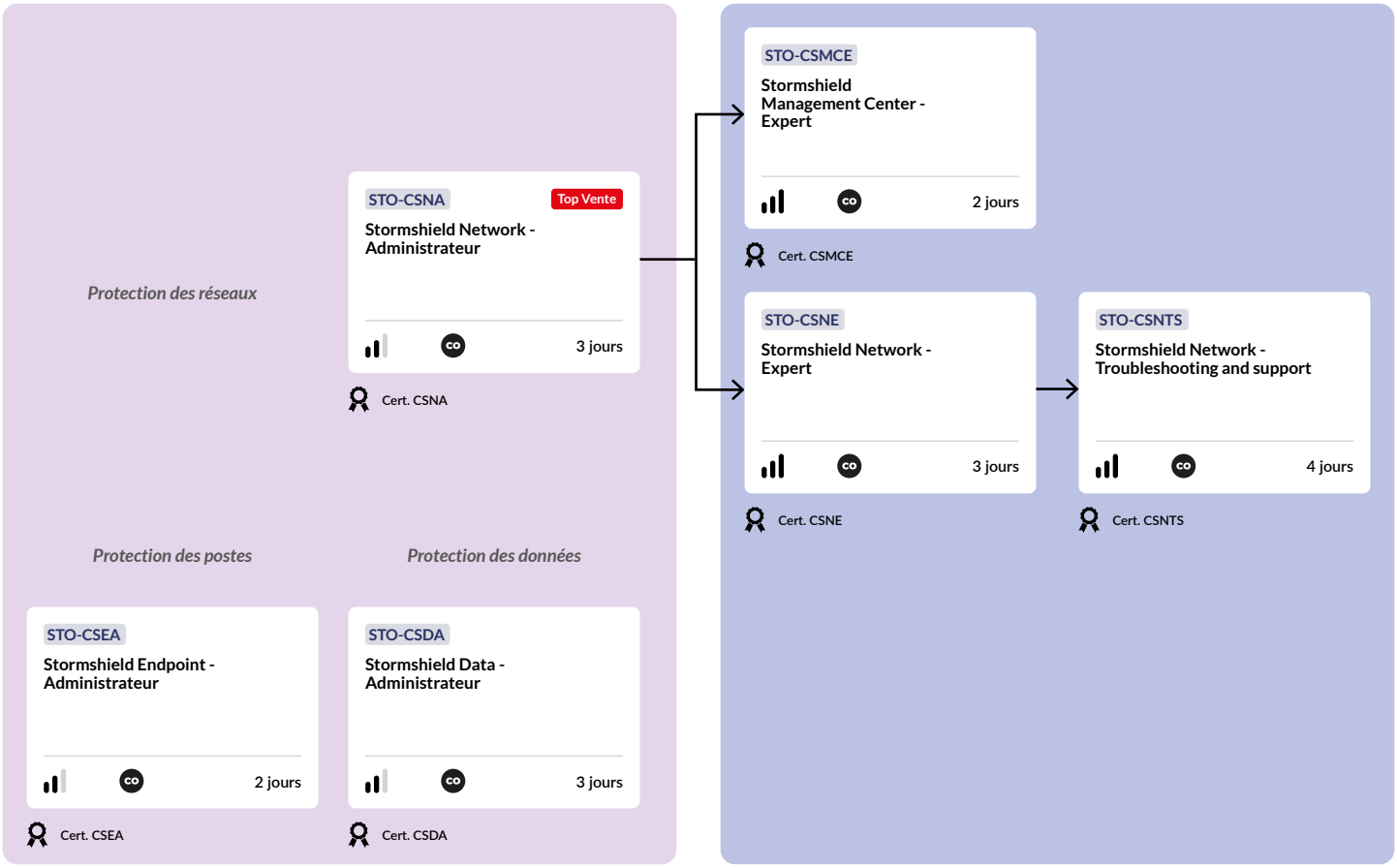
Fonctionnalités avancées

Expertise / Spécialisation

Palo Alto Networks



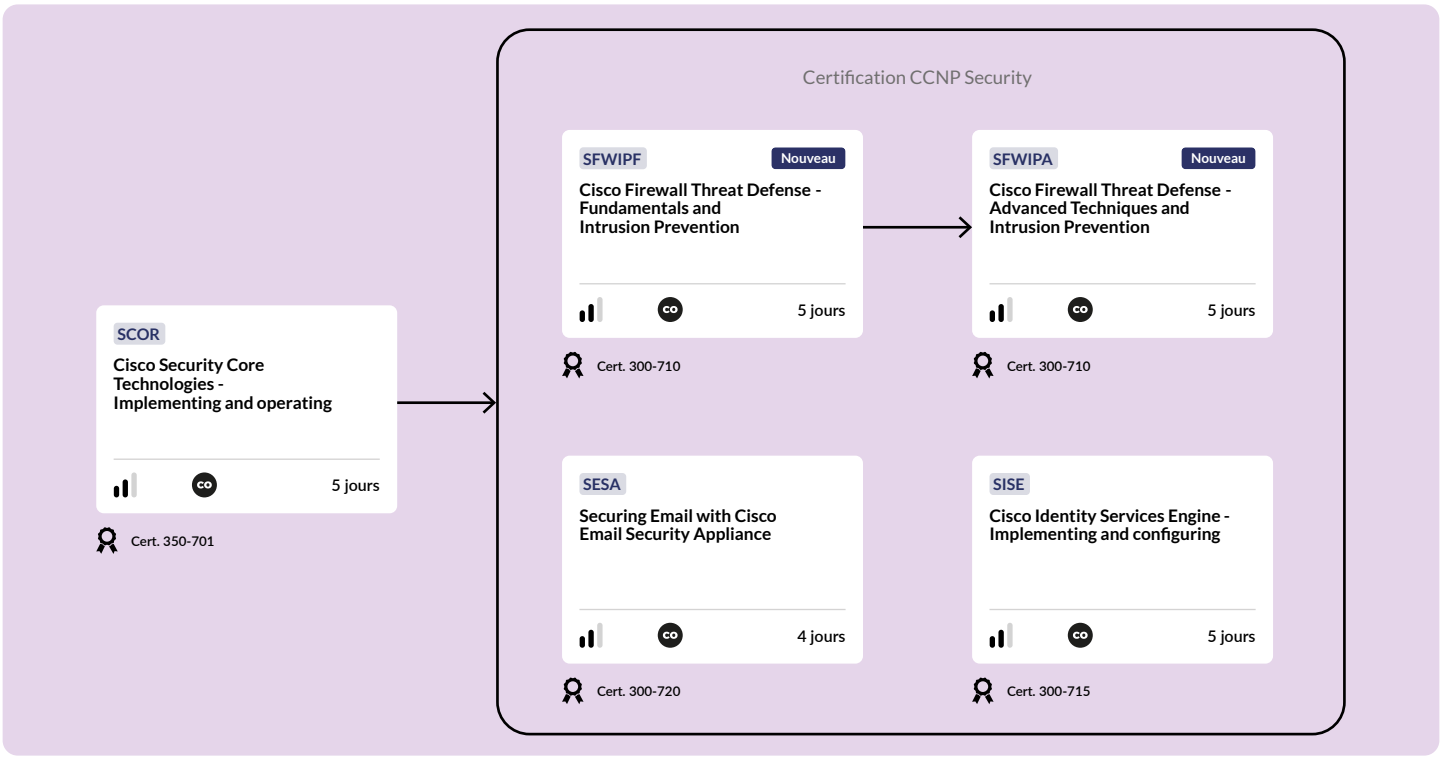
Stormshield



Offre éditeurs

Fonctionnalités avancées

Cisco



Expertise / Spécialisation

Nouveau Cours Officiel

Les fondamentaux de Microsoft en matière de sécurité, conformité et identité

[MSSC900]

CERTIFICATION

Microsoft SC-900 *(tarif : 200€)*

PUBLIC CONCERNÉ

Toute personne souhaitant se familiariser avec les principes fondamentaux de la sécurité, de la conformité et de l'identité (SCI) à travers le Cloud et les services Microsoft associés.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les concepts clés qui constituent la base des solutions de sécurité, de conformité et d'identité, notamment la responsabilité partagée, la Confiance Zéro, la résidence des données, le rôle des fournisseurs d'identités et plus encore
- Gérer les identités et les accès sur Microsoft Entra ID
- Découvrir les services Microsoft Entra et les principes d'identité, l'authentification sécurisée, les capacités de gestion des accès ainsi que la protection et la gouvernance des identités
- Explorer les fonctionnalités de sécurité de Microsoft (fonctionnalités de réseau et de plateforme d'Azure, gestion de la sécurité Azure et Sentinel, protection contre les menaces avec Microsoft Defender XDR et gestion de la sécurité Microsoft 365)
- Découvrir les solutions de conformité dans Microsoft (portail de conformité Microsoft Purview, protection et gouvernance des données dans Microsoft 365, risques internes, audits et solutions eDiscovery).

PRÉREQUIS

Avoir une compréhension générale des concepts des réseaux et du Cloud Computing et de Microsoft Azure et Microsoft 365, ainsi qu'une connaissance générale en informatique.

DURÉE

1 jour (7h)

TARIF

710 €HT

LES PLUS DE LA FORMATION

Un lien URL sera fourni aux stagiaires lors de la formation, afin de récupérer le support.

Le support de cours et les Microsoft Labs Online sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau

Windows Server 2022 / 2025 - Sécurité - Niveau 1

[WS25-SEC]

PUBLIC CONCERNÉ

Toute personne impliquée dans la sécurité du système d'information.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Concevoir et configurer une infrastructure sécurisée sous Windows Server 2019, Windows Server 2022 et Windows Server 2025
- Identifier et analyser les risques
- Lister les principales méthodes de sécurisation d'un parc Windows Server
- Respecter les bonnes pratiques.

PRÉREQUIS

Avoir une expérience en administration Windows Server de minimum 4 ans.

DURÉE

4 jours (28h)

TARIF

2680 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau

Windows Server 2022 / 2025 - Sécurité - Niveau 2

[WS25-SEC2]

PUBLIC CONCERNÉ

Architectes et administrateurs système et ingénieurs sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Appliquer les notions de sécurité avancées d'un environnement Windows Server
- Utiliser les différentes méthodes de gestion des risques IT et le management associé
- Mettre en œuvre la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- Appliquer les mesures de sécurité
- Gérer les accès privilégiés et le durcissement de l'identité
- Protéger les accès et les données
- Sécuriser les échanges
- Auditer la sécurité
- Reconnaître les différentes bonnes pratiques.

PRÉREQUIS

Avoir suivi la formation WS25-SEC « Windows Server 2022 / 2025 - Sécurité - Niveau 1 » ou avoir les connaissances équivalentes. Avoir de l'expérience en administration Windows Server 2016 / 2019 / 2022 / 2025 de minimum 4 ans.

DURÉE

5 jours (35h)

TARIF

3550 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Microsoft Azure - Gestion de la sécurité

[SEC-AZU]

PUBLIC CONCERNÉ

RSSI, responsables sécurité, chefs de projets et administrateurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Définir les normes et standards pour sécuriser le Cloud Microsoft
- Reconnaître les moyens offerts pour la sécurisation du Cloud Microsoft
- Sécuriser votre approche Cloud
- Eviter la mise en place d'une sécurité coûteuse et laborieuse
- Effectuer des attaques et des tests de pénétration sur le tenant
- Mettre en place des architectures sécurisées
- Sécuriser l'infrastructure du tenant
- Utiliser les bonnes pratiques.

PRÉREQUIS

Avoir des connaissances de base sur l'informatique et Microsoft Azure IaaS.

DURÉE

2 jours (14h)

TARIF

1420 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Microsoft Azure - Security Technologies

[MSAZ500]

CERTIFICATION

Microsoft AZ-500 *(tarif : 200€)*

PUBLIC CONCERNÉ

Administrateurs, professionnels de l'IT, responsables sécurité et/ou ingénieurs en sécurité Azure.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Mettre en œuvre la gestion des identités et des accès dans Microsoft Entra ID, la sécurisation des utilisateurs, des groupes et des identités externes, l'implémentation des contrôles d'authentification et d'autorisation, la gestion de l'accès et de la sécurité des applications
- Déterminer les complexités de la sécurisation des réseaux Azure, y compris les réseaux virtuels, le chiffrement, la configuration du pare-feu, l'accès privé et la protection DDoS, avec cette formation complète
- Sécuriser des ressources de calcul, de stockage et de bases de données Azure, notamment les mesures de sécurité avancées, le chiffrement, le contrôle d'accès et la protection des bases de données
- Gérer des opérations de sécurité dans Azure, de la gouvernance et la création de stratégies à la sécurité de l'infrastructure, la gestion des clés, la posture de sécurité, la protection contre les menaces, et la supervision et l'automatisation avancées de la sécurité.

PRÉREQUIS

Avoir suivi la formation MSAZ900T00 « Microsoft Azure - Fondamentaux » ou avoir les connaissances équivalentes. Avoir une solide expérience en infrastructure réseau et en serveurs.

DURÉE

4 jours (28h)

TARIF

2840 €^{HT}

LES PLUS DE LA FORMATION

Un lien URL sera fourni aux stagiaires lors de la formation, afin de récupérer le support.

Le support de cours et les Microsoft Labs Online sont en anglais.

Ce cours ne couvre pas les bases de la gestion d'Azure, mais tient plutôt compte des connaissances existantes et y ajoute des informations spécifiques à la sécurité.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Cours Officiel

Architecte en cybersécurité Microsoft

[MSSC100]

CERTIFICATION

Microsoft SC-100 *(tarif : 200€)*

PUBLIC CONCERNÉ

Ingénieurs de sécurité Cloud expérimentés, architectes solutions.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser les meilleures pratiques de sécurité Microsoft telles que le Cloud Adoption Framework (CAF), le Well-Architected Framework (WAF) et le Microsoft Cybersecurity Reference Architecture (MCRA)
- Améliorer la posture de sécurité d'une organisation
- Appliquer les principes de confiance zéro et minimiser les risques d'attaques émergentes
- Concevoir des solutions pour les opérations de sécurité (SecOps), la gestion des identités et des accès, les accès privilégiés et la conformité réglementaire
- Elaborer des solutions pour sécuriser les données et les applications
- Définir la sécurité de l'infrastructure, y compris la spécification des exigences pour les différents modèles de Cloud
- Concevoir des solutions pour la gestion de la posture dans les environnements hybrides et multiclouds, et la sécurisation des points d'extrémité.

PRÉREQUIS

Avoir connaissance des stratégies de sécurité, de l'architecture de Confiance Zéro, de la gestion des environnements hybrides, ainsi qu'une expérience avancée en accès et identités, protection des plateformes, opérations de sécurité, sécurisation des données et applications, et implémentations hybrides et Cloud.

DURÉE

4 jours (28h)

TARIF

2840 €^{HT}

LES PLUS DE LA FORMATION

Un lien URL sera fourni aux stagiaires lors de la formation, afin de récupérer le support.

Le support de cours est en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

LogPoint - Administrateur

[LOG-ADM]

CERTIFICATION

LogPoint Certified Administrator

PUBLIC CONCERNÉ

Professionnels de la sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les composants et l'architecture de la solution
- Définir les règles de normalisation, d'enrichissement et de stockage des logs
- Configurer la collecte des logs
- Administrer et déployer LogPoint Core et UEBA.

PRÉREQUIS

Avoir des connaissances sur l'administration d'un poste de travail (Windows et Linux), et l'administration des équipements réseau (switch, routeur, VLAN). Il est également recommandé de savoir utiliser les outils Office et les fichiers PDF.

DURÉE

2 jours (14h)

TARIF

1650 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

LogPoint - Utilisateur

[LOG-UT]

CERTIFICATION

LogPoint Certified User

PUBLIC CONCERNÉ

Professionnels de la sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire la différence entre les logs bruts et les logs normalisés
- Faire des recherches dans les logs bruts et/ou normalisés
- Utiliser les macros, search views et template pour simplifier la recherche
- Utiliser le module d'enrichissement de LogPoint
- Configurer des alertes et du reporting dans la solution.

PRÉREQUIS

Avoir des connaissances sur l'administration du poste de travail (Windows et Linux) et des équipements réseau (switch, routeur, VLAN). Il est également recommandé de savoir utiliser les outils Office et les fichiers PDF.

DURÉE

2 jours (14h)

TARIF

1650 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Check Point - Certified Security Administrator R81.x

[CHK81-ADM]

CERTIFICATION

CCSA *(tarif : 300€)*

PUBLIC CONCERNÉ

Professionnels techniques qui assistent, installent, déploient ou administrent des produits Check Point ou toute personne souhaitant passer la certification CCSA.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les principaux composants d'une architecture à trois niveaux (Check Point) et expliquer comment ils fonctionnent ensemble dans l'environnement Check Point
- Expliquer comment la communication est sécurisée et comment le trafic est acheminé dans l'environnement Check Point
- Décrire les fonctions de base du système d'exploitation Gaia
- Identifier le flux de travail de base pour installer Security Management Server et Security Gateway pour une solution à domaine unique
- Créer des objets SmartConsole correspondant à la topologie de l'organisation pour les utiliser dans les politiques et les règles
- Identifier les outils disponibles pour gérer les licences et les contrats Check Point, y compris leur objectif et leur utilisation
- Identifier les fonctionnalités et les capacités qui améliorent la configuration et la gestion de la politique de sécurité
- Expliquer comment les couches de politique affectent l'inspection du trafic
- Expliquer comment la traduction d'adresses réseau affecte le trafic
- Configurer la traduction d'adresses réseau (NAT) manuelle et automatique
- Démontrer une compréhension des capacités de contrôle des applications, de filtrage des URL et de prévention autonome des menaces, et configurer ces solutions pour répondre aux exigences de sécurité d'une organisation
- Expliquer comment les clés pré-partagées et les certificats peuvent être configurés pour l'authentification avec des passerelles VPN tierces et gérées en externe
- Analyser et interpréter le trafic des tunnels VPN
- Configurer les paramètres de journalisation
- Utiliser des requêtes prédéfinies et personnalisées pour filtrer les résultats des journaux
- Surveiller la santé du matériel Check Point supporté en utilisant le portail Gaia et la ligne de commande
- Décrire les différentes méthodes de sauvegarde des informations du système Check Point et discuter des meilleures pratiques et des recommandations pour chaque méthode.

PRÉREQUIS

Avoir une connaissance pratique des systèmes d'exploitation de type Unix et Windows et des réseaux TCP/IP.

DURÉE

3 jours (21h)

TARIF

2160 €HT

LES PLUS DE LA FORMATION

Cette formation est de nouveau délivrée en français. Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Check Point - Certified Security Expert R81.x

[CHK81-EXP]

CERTIFICATION

CCSE *(tarif : 300€)*

PUBLIC CONCERNÉ

Professionnels techniques qui conçoivent, mettent à niveau, entretiennent et supportent les produits Check Point.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les interfaces de base utilisées pour gérer l'environnement Check Point
- Identifier les types de technologies que Check Point supporte pour l'automatisation
- Expliquer le but du déploiement de Check Management High Availability (HA)
- Identifier le flux de travail suivi pour déployer un serveur primaire et une solution secondaire
- Expliquer les concepts de base du clustering et de ClusterXL, y compris les protocoles, la synchronisation, le maintien de la connexion
- Exclure des services de la synchronisation ou retarder la synchronisation
- Expliquer le processus d'installation des politiques
- Expliquer l'objectif des objets dynamiques, des objets pouvant être mis à jour et des flux réseau
- Gérer l'accès des utilisateurs internes et externes
- Décrire les composants et les configurations d'Identity Awareness
- Décrire les différentes solutions de prévention des menaces Check Point
- Expliquer comment le système de prévention des intrusions est configuré
- Obtenir des connaissances sur Check Point's IoT Protect
- Expliquer l'objectif des VPN basés sur un domaine
- Décrire les situations dans lesquelles l'authentification par certificat géré en externe est utilisée
- Décrire comment la sécurité du client peut être assurée par l'accès à distance
- Discuter de la lame logicielle d'accès mobile
- Déterminer si la configuration est conforme aux meilleures pratiques
- Définir les solutions d'optimisation des performances et le flux de travail de la configuration de base
- Identifier les méthodes et procédures de mise à niveau et de migration prises en charge pour les serveurs de gestion de la sécurité et les serveurs de journalisation et d'événements intelligents dédiés
- Identifier les méthodes et procédures de mise à niveau prises en charge pour les passerelles de sécurité.

PRÉREQUIS

Avoir suivi la formation CHK81-ADM « Check Point - Certified Security Administrator R81.x » ou être certifié CCSA. Avoir des connaissances fondamentales d'Unix et de Windows. Avoir de l'expérience sur la gestion des certificats, et des connaissances en matière d'administration des systèmes et des réseaux.

DURÉE

3 jours (21h)

TARIF

2160 €HT

LES PLUS DE LA FORMATION

Cette formation est de nouveau délivrée en français. Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Red Hat Security - Linux in Physical, Virtual, and Cloud

[RH415]

PUBLIC CONCERNÉ

Administrateurs système, administrateurs de sécurité informatique, ingénieurs de sécurité informatique et autres professionnels chargés de la conception, de la mise en œuvre, du maintien et de la gestion de la sécurité de systèmes Red Hat Enterprise Linux conformément aux politiques de sécurité en vigueur dans l'entreprise.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Analyser et corriger des problèmes de conformité du système à l'aide d'OpenSCAP et de SCAP Workbench
- Utiliser et adapter le contenu de politiques de référence fourni avec Red Hat Enterprise Linux
- Gérer les activités en lien avec la sécurité sur vos systèmes à l'aide de l'infrastructure d'audit du noyau
- Mettre en œuvre des techniques SELinux avancées pour restreindre l'accès au niveau des utilisateurs, des processus et des machines virtuelles
- Déterminer l'intégrité des fichiers et leurs permissions avec l'utilitaire AIDE
- Bloquer l'utilisation de périphériques USB non autorisés à l'aide d'USBGuard
- Protéger des données au repos avec déchiffrement automatique sécurisé dès le démarrage avec NBDE
- Identifier des risques et des erreurs de configuration de façon proactive sur les systèmes et correction à l'aide de Red Hat Insights
- Analyser l'état de conformité et corriger à grande échelle à l'aide d'OpenSCAP, de Red Hat Insights, de Red Hat Satellite et de Red Hat Ansible Tower.

PRÉREQUIS

Etre titulaire de la certification RHCE (Ingénieur Certifié Red Hat), ou avoir des connaissances et/ou expérience(s) équivalentes de l'utilisation de Red Hat Enterprise Linux. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5 jours (26h15)

TARIF

3740 €HT

LES PLUS DE LA FORMATION

En distanciel, ce cours est dispensé sur 26h15, soit 5 jours, de 9h à 15h (avec une pause déjeuner de 45 minutes).

En présentiel, ce cours est dispensé sur 4 jours (de 9h à 17h).

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Red Hat Security - Linux in Physical, Virtual, and Cloud (RH415) + examen (EX415)

[RH416]

CERTIFICATION

EX415

PUBLIC CONCERNÉ

Administrateurs système, administrateurs de sécurité informatique, ingénieurs de sécurité informatique et autres professionnels chargés de la conception, de la mise en œuvre, du maintien et de la gestion de la sécurité de systèmes Red Hat Enterprise Linux conformément aux politiques de sécurité en vigueur dans l'entreprise.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Analyser et corriger des problèmes de conformité du système à l'aide d'OpenSCAP et de SCAP Workbench
- Utiliser et adapter le contenu de politiques de référence fourni avec Red Hat Enterprise Linux
- Gérer les activités en lien avec la sécurité sur vos systèmes à l'aide de l'infrastructure d'audit du noyau
- Mettre en œuvre des techniques SELinux avancées pour restreindre l'accès au niveau des utilisateurs, des processus et des machines virtuelles
- Déterminer l'intégrité des fichiers et de leurs permissions avec l'utilitaire AIDE
- Bloquer l'utilisation de périphériques USB non autorisés à l'aide d'USBGuard
- Protéger des données au repos avec déchiffrement automatique sécurisé dès le démarrage avec NBDE
- Identifier des risques et des erreurs de configuration de façon proactive sur les systèmes et correction à l'aide de Red Hat Insights
- Analyser l'état de conformité et corriger à grande échelle à l'aide d'OpenSCAP, de Red Hat Insights, de Red Hat Satellite et de Red Hat Ansible Tower.

PRÉREQUIS

Etre titulaire de la certification RHCE (Ingénieur Certifié Red Hat), ou avoir des connaissances et/ou expérience(s) équivalentes de l'utilisation de Red Hat Enterprise Linux. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

DURÉE

5,5 jours (30h15)

TARIF

4057 €HT

LES PLUS DE LA FORMATION

En distanciel, ce cours est dispensé sur 30h15, soit 5,5 jours, de 9h à 15h (avec une pause déjeuner de 45 minutes). Cette durée inclut le passage de l'examen en Kiosk (à froid), d'une durée de 4h.

En présentiel, ce cours est dispensé sur 4,5 jours (de 9h à 17h) dont la dernière demi-journée est dédiée au passage de l'examen, d'une durée de 4h.

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Top Vente Cours Officiel

Fortinet NSE 4 - FortiGate Administrator

[FGT-ADMIN]

PUBLIC CONCERNÉ

Professionnels des réseaux et de la sécurité impliqués dans la gestion, la configuration, l'administration et la surveillance des dispositifs FortiGate utilisés pour sécuriser les réseaux de leurs organisations.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Implémenter le paramétrage de base réseau à partir de la configuration usine
- Configurer et contrôler les accès administrateur au Fortigate
- Utiliser l'interface graphique et le CLI pour l'administration
- Contrôler l'accès aux réseaux configurés à l'aide de stratégies de pare-feu
- Appliquer le transfert de port, le NAT à la source et le NAT à la destination
- Analyser une table de routage FortiGate
- Mettre en pratique le routage des paquets à l'aide de routes statiques et basées sur des règles pour les déploiements à trajets multiples et à charge équilibrée
- Authentifier les utilisateurs à l'aide de stratégies de pare-feu
- Monitorer les utilisateurs à l'aide de la GUI
- Offrir un accès Fortinet Single Sign-On (FSSO) aux services du réseau, intégré à Microsoft Active Directory (AD)
- Identifier les fonctions de cryptage et les certificats
- Inspecter le trafic sécurisé SSL/TLS pour empêcher le cryptage utilisé pour contourner les politiques de sécurité
- Configurer les profils de sécurité pour neutraliser les menaces et les abus, y compris les virus, les torrents et les sites Web inappropriés
- Pratiquer des techniques de contrôle des applications pour surveiller et contrôler les applications réseau susceptibles d'utiliser des protocoles et des ports standards ou non standards
- Proposer un VPN SSL pour un accès sécurisé à votre réseau privé
- Etablir un tunnel VPN IPsec entre deux équipements FortiGate
- Configurer SD-WAN
- Identifier les caractéristiques de la Security Fabric de Fortinet
- Déployer les équipements FortiGate en tant que cluster HA pour la tolérance aux pannes et la haute performance
- Diagnostiquer et corriger les problèmes courants.

PRÉREQUIS

Avoir une connaissance des protocoles de réseau et une compréhension de base des concepts de pare-feu.

DURÉE

4 jours (28h)

TARIF

3500 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Ce module fait partie du parcours de formation menant à la certification Fortinet Certified Professional (FCP) Network Security.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Cours Officiel

Fortinet NSE 5 - FortiManager Administrator

[FGT-MANAG]

PUBLIC CONCERNÉ

Toute personne responsable de la gestion quotidienne des politiques de sécurité FortiGate à l'aide de la plateforme FortiManager.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les principales caractéristiques et capacités du FortiManager
- Définir l'API du FortiManager et les champs méta
- Déployer des domaines administratifs (ADOM) pour prendre en charge plusieurs clients sur un seul FortiManager
- Restreindre l'accès simultané aux ADOM en utilisant les espaces de travail et le mode workflow
- Utiliser des modèles de provisionnement pour les changements au niveau de plusieurs appareils
- Identifier les états de synchronisation et gérer l'historique des révisions des appareils gérés
- Gérer les politiques de pare-feu sur plusieurs appareils FortiGate en utilisant des paquets de politiques avec des objets partagés et dynamiques
- Déployer des politiques et des objets de l'ADOM global vers plusieurs ADOM
- Définir la Security Fabric de Fortinet avec FortiManager
- Décrire les options de haute disponibilité (HA), de sauvegarde et de restauration pour FortiManager
- Gérer le firmware des appareils pris en charge de manière centralisée
- Intégrer un serveur de distribution FortiGuard local à vos appareils Fortinet
- Diagnostiquer et résoudre les problèmes d'importation et d'installation.

PRÉREQUIS

Avoir suivi la formation FGT-ADMIN « Fortinet NSE 4 - FortiGate Administrator » ou avoir les connaissances équivalentes. Avoir une connaissance des concepts de pare-feu dans un réseau IPv4 et avoir une compréhension de base des systèmes de gestion de réseau.

DURÉE

2 jours (14h)

TARIF

2050 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Ce module fait partie du parcours de formation menant à la certification Fortinet Certified Professional (FCP) Network Security.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Cours Officiel

Fortinet NSE 6 - FortiAnalyzer Administrator

[FGT-ANALY]

PUBLIC CONCERNÉ

Toute personne responsable de la gestion quotidienne des dispositifs FortiAnalyzer.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire l'objectif du FortiAnalyzer
- Décrire les modes de fonctionnement du FortiAnalyzer
- Expliquer la journalisation dans un environnement Fortinet Security Fabric
- Décrire le FortiAnalyzer Fabric
- Gérer les domaines administratifs (ADOM)
- Configurer les paramètres réseau
- Configurer l'accès administratif sécurisé
- Gérer le quota de disque
- Effectuer une sauvegarde de la configuration du système
- Gérer le RAID (Redundant Array of Independent Disks)
- Gérer la haute disponibilité (HA)
- Enregistrer et gérer les périphériques
- Décrire le flux de travail des fichiers journaux
- Effectuer des sauvegardes de journaux
- Définir les connecteurs Fabric
- Configurer la redondance et le cryptage des journaux
- Configurer la politique de transfert et de conservation des journaux
- Gérer les rapports.

PRÉREQUIS

Avoir suivi la formation FGT-ADMIN « Fortinet NSE 4 - FortiGate Administrator » ou avoir les connaissances équivalentes.

DURÉE

1 jour (7h)

TARIF

1490 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Ce module fait partie du parcours de formation menant à la certification Fortinet Certified Professional (FCP) Network Security.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

EGERIE Risk Manager avec ISO 27005

[EGERIE-ISO]

PUBLIC CONCERNÉ

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

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Analyser les risques du système d'information avec l'outil EGERIE
- Construire une vision globale des risques projets
- Améliorer votre pilotage des risques
- Industrialiser les analyses de risques.

PRÉREQUIS

Avoir une connaissance générale des méthodes d'appréciation des risques telle que la méthode EBIOS ou la démarche ISO 27005.

DURÉE

2 jours (14h)

Consultez le programme détaillé en scannant ce code

Fonctionnalités avancées

Cours Officiel

EGERIE Risk Manager v4 avec EBIOS RM - Avec certification

[EGERIE-EBIOS]

CERTIFICATION

EGERIE Risk Manager v4

PUBLIC CONCERNÉ

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

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Analyser les risques du système d'information avec l'outil EGERIE
- Construire une vision globale des risques projets
- Améliorer votre pilotage des risques
- Industrialiser les analyses de risques.

PRÉREQUIS

Avoir une connaissance générale de la méthode EBIOS Risk Manager 2018.

DURÉE

2 jours (14h)

TARIF

1500 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Trellix Application and Change Control - Administration 8.0

[MCA-ACC]

PUBLIC CONCERNÉ

Administrateurs système et réseau ou toute personne concernée par la sécurité des terminaux système.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Installer, configurer, utiliser et résoudre efficacement les problèmes liés à Trellix Application Control et Change Control pour protéger la propriété intellectuelle et garantir la conformité
- Utiliser Trellix ePolicy Orchestrator (Trellix ePO)
- Mettre en place seulement les applications de confiance s'exécutant avec Application Control
- Surveiller et prévenir les changements apportés au système de fichiers, au registre et aux comptes d'utilisateurs avec Change Control.

PRÉREQUIS

Avoir une solide connaissance de l'administration du système Microsoft Windows et des technologies réseau, de la sécurité informatique, de la syntaxe en ligne de commande, des logiciels malware / anti-malware, des virus / antivirus et des technologies Web. Avoir une expérience dans l'utilisation du logiciel Trellix ePolicy Orchestrator (Trellix ePO).

DURÉE

4 jours (28h)

TARIF

4110 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Trellix Data Loss Prevention Endpoint - Administration

[MCA-DLP]

PUBLIC CONCERNÉ

Administrateurs système et réseau, membres d'une équipe de sécurité, auditeurs et/ou consultants concernés par la sécurité des points de terminaison (endpoints) des systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Mettre en pratique les outils nécessaires à la conception, la mise en œuvre, la configuration et l'utilisation de Data Loss Prevention Endpoint pour protéger la propriété intellectuelle et assurer la conformité
- Expliquer comment cette solution utilise le logiciel ePolicy Orchestrator (ePO) pour une gestion centralisée
- Surveiller et traiter les actions quotidiennes à risque des utilisateurs finaux, telles que l'envoi de courriels, la publication d'articles sur le Web, l'impression, les presse-papiers, les captures d'écran, le contrôle des appareils, le téléchargement vers le Cloud, et plus encore.

PRÉREQUIS

Avoir de solides connaissances de Windows, de l'administration système, des technologies de réseau, de la sécurité informatique, des concepts de sécurité du Cloud et des technologies Web. Il est également recommandé d'avoir une expérience préalable de l'utilisation du logiciel McAfee MVISION ePO.

DURÉE

4 jours (28h)

TARIF

4110 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Trellix 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

A l'issue de cette formation, vous serez capable de :

- Mettre en place et administrer le produit Trellix Endpoint Security (ENS)
- Utiliser Trellix 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 Trellix Endpoint Security, ainsi qu'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 (35h)

TARIF

5140 €HT

LES PLUS DE LA FORMATION

Plus de certification disponible pour le moment.

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Trellix Endpoint Detection and Response (EDR) - Administration

[TRELL-EDR]

PUBLIC CONCERNÉ

Analystes et/ou ingénieurs responsables de la configuration, de la gestion et de la surveillance des activités sur leurs systèmes, réseaux, bases de données et applications utilisant la solution EDR.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Installer EDR dans un environnement ePolicy Orchestrator (ePO) On-Premise
- Naviguer efficacement dans le tableau de bord du produit, effectuer des investigations guidées et créer des collecteurs et réactions personnalisés
- Exploiter les fonctionnalités de l'EDR pour détecter les menaces avancées pesant sur les appareils, les étudier de manière approfondie et y répondre rapidement
- Utiliser le classement des alertes et la visualisation des données pour comprendre rapidement les menaces et prioriser les actions.

PRÉREQUIS

Avoir une solide connaissance des concepts d'administration des réseaux et des systèmes, des concepts de sécurité informatique, des concepts et des pratiques de sécurité des réseaux, ainsi qu'une connaissance pratique de l'analyse, de la forensics, des tactiques et des techniques en matière de logiciels malveillants. Avoir également une compréhension générale des réseaux et des logiciels d'application.

DURÉE

2 jours (14h)

TARIF

2055 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Trellix ePolicy Orchestrator - Administration

[MCA-VS]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseaux, personnels de sécurité et consultants concernés par la sécurité des systèmes et des réseaux.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Installer et configurer la console ePolicy Orchestrator
- Configurer le serveur ePolicy Orchestrator
- Gérer des utilisateurs et des ressources
- Gérer la sécurité réseau, les politiques et bases de données
- Installer et utiliser l'agent Trellix.

PRÉREQUIS

Avoir des connaissances sur l'administration de Microsoft Windows et concepts d'administration des systèmes. Avoir des connaissances de base des concepts de sécurité informatique.

DURÉE

5 jours (35h)

TARIF

5140 €HT

LES PLUS DE LA FORMATION

Plus de certification disponible pour le moment.

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Trellix ePolicy Orchestrator - Advanced Topics

[TRELL-EPOAV]

PUBLIC CONCERNÉ

Administrateurs de systèmes et de réseaux, personnels chargés de la sécurité, auditeurs et/ou consultants concernés par la sécurité des réseaux et des systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser les fonctionnalités avancées d'ePO - On-prem
- Utiliser des outils pour les mises à niveau et les migrations d'ePO, la surveillance, la maintenance et le dépannage ainsi que la configuration avancée des règles.

PRÉREQUIS

Avoir suivi le cours MCA-VS « Trellix ePolicy Orchestrator - Administration » ou avoir les connaissances équivalentes. Avoir une connaissance pratique des systèmes d'exploitation Windows, de l'administration des systèmes et des technologies de réseau. Une connaissance de base de la sécurité informatique, de la syntaxe de la ligne de commande, des logiciels malveillants / antimalveillants, des virus / antivirus et des technologies Web est recommandée. Une expérience préalable ou une connaissance pratique d'ePolicy Orchestrator est également requise.

DURÉE

4 jours (28h)

TARIF

4110 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Splunk - Les essentiels

[SPLUNK-ESS]

PUBLIC CONCERNÉ

Administrateurs systèmes et réseaux, architectes systèmes et réseaux, Data Analysts, Data Scientists et/ou consultants Big Data.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser Splunk pour collecter, analyser et générer des rapports sur les données
- Enrichir les données opérationnelles à l'aide de recherches et de flux
- Créer des alertes en temps réel
- Intégrer des graphiques avancés
- Mettre en place les bons réflexes d'exploitation de Splunk
- Améliorer l'exploitation de données avec Splunk
- Expliquer les obligations légales en matière de conservation des données
- Reconnaître la démarche d'une analyse de log
- Interpréter la corrélation et l'analyse avec Splunk.

PRÉREQUIS

Avoir des connaissances de base en systèmes et réseaux ainsi qu'en gestion de données.

DURÉE

3 jours (21h)

TARIF

2280 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau

Splunk - Niveau avancé

[SPLUNK-AV]

PUBLIC CONCERNÉ

Administrateurs et/ou ingénieurs systèmes.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Approfondir vos compétences en utilisant « Splunk Core Certified Power User » (ou Splunk niveau avancé)
- Effectuer des analyses avancées et résoudre des problèmes complexes.

PRÉREQUIS

Avoir suivi la formation SPLUNK-ESS « Splunk - Les essentiels » ou avoir les connaissances équivalentes.

DURÉE

3 jours (21h)

TARIF

2550 €HT

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

SonicWall Network Security Administrator

[SNSA]

CERTIFICATION

CSSA

PUBLIC CONCERNÉ

Toute personne concernée par l'administration au quotidien de boîtiers SonicWall.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Configurer, contrôler, gérer et optimiser les appareils de pare-feu de sécurité de réseau de SonicWall exécutant SonicOS
- Vous défendre contre le développement, le réseau naissant et les menaces de sécurité informatique
- Configurer le pare-feu de SonicWall pour la connectivité sécurisée et éloignée, l'optimisation de réseau et la protection de menace avancée.

PRÉREQUIS

Etre à l'aise avec un PC sous Windows (7, 8 ou 10). Avoir des connaissances de base sur les réseaux et TCP/IP et des notions en sécurité informatique est un plus.

DURÉE

2 jours (14h)

TARIF

1400 €HT

LES PLUS DE LA FORMATION

Le support de cours est en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente Cours Officiel

Palo Alto Networks - Firewall 11.x - Essentials - Configuration et management

[PAN-EDU210]

PUBLIC CONCERNÉ

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

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Configurer et gérer les fonctionnalités essentielles des firewalls de nouvelle génération Palo Alto Networks
- Configurer et gérer des politiques de sécurité et de NAT pour la gestion des flux autorisés
- Configurer et gérer les profils de gestion des menaces afin de bloquer le trafic provenant d'adresses, domaines et URL connus et inconnus
- Monitorer le trafic réseau en utilisant l'interface Web et les rapports intégrés.

PRÉREQUIS

Avoir des connaissances de base sur les concepts de sécurité et de réseau, incluant le routage, le switching et l'adressage IP. Une expérience sur des technologies de sécurité (IPS, proxy, filtrage de contenus) est un plus.

DURÉE

5 jours (35h)

TARIF

4015 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Palo Alto Networks - Panorama 11.x - Management des firewalls à grande échelle

[PAN-EDU220]

PUBLIC CONCERNÉ

Ingénieurs, administrateurs, analystes et architectes sécurité.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Configurer et manager le serveur de management Panorama
- Configurer des modèles (incluant des variables) et des groupes de boîtiers
- Administrer, gérer des logs et créer des rapports
- Gérer, implémenter l'architecture et le déploiement de la solution Panorama.

PRÉREQUIS

Avoir suivi la formation PAN-EDU210 « Palo Alto Networks - Firewall 11.x - Essentials - Configuration et management » ou avoir les connaissances équivalentes. Etre familier avec les fondamentaux des concepts réseaux (routage, switching et adressage IP).

DURÉE

2 jours (14h)

TARIF

2145 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Cours Officiel

Palo Alto Networks - Prisma Access SSE - Configuration et déploiement

[PAN-EDU318]

PUBLIC CONCERNÉ

Ingénieurs en sécurité, administrateurs réseau, spécialistes des opérations de sécurité, analystes cyber et ingénieurs réseau.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Protéger vos applications, vos réseaux distants et vos utilisateurs mobiles en utilisant une implémentation SASE.

PRÉREQUIS

Il est recommandé d'avoir suivi le cours PAN-EDU210 « Palo Alto Networks - Firewall 11.x - Essentials - Configuration et management » ou avoir une expérience équivalente. Avoir des connaissances de base de l'informatique et du Cloud public, une expérience des concepts de réseau comme le routage, la commutation et l'adressage IP.

L'apprenant s'engage à respecter les prérequis nécessaires via un questionnaire qui lui sera transmis en amont de la formation.

Afin d'être préparé de manière optimale, l'apprenant devra également suivre un parcours d'apprentissage numérique avant l'entrée en formation.

DURÉE

4 jours (28h)

TARIF

3750 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Palo Alto Networks - Cortex XDR 3.6 - Prévention et déploiement

[PAN-EDU260]

PUBLIC CONCERNÉ

Analystes en cybersécurité, administrateurs système ou toute personne en charge du déploiement.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire l'architecture et les composants de la famille Cortex XDR
- Utiliser la console Web Cortex XDR, les rapports et les dashboards
- Utiliser pleinement la console Cortex XDR
- Créer des packages d'installation, des groupes d'Endpoints et des stratégies d'agent Cortex XDR
- Déployer l'agent sur les Endpoints
- Créer et gérer des profils de prévention contre les « exploits » et les logiciels malveillants
- Examiner les alertes et les classer par ordre de priorité (à l'aide de stratégies de score, de favori ou d'exclusion)
- Gérer la sécurité des exceptions Cortex XDR
- Effectuer et suivre les actions de réponse dans le centre d'action
- Effectuer un dépannage de base lié aux agents Cortex XDR
- Déployer une VM Broker et activer l'Applet Local Agents Settings
- Gérer les concepts liés au déploiement de Cortex XDR et les exigences d'activation
- Administrer le portail de support et la Gateway Cortex XDR pour l'authentification et les autorisations des utilisateurs.

PRÉREQUIS

Etre familiarisé avec les déploiements d'entreprise, le réseau et les bases de la sécurité.

DURÉE

3 jours (21h)

TARIF

2915 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Palo Alto Networks - Firewall 11.x - Troubleshooting avancé

[PAN-EDU330]

PUBLIC CONCERNÉ

Ingénieurs sécurité et réseaux, administrateurs sécurité, spécialistes des opérations de sécurité, analystes en sécurité et membres d'une équipe de support.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Investiguer les problèmes de connexion réseau en utilisant les outils et la CLI
- Suivre des procédures de troubleshooting éprouvées
- Effectuer une analyse avancée des logs pour résoudre des scénarios variés du quotidien
- Mettre en pratique ces méthodes dans des labs (exercices pratiques de lab basés sur des scénarios).

PRÉREQUIS

Avoir suivi la formation PAN-EDU210 « Palo Alto Networks - Firewall 11.x - Essentials - Configuration et management » ou avoir une expérience pratique équivalente. Etre familier avec les fondamentaux des concepts réseaux (routage, switching, adressage IP). Avoir une expérience professionnelle d'au moins 6 mois sur les firewalls de Palo Alto Networks.

DURÉE

3 jours (21h)

TARIF

2915 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Nouveau Cours Officiel

Palo Alto Networks - Cortex XDR 3.6 - Investigation et réponse

[PAN-EDU262]

PUBLIC CONCERNÉ

Analystes et ingénieurs en cybersécurité et/ou toute personne travaillant dans un SOC.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Enquêter et gérer les incidents
- Décrire la causalité Cortex XDR et les concepts analytiques
- Analyser les alertes à l'aide des vues Causalité et Chronologie
- Travailler avec les actions Cortex XDR Pro telles que l'exécution de scripts à distance
- Créer et gérer des requêtes de recherche à la demande et les planifier dans le Centre de requêtes
- Créer et gérer les règles Cortex XDR BIOC et IOC
- Travailler avec les actifs et les inventaires Cortex XDR
- Ecrire des requêtes XQL pour rechercher des ensembles de données et visualiser les ensembles de résultats
- Travailler avec la collecte de données externes de Cortex XDR.

PRÉREQUIS

Avoir suivi la formation PAN-EDU260 « Palo Alto Networks - Cortex XDR 3.6 - Prévention et déploiement » ou avoir les connaissances équivalentes. Etre familiarisé avec l'analyse d'évènements de sécurité.

L'apprenant s'engage à respecter les prérequis nécessaires via un questionnaire qui lui sera transmis en amont de la formation.

DURÉE

2 jours (14h)

TARIF

2145 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Top Vente Cours Officiel

Stormshield Network - Administrateur

[STO-CSNA]

CERTIFICATION

CSNA

PUBLIC CONCERNÉ

Responsables informatique, administrateurs réseaux et techniciens informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Prendre en main un firewall SNS et décrire son fonctionnement
- Configurer un firewall dans un réseau
- Définir et mettre en œuvre des politiques de filtrage et de routage
- Configurer un contrôle d'accès aux sites Web en HTTP et HTTPS (proxy)
- Configurer des politiques d'authentification
- Mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL).

PRÉREQUIS

Avoir de bonnes connaissances en TCP/IP. Avoir suivi une formation IP au préalable est un plus.

DURÉE

3 jours (21h)

TARIF

2550 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont également disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Stormshield Management Center - Expert

[STO-CSMCE]

CERTIFICATION

CSMCE

PUBLIC CONCERNÉ

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

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- 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 SNS 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 (14h)

TARIF

1890 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont également disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Stormshield Network - Expert

[STO-CSNE]

CERTIFICATION

CSNE

PUBLIC CONCERNÉ

Responsables informatique, administrateurs réseaux, tout technicien informatique ayant obtenu la certification CSNA.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Utiliser de manière avancée l'IHM (Interface Homme Machine)
- Configurer avec précision le moteur de prévention d'intrusions
- Mettre en place une PKI (Public Key Infrastructure) et une authentification transparente
- Mettre en place un VPN IPSec par certificat
- Créer un cluster haute disponibilité.

PRÉREQUIS

Avoir suivi la formation STO-CSNA « Stormshield Network - Administrateur » avec l'obtention de la certification (durant les 3 dernières années).

DURÉE

3 jours (21h)

TARIF

2550 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont également disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Expertise / Spécialisation

Cours Officiel

Stormshield Network - Troubleshooting and support

[STO-CSNTS]

CERTIFICATION

CSNTS

PUBLIC CONCERNÉ

Responsables informatique, administrateurs réseaux, ou tout technicien informatique.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Reconnaître l'organisation du système de fichiers ainsi que les démons et processus d'une appliance Stormshield Network
- Localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs)
- Distinguer des particularités et anomalies dans une configuration réseau et routage
- Réaliser et étudier des captures de trafic réseau
- Etudier une politique de sécurité et en identifier les directives générales et les paramètres particuliers
- Identifier les traitements appliqués aux connexions en cours
- Produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic
- Configurer des politiques de tunnels VPN IPSec, identifier les mécanismes activés et en diagnostiquer les dysfonctionnements
- Analyser et diagnostiquer une configuration en haute disponibilité.

PRÉREQUIS

Avoir suivi la formation STO-CSNE « Stormshield Network - Expert ». Avoir une certification CSNE en cours de validité. Avoir des connaissances approfondies en TCP/IP et shell UNIX.

DURÉE

4 jours (28h)

TARIF

4000 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont également disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Stormshield Endpoint - Administrateur

[STO-CSEA]

CERTIFICATION

CSEA

PUBLIC CONCERNÉ

Administrateurs systèmes et sécurité, responsables de projets, techniciens informatique et support.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Installer et administrer la solution SES Evolution (Stormshield Endpoint Security)
- Déployer des agents SES Evolution sur un parc de postes et serveurs à protéger
- Mettre en place une politique pour protéger le système
- Mettre en place une politique de contrôle des périphériques et des réseaux
- Mettre en place une politique de configuration conditionnelle.

PRÉREQUIS

Avoir de bonnes connaissances du système et de la sécurité de Microsoft Windows Client et de Microsoft Active Directory.

DURÉE

2 jours (14h)

TARIF

1890 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont également disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Stormshield Data - Administrateur

[STO-CSDA]

CERTIFICATION

CSDA

PUBLIC CONCERNÉ

Administrateurs systèmes et sécurité, responsables de projets, techniciens informatique et support.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Identifier les concepts de cryptographie
- Utiliser la console SDMC pour créer des politiques de sécurité liées à vos annuaires et PKI d'entreprise
- Installer l'agent SDS Enterprise sur des postes client et déployer les politiques de sécurité
- Mettre en œuvre et déployer des politiques de sécurité pour protéger toutes les données d'une entreprise (données locales du poste de travail des collaborateurs, données hébergées sur les serveurs de l'entreprise, données synchronisées sur des Clouds publics, emails).

PRÉREQUIS

Avoir de bonnes connaissances sur le système Windows Client. Avoir des notions d'annuaire LDAP / Active Directory, Client Outlook. Avoir des connaissances sur les mécanismes des autorités de certification serait un plus.

DURÉE

3 jours (21h)

TARIF

2600 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont disponibles en français et en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Cisco Security Core Technologies - Implementing and operating

[SCOR]

CERTIFICATION

350-701 *(tarif : 593€)*

PUBLIC CONCERNÉ

Ingénieurs sécurité et/ou réseaux, concepteurs réseaux, administrateurs réseaux, ingénieurs systèmes, ingénieurs conseil systèmes, architectes des solutions techniques, intégrateurs / partenaires Cisco, gestionnaires de réseau.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les concepts et les stratégies de sécurité de l'information au sein du réseau
- Identifier les attaques courantes de TCP/IP, d'applications réseau et de points d'extrémité
- Expliquer comment les différentes technologies de sécurité des réseaux fonctionnent ensemble pour se protéger contre les attaques
- Mettre en place un contrôle d'accès sur l'appliance Cisco ASA et le Cisco Firepower Next-Generation Firewall (NGFW)
- Identifier et mettre en œuvre les fonctions de base de la sécurité du contenu du courrier électronique fournies par l'application Cisco Email Security Appliance
- Décrire et mettre en œuvre les caractéristiques et les fonctions de sécurité du contenu Web fournies par le Cisco Web Security Appliance
- Reconnaître les capacités de sécurité de Cisco Umbrella, les modèles de déploiement, la gestion des politiques et la console Investigate
- Identifier les VPN et décrire les solutions et les algorithmes de cryptographie
- Décrire les solutions de connectivité sécurisée de point à point Cisco et expliquer comment déployer les VPN IPsec point à point basés sur le système IOS VTI de Cisco et les VPN IPsec point à point sur le Cisco ASA et le Cisco Firepower NGFW
- Décrire et déployer les solutions de connectivité d'accès à distance sécurisé Cisco et décrire comment configurer l'authentification 802.1X et EAP
- Expliquer la sécurité des points d'accès et décrire l'architecture et les caractéristiques de base de l'AMP pour les points d'accès
- Examiner les différentes défenses des dispositifs Cisco qui protègent le plan de contrôle et de gestion
- Configurer et vérifier les contrôles des plans de données de la couche 2 et de la couche 3 du logiciel Cisco IOS
- Identifier les solutions Stealthwatch Enterprise et Stealthwatch Cloud de Cisco
- Décrire les principes de base de l'informatique en Cloud, les attaques courantes dans le Cloud, ainsi que la manière de sécuriser l'environnement Cloud.

PRÉREQUIS

Etre familiarisé avec Ethernet et les réseaux TCP/IP. Avoir des connaissances pratiques du système d'exploitation Windows, des réseaux et des concepts de Cisco IOS. Avoir des notions de base de la sécurité des réseaux. De plus, il est recommandé d'avoir suivi la formation CCNA « Cisco Solutions - Implementing and administering ».

DURÉE

5 jours (35h)

TARIF

4060 €HT

LES PLUS DE LA FORMATION

Ce cours comprend des modules en présentiel et d'autres à suivre en e-learning de manière autonome (modules accessibles durant 90 jours, dès le début de la formation).

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Cisco Firewall Threat Defense - Fundamentals and Intrusion Prevention

[SFWIPF]

CERTIFICATION

300-710 *(tarif : 476€)*

PUBLIC CONCERNÉ

Ingénieurs en sécurité des réseaux et administrateurs.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire Cisco Secure Firewall Threat Defense
- Décrire les options de déploiement de Cisco Secure Firewall Threat Defense
- Décrire les options de gestion de Cisco Secure Firewall Threat Defense
- Configurer les paramètres initiaux de base sur Cisco Secure Firewall Threat Defense
- Configurer la haute disponibilité sur Cisco Secure Firewall Threat Defense
- Configurer la NAT (Network Address Translation) de base sur Cisco Secure Firewall Threat Defense
- Décrire les politiques de Cisco Secure Firewall Threat Defense et expliquer comment les différentes politiques influencent le traitement des paquets par le périphérique
- Configurer la politique de détection sur Cisco Secure Firewall Threat Defense
- Configurer et expliquer les règles de préfiltre et de tunnel dans la politique de préfiltre
- Configurer une politique de contrôle d'accès sur Cisco Secure Firewall Threat Defense
- Configurer l'intelligence de sécurité Cisco Secure Firewall Threat Defense
- Configurer la politique de fichiers Cisco Secure Firewall Threat Defense
- Configurer la politique d'intrusion sur Cisco Secure Firewall Threat Defense
- Effectuer une analyse de base des menaces à l'aide de Cisco Secure Firewall Management Center
- Effectuer des tâches de gestion et d'administration système de base sur Cisco Secure Firewall Threat Defense
- Effectuer un dépannage de base du flux de trafic sur Cisco Secure Firewall Threat Defense
- Gérer Cisco Secure Firewall Threat Defense avec Cisco Secure Firewall Threat Defense Manager.

PRÉREQUIS

Avoir une bonne compréhension de TCP/IP, des protocoles de routage de base, des concepts de pare-feu, de VPN et d'IPS. De plus, il est recommandé d'avoir suivi les cours CCNA « Cisco Solutions - Implementing and administering » et SCOR « Cisco Security Core Technologies - Implementing and operating », ou avoir les connaissances équivalentes.

DURÉE

5 jours (35h)

TARIF

4260 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Nouveau Cours Officiel

Cisco Firewall Threat Defense - Advanced Techniques and Intrusion Prevention

[SFWIPA]

CERTIFICATION

300-710 *(tarif : 476€)*

PUBLIC CONCERNÉ

Installateurs de systèmes, intégrateurs de systèmes, administrateurs de systèmes, administrateurs de réseaux et/ou concepteurs de solutions.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire Cisco Secure Firewall Threat Defense
- Décrire les options de déploiement avancées de Cisco Secure Firewall Threat Defense
- Décrire les paramètres avancés de l'appareil Cisco Secure Firewall Threat Defense
- Configurer le routage dynamique sur Cisco Secure Firewall Threat Defense
- Configurer la traduction d'adresse réseau avancée sur Cisco Secure Firewall Threat Defense
- Configurer la politique de décryptage SSL sur Cisco Secure Firewall Threat Defense
- Déployer le VPN d'accès à distance sur Cisco Secure Firewall Threat Defense
- Déployer des politiques basées sur l'identité sur Cisco Secure Firewall Threat Defense
- Déployer un VPN IPsec de site à site sur Cisco Secure Firewall Threat Defense
- Déployer des paramètres de contrôle d'accès avancés sur Cisco Secure Firewall Threat Defense
- Décrire la gestion avancée des évènements sur Cisco Secure Firewall Threat Defense
- Décrire les intégrations disponibles avec Cisco Secure Firewall Threat Defense
- Dépanner le flux de trafic à l'aide des options avancées de Cisco Secure Firewall Threat Defense
- Décrire les avantages de l'automatisation de la configuration et des opérations de Cisco Secure Firewall Threat Defense
- Décrire la migration de la configuration vers Cisco Secure Firewall Threat Defense.

PRÉREQUIS

Avoir suivi les cours CCNA « Cisco Solutions - Implementing and administering » et SFWIPF « Cisco Firewall Threat Defense - Fundamentals and Intrusion Prevention », ou avoir les connaissances équivalentes. Connaître le protocole de contrôle de transmission/protocole Internet (TCP/IP) et avoir des connaissances de base des protocoles de routage.

DURÉE

5 jours (35h)

TARIF

4260 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Securing Email with Cisco Email Security Appliance

[SESA]

CERTIFICATION

300-720 *(tarif : 476€)*

PUBLIC CONCERNÉ

Ingénieurs, administrateurs, architectes et techniciens sécurité, ingénieurs d'exploitation et réseau, administrateurs, techniciens et gestionnaires réseau, concepteurs de systèmes, intégrateurs et/ou partenaires Cisco.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire et administrer le Cisco Email Security Appliance
- Contrôler les domaines des expéditeurs et des destinataires
- Contrôler le spam avec Talos SenderBase et l'anti-spam
- Utiliser les filtres antivirus et anti-outbreak
- Utiliser les politiques de messagerie
- Utiliser les filtres de contenu
- Utiliser les filtres de messages
- Prévenir la perte de données
- Effectuer des requêtes LDAP (Lightweight Directory Access Protocol)
- Authentifier les sessions SMTP (Simple Mail Transfer Protocol)
- Authentifier les emails
- Chiffrer les emails
- Utiliser les quarantaines systèmes et les méthodes de livraison
- Effectuer une gestion centralisée à l'aide de clusters
- Tester et dépanner.

PRÉREQUIS

Avoir des compétences et connaissances sur les services TCP/IP (y compris le Domain Name System : DNS, Secure Shell (SSH), File Transfer Procol (FTP), Simple Network Management Protocol (SNMP), HTTP et HTTPS) et avoir une expérience en matière de routage IP. De plus, il est recommandé d'avoir suivi les cours CCNA « Cisco Solutions - Implementing and administering » et SCOR « Cisco Security Core Technologies - Implementing and operating », ou avoir les connaissances équivalentes. Afin d'obtenir la certification CCNP Security, il faut avoir passé l'examen Core 350-701 et l'examen 300-720.

DURÉE

4 jours (28h)

TARIF

3560 €HT

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

Fonctionnalités avancées

Cours Officiel

Cisco Identity Services Engine - Implementing and configuring

[SISE]

CERTIFICATION

300-715 *(tarif : 476€)*

PUBLIC CONCERNÉ

Ingénieurs en sécurité des réseaux (y compris les réseaux sans fil), administrateurs ISE et/ou intégrateurs et partenaires Cisco.

OBJECTIFS PÉDAGOGIQUES

A l'issue de cette formation, vous serez capable de :

- Décrire les déploiements Cisco ISE, y compris les composants de base du déploiement et comment ils interagissent pour créer une architecture de sécurité cohésive
- Exposer les avantages d'un tel déploiement et comment chaque capacité Cisco ISE contribue à ces avantages
- Décrire les concepts et configurer les composants liés à l'authentification 802.1X et au MAC Authentication Bypass (MAB), à la gestion d'identité et aux services de certificats
- Représenter comment les stratégies Cisco ISE sont utilisées pour mettre en œuvre l'authentification et l'autorisation, et comment exploiter cette capacité pour répondre aux besoins de votre organisation
- Décrire les dispositifs d'accès au réseau (NAD) tiers, Cisco TrustSec et Easy Connect
- Reconnaître et configurer l'authentification Web, les processus, le fonctionnement et les services invités, y compris les composants d'accès invités et divers scénarios d'accès invités
- Décrire et configurer les services de profilage Cisco ISE, et surveiller ces services pour améliorer votre connaissance de la situation des points d'extrémité connectés au réseau
- Appliquer les bonnes pratiques pour le déploiement de ce service de profilage dans votre environnement spécifique
- Expliquer les défis, les solutions, les processus et les portails BYOD (Bring Your Own Device)
- Configurer une solution BYOD et expliquer la relation entre les processus BYOD et leurs composantes de configuration connexes
- Décrire et configurer les différents certificats liés à une solution BYOD.

PRÉREQUIS

Avoir des connaissances de base sur l'interface de ligne de commande (CLI) du logiciel Cisco IOS, sur le client de mobilité sécurisé Cisco AnyConnect, sur les systèmes d'exploitation Microsoft Windows et sur la norme 802.1X. De plus, il est recommandé d'avoir suivi les cours CCNA « Cisco Solutions - Implementing and administering » et SCOR « Cisco Security Core Technologies - Implementing and operating », ou avoir les connaissances équivalentes. Afin d'obtenir la certification CCNP Security, il faut avoir passé l'examen Core 350-701 et l'examen 300-715.

DURÉE

5 jours (35h)

TARIF

4160 €^{HT}

LES PLUS DE LA FORMATION

Le support de cours et les labs sont en anglais.

Consultez le programme détaillé et les prochaines dates en scannant ce code

MaCarrière

m2i Formation

DÉCOUVREZ TOUTE L'OFFRE DE FORMATIONS MÉTIERS M2i POUR DÉMARRER VOTRE NOUVELLE VIE

macarriere.m2iformation.fr

Une solution du groupe

m2i Formation

MonCPF m2i Formation · 2i Academy · m2i Scribtel · m2i Skills

TOUS NOS CENTRES À VOTRE ÉCOUTE

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
11 rue Joseph Fourier
L'atelier Gourmand d'Angers
49070 Beaucouzé
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
Campus Eductive Bordeaux
37 rue du Jardin Public
33000 Bordeaux
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
3 place Jean Nouzille
14000 Caen
Tél. : 02 31 44 24 46
caen@m2iformation.fr

CHÂTEAUROUX
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

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

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

METZ
Immeuble B6
9 rue Graham Bell
57070 Metz
Tél. : 03 83 90 58 28
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 Vandoeuvre-Lès-Nancy
Tél. : 03 83 90 58 28
nancy@m2iformation.fr

NANTES
2/4 rue Michael Faraday
Ampère - Bâtiment B
44800 Saint-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

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

PARIS LA DÉFENSE
18-19 place des Reflets
92400 Courbevoie
Tél. : 01 49 67 09 50
paris@m2iformation.fr

PARIS SAINT-DENIS
52 rue Charles Michels
Entrée Sud
93200 Saint-Denis
Tél. : 01 49 67 09 50
paris@m2iformation.fr

POITIERS
15 avenue René Cassin
Bureaux du Lac
86360 Chasseneuil-du-Poitou
Tél. : 05 49 55 13 75
poitiers@m2iformation.fr

REIMS
Maison des Agriculteurs (MDA)
2 rue Léon Patoux
51100 Reims
Tél. : 03 26 02 48 45
reims@m2iformation.fr

RENNES
8 square du Chêne Germain
RDC droite
Les Lanthanides - Bât F2 - Promotheum
35510 Cesson-Sévigné
Tél. : 02 30 04 12 02
rennes@m2iformation.fr

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

SAINT-ÉTIENNE
10 rue du Plateau des Glières
Qosinus
42000 Saint-Étienne
Tél. : 04 72 68 99 60
saintetienne@m2iformation.fr

SOPHIA-ANTIPOLIS
MARCO POLO 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

TOULOUSE
78 allées Jean Jaurès
Bâtiment Allianz étage 5
(entrée via rue Arnaud Vidal)
31000 Toulouse
Tél. :04 67 82 81 80
toulouse@m2iformation.fr

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

VALENCE
4 rue d'Aubigny
Le Terra Mundi
69003 Lyon
Tél. : 04 72 68 99 60
valence@m2iformation.fr

GUADELOUPE
3617 boulevard du Marquisat de Houelbourg
Immeuble Simkel - ZI Jarry
1er étage
97122 Baie Mahault
guadeloupe@m2iformation.fr

GUYANE
Route de Montabo 1
Avenue Gustave Charlery
Immeuble Faic
97300 Cayenne
guyane@m2iformation.fr

MARTINIQUE
11 rue des Arts et Métiers
Immeuble Avantage
Lotissement Dillon Stade
97200 Fort-de-France
martinique@m2iformation.fr