4CYSEC

CYBER SECURITY EXPERT

Catalogue des formations

Développez vos compétences

#RGPD #stratégie #ingénierie_sociale #iso27001 #dpo #rssi #risques #cybersécurité #audit #pentester #sensibilisation #privacy #amélioration

édito

DÉVELOPPEZ VOS COMPÉTENCES

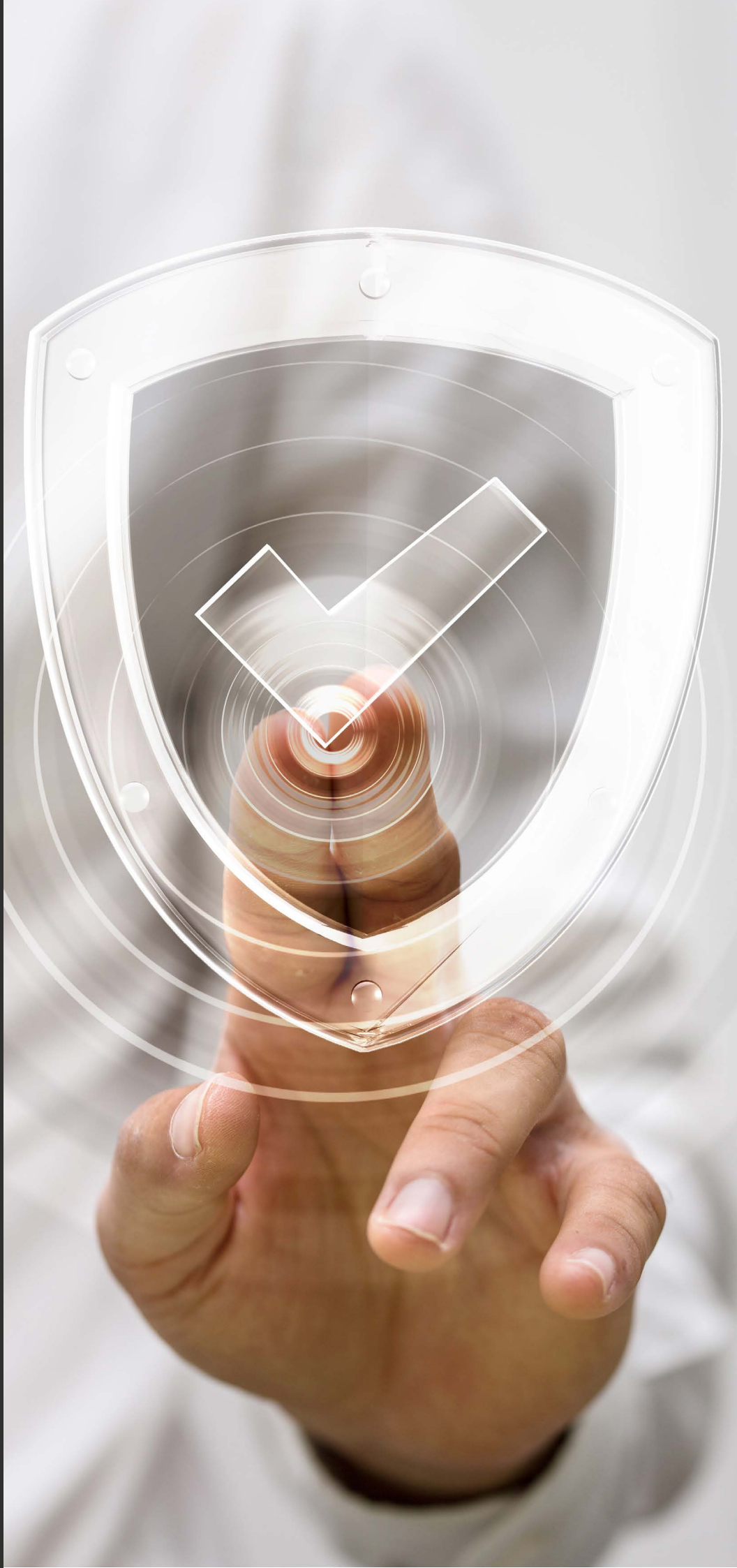
Les dernières années ont vu fleurir pléthore de nouvelles façons de se former : e-learning, blended learning, mooc, e-tutorat, vidéos etc. Quant au présentiel avec des formations inter-entreprises, intra-entreprise, séminaire, cours particulier, il reste une méthode éprouvée. Toutes ces démarches ciblent le même objectif qui est celui de vous amener à développer de nouvelles compétences au sein de votre fonction et de votre métier.

4CYSEC s'inscrit dans une **démarche qualité** au sein de son organisme de formation. Nous garantissons un ensemble de processus qui conduit à mettre en place des sessions de formation correspondantes aux besoins de qualification des personnes.

Nous analysons vos objectifs professionnels afin de **concevoir un parcours pédagogique** en adéquation avec les **compétences visées**. Nos formateurs sont **autant pédagogues qu'experts** dans leurs domaines d'intervention.

Nous accompagnons les stagiaires dans **la mise en œuvre de leurs acquis** et nous proposons notre savoir-faire pour obtenir des résultats tout au long de leur carrière sous la forme de **nouvelles compétences.**

La formation, c'est notre métier.



SOMMAIRE

Formations RGPD

Sensibilisation au RGPD page 05
Explorez la gouvernance des données page 06
Privacy by design : intégrer la protection des données personnelles dés la conception page 07
Le RGPD et la sous-traitance page 08
Réaliser son analyse d'impact sur la protection des données (PIA) page 09
Le RGPD et la norme ISO 27001 page 10
Devenir DPO : Délégué à la protection des données page 11

Formations Stratégie de la cybersécurité

Intégrer la cybersécurité à votre stratégie page 13
Sensibilisation à la Cybersécurité page 14
Les attaques par ingénierie sociale page 15

Formations Management de la Sécurité des systèmes d'information

Concevoir la sécurité de votre système d'information page 17
La Sécurité des SI et le Droit page 18
Devenir RSSI : Responsable sécurité des systèmes d'information page 19
Gérer la Sécurité du Cloud page 20
Gérer la Sécurité des smartphones et des tablettes page 21
Gérer la Sécurité des réseaux sans fil page 22
Rédiger une PSSI page 23
Auditer et contrôler la sécurité de votre système d'information page 24
Les principes clés des normes ISO 27001 et ISO 27002 page 25
ISO 27001 Lead Auditor (formation certifiante éligible au CPF) page 26
ISO 27001 Lead Implementer (formation certifiante éligible au CPF) page 27
EBIOS Risk Manager (formation certifiante éligible au CPF) page 28
ISO 27005 Risk Manager (formation certifiante éligible au CPF) page 29

Formations Hacking éthique et Sécurité des systèmes d'information

Les bases du hacking et de la cybersécurité page 31
Hacking éthique et sécurité avancée page 32
Audit de sécurité et tests d'intrusion : Pentest page 33

Formations Prévention, surveillance, détection et analyse inforensique

Surveiller, détecter et répondre aux incidents page 35
S'initier à l'analyse inforensique page 36
Perfectionner son analyse inforensique page 37

Formations Résilience et continuité d'activité

Devenir Responsable du Plan de Continuité d'Activité page 39
ISO 22301 Lead Auditor (formation certifiante éligible au CPF) page 40
ISO 22301 Lead Implementer (formation certifiante éligible au CPF) page 41

Règlement général de la protection des données personnelles

Depuis le 25 mai 2018, toutes les entreprises traitant de données à caractère personnel doivent être en conformité avec le Réglement Général de la Protection des Données, le RGPD.

Les formations de cette catégorie vous guident dans votre mise en conformité et vous permettent de gagner du temps.

En intra-entreprise, nous mettrons en place des ateliers de réflexion à vos propres cas et problématiques.

Sensibilisation au RGPD

Votre mise en conformité au RGPD est conditionnée par la compréhension et l'implication de tous les collaborateurs de votre organisation. Souvent considérés comme des maillons faibles, vos collaborateurs peuvent devenir de véritables atouts s'ils sont intégrés à la démarche.

Compétences visées

- Assurer la protection des données personnelles traitées
- Déjouer des attaques par ingénierie sociale

Objectifs pédagogiques

- Lister les concepts fondamentaux en matière de protection de données
- Concilier protection des données et contraintes sectorielles
- Acquérir les bons réflexes pour assurer la sécurité et la confidentialité des données
- Mettre en marche une démarche de mise en conformité

Public

Tout collaborateur manipulant, traitant des données à caractère personnel (toute information relative à une personne physique pouvant être identifiée) et voulant connaître les impacts de la nouvelle réglementation européenne (Règlement (UE) 2016/679)

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Les définitions et mots-clés

- Les définitions (donnée à caractère personnel, traitement, fichier etc.)
- Les nouveaux concepts du règlement européen Accountability, Privacy by Design, Analyse d'impact...

Les principes fondamentaux

- Les droits des personnes concernées
- Les finalités d'un fichier
- La transparence
- La pertinence des données
- La conservation des données
- La sécurité et la confidentialité des données

Le cadre légal en matière de protection de données personnelles

- Historique et contexte
- Le cadre légal

Contribuer à la démarche de conformité de mon organisme

- Déploiement d'une démarche en 4 étapes
- Atelier de réflexion

Durée
1 jour - 7 heures

Prix inter
850 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de la protection des données.

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Privacy by design, Le RGPD et la sous-traitance, Réaliser son analyse d'impact sur la protection des données, Le RGPD et la norme ISO 27001, Devenir DPO.

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de la gouvernance des données.

Après cette formation, vous pouvez suivre les formations Sensibilisation au RGPD, Privacy by design, Le RGPD et la sous-traitance, Réaliser son analyse d'impact sur la protection des données, Le RGPD et la norme ISO 27001, Devenir DPO.

Explorez la gouvernance des données

La donnée est aujourd'hui, l'un des actifs les plus importants dans l'entreprise. Sans gouvernance, il est pratiquement impossible de traiter ses données en respectant leur intégrité, leur disponibilité et leur sécurité.

Compétences visées

- Concevoir une démarche de gouvernance de données
- Assurer des cycles de données opérationnels

Objectifs pédagogiques

- Définir le rôle stratégique de la gouvernance des données
- Identifier les principes d'architecture des données
- Mettre en œuvre une méthode de gouvernance
- Intégrer la gestion des données maîtres (Master Data) dans la démarche

Public

Toute personne voulant mettre en place une démarche de gouvernance des données

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Définitions et notions fondamentales

- Définir les notions Donnée et Information
- Où sont les sources de données dans l'organisation
- Identifier les systèmes d'information opérationnel et décisionnel

La gouvernance des données

- Définition et enjeux de la gouvernance des données
- Les acteurs de la gouvernance des données
- Identifier la démarche de gouvernance de données

Le Master Data Management (MDM)

- Identifier le Master Data Management
- Lister les étapes de la démarche MDM
- Définir des architectures MDM
- Administrer les données maîtres
- Le rôle des utilisateurs dans le dispositif MDM

Cycle de vie des données

- Définir les typologies et les volumes de données
- Mettre en œuvre des archivages de base de données
- Sécuriser ses données

Atelier pratique

- Cas pratiques sur la gouvernance de données

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Visitez notre site 4cysec.io pour les dates
contact@4cysec.io - 09 74 76 85 78

Privacy by design : intégrer la protection des données personnelles dés la conception de votre produit ou service

Obligatoire depuis le 25 mai 2018, l'approche Privacy by design (Protection de la vie privée dès la conception) est une opportunité pour les entreprises d'apporter de la confiance vis à vis de leurs clients ainsi que de leurs salariés.

Compétences visées

- Assurer la conformité au cadre réglementaire des nouveaux produits ou services de l'entreprise
- Mettre en place la méthodologie Privacy by design

Objectifs pédagogiques

- Définir l'approche Privacy by Design et ses atouts
- Intégrer la protection des données dans les cahiers des charges de conception de nouveaux produits
- Déterminer et mettre en place une méthodologie Privacy by Design

Public

Tout manager voulant mettre en place le privacy by design pour la conception de nouveaux produits et rester en conformité au RGPD. DSI, RSSI, DPO, consultant, directeur

Prérequis

Posséder les connaissances de base sur le RGPD ou avoir déjà suivi une formation Sensibilisation au RGPD.

Programme

Rappel des notions fondamentales

- Rappel des principes du RGPD
- Rappel sur les obligations des responsables de traitement

Le Privacy by design

- Historique de la démarche
- Les articles du RGPD concernant les notions de Privacy by design et Privacy by default
- Les risques en cas de non-respect du Privacy by Design
- Exemples de cas
- Prévoir un audit de conformité dès la conception du produit
- L'analyse d'impact et les mesures de sécurité par défaut
- Mettre en place des mesures organisationnelles
- Posséder une vision globale de la méthodologie Privacy by design

Atelier de la théorie à la pratique

- Réflexions et travaux tutorés sur des cas pratiques

Durée
1 jour - 7 heures

Prix inter
900 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert du concept de Privacy by design et du RGPD.

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Le RGPD et la sous-traitance, Réaliser son analyse d'impact sur la protection des données, Le RGPD et la norme ISO 27001, Devenir DPO.

Durée
1 jour - 7 heures

Prix inter
850 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine du RGPD.

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Privacy by design, Réaliser son analyse d'impact sur la protection des données, Le RGPD et la norme ISO 27001, Devenir DPO.

Le RGPD et la sous-traitance

Avec le RGPD, toutes les organisations qui participent aux traitements de données à caractère personnel sont responsables, et susceptibles d'être sanctionnés en cas de problème. Les responsables de traitement et les sous-traitants sont fortement impactés. Les obligations de ces derniers sont considérablement renforcées.

Compétences visées

- Mettre son organisation en conformité au RGPD
- Reconnaître des contrats de sous-traitance en conformité avec ses traitements de données

Objectifs pédagogiques

- Identifier les changements majeurs apportés par le Règlement Européen (RGPD)
- Analyser les implications opérationnelles en tant que sous-traitant
- Définir et mettre en œuvre un plan d'actions pour se conformer aux nouvelles règles

Public

Sous-traitant, prestataire traitant de données personnelles pour son client, hébergeur de données, responsable de service de cloud computing, personnel en charge des activités de cloud computing, RSSI, Responsable qualité, DPO

Prérequis

Posséder les connaissances de base sur le RGPD ou avoir déjà suivi une formation Sensibilisation au RGPD.

Programme

Le RGPD et les sous-traitants

- Rappel des notions fondamentales du RGPD
- Rappel des grands principes du RGPD
- Définir le nouveau cadre légal applicable aux prestataires
- Identifier les obligations du prestataire pour démontrer sa conformité

La mise en conformité RGPD

- Tenir le registre des traitements du sous-traitant
- Désigner un Délégué à la Protection de données
- Évaluer les risques
- Mettre en œuvre les mesures de sécurité adaptées
- Concevoir de nouveaux produits en appliquant le Privacy by Design et by Default

Les obligations des contrats de sous-traitance

- Identifier les nouvelles clauses à mettre en place
- Concevoir de nouveaux contrats
- Créer des avenants aux contrats existants
- Gérer la sous-traitance de la sous-traitance

Les obligations envers le responsable de traitement

- Donner des conseils et coopérer avec le client
- Faire respecter les droits des personnes
- Garantir la protection des données
- Mener une analyse d'impact
- Notifier toute violation de données

Quelques cas de sous-traitance

- Gérer un service SaaS
- Effectuer l'hébergement de données de santé
- Être un prestataire de cloud computing

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Visitez notre site 4cysec.io pour les dates
contact@4cysec.io - 09 74 76 85 78

Réaliser son analyse d'impact sur la protection des données (Privacy Impact Assessment - PIA)

Avec le RGPD, les responsables de traitement et les sous-traitants doivent, dans certains cas, mettre en place des analyses de risques. L'enjeu est d'analyser les risques liés à l'atteinte des données personnelles, de les prioriser et de prendre des mesures en conséquence.

Compétences visées

- Assurer la conformité de son organisation au RGPD
- Réaliser un PIA

Objectifs pédagogiques

- Identifier les principes du PIA
- Lister les différentes composantes juridiques, techniques et organisationnelles
- Évaluer les risques sur son système d'information et prendre les bonnes mesures

Public

Tout manager, DSI, RSSI, DPO, consultant, directeur

Prérequis

Posséder les connaissances de base sur le RGPD ou avoir déjà suivi une formation Sensibilisation au RGPD.

Programme

Rappels et introduction au PIA

- Rappel des notions fondamentales du RGPD
- Rappel des principes fondateurs du RGPD
- Définir la notion d'analyse d'impact sur la protection des données (PIA)
- Lister les traitements concernés par le PIA
- Intégrer le PIA dans la démarche de conformité
- Identifier les référentiels juridiques

Mettre en œuvre un PIA

- Décrire les différentes approches possibles
- Lister les outils à disposition : normatifs, de la CNIL, du G29
- Mettre en place les différentes étapes d'une analyse de risque : modèle PDCA ou EBIOS
- Appliquer les mesures opérationnelles du PIA

Valider le PIA

- Évaluer les mesures et les risques résiduels
- Impliquer la direction pour la validation finale
- Communiquer sur sa démarche

Réaliser la documentation d'un PIA

- Concevoir le rapport d'analyse d'impact PIA
- Utiliser la documentation en vue d'une amélioration continue de ses mesures de sécurité

Atelier

- Cas pratiques sur la réalisation d'un PIA

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert en gestion des risques SI.

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Privacy by design, Le RGPD et la sous-traitance, Le RGPD et la norme ISO 27001, Devenir DPO.

Durée
1 jour - 7 heures

Prix inter
900 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert RGPD et ISO 27001

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Le RGPD et la sous-traitance, Privacy by design, Réaliser son analyse d'impact sur la protection des données, Devenir DPO.

Le RGPD et la norme ISO 27001

La norme ISO/IEC 27001 permet de mettre en œuvre un système de Management de la sécurité de l'Information. L'efficacité éprouvée de cette norme permet de poser les bases pour une mise en conformité RGPD. Par contre, une certification ISO 27001 n'est pas suffisant pour être "RGPD Ready".

Compétences visées

- Mettre son organisation en conformité au RGPD
- Reconnaître les synergies entre la norme ISO/IEC 27001 et le RGPD

Objectifs pédagogiques

- Identifier les principes apportés par le Règlement Européen (RGPD)
- Analyser les implications opérationnelles sur votre système d'information
- Intégrer des processus à son SMSI pour se conformer aux nouvelles règles

Public

RSSI, Responsable qualité, DPO, DSI, consultant, directeur

Prérequis

Connaître la norme ISO/IEC 27001 et avoir mis en place un SMSI.

Programme

Les définitions et mots-clés

- Les définitions (donnée à caractère personnel, traitement, fichier etc.)
- Les nouveaux concepts du règlement européen : Accountability, Privacy by Design, Analyse d'impact...

Les principes fondamentaux

- Les droits des personnes concernées
- Les finalités d'un fichier
- La transparence
- La pertinence des données
- La conservation des données
- La sécurité et la confidentialité des données

Les obligations du responsable de traitement

- Mettre en œuvre des mesures techniques et organisationnelles
- Apporter des preuves de la conformité des traitements
- Mettre en concordance son SMSI et ses garanties

La gestion de la sous-traitance

- Vérifier le SMSI de ses sous-traitants
- Examiner la déclaration d'Applicabilité de ses prestataires
- Les obligations des sous-traitants pour le RGPD

La notification d'une violation de données

- Mettre en place un processus viable pour réagir dans les 72 heures à une violation de données
- Mettre en corrélation les clauses A.16.1.1 à A.16.1.7 de l'ISO 27002 pour assurer cette conformité RGPD

L'analyse d'impact

- Identifier les principes de l'analyse d'impact
- Comparer l'analyse d'impact avec la gestion des risques d'un SMSI
- Adapter la méthode d'analyse des risques en impliquant les directions métiers
- Rechercher l'amélioration continue

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Devenir DPO : Délégué à la protection des données

Pilote de la mise en œuvre de la conformité RGPD de l'organisation qui l'a désigné, il doit disposer de qualités managériales, de connaissances précises, et de moyens matériels et organisationnels garantis par le responsable de traitement pour lui permettre d'exercer ses missions.

Compétences visées

- Assurer la conformité au RGPD
- Gérer les équipes métiers pour la sécurité des données
- Sensibiliser les personnes de l'organisation concernée par le RGPD

Objectifs pédagogiques

- Identifier les fonctions stratégiques de l'entreprise concernées par la mise en conformité
- Mettre en œuvre le plan d'actions de conformité au RGPD
- Surveiller la mise en oeuvre de la sécurité des données
- Interagir avec la CNIL

Public

DPO, futur DPO, toute personne dont la mission est d'assurer le respect de la protection des données personnelles au sein d'au moins une organisation

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Introduction au RGPD

- Décrire le contexte historique du RGPD
- Rappeler la Loi Informatique et Libertés
- Comparer la loi 2018 sur la protection des données personnelles et le RGPD

Les définitions et mots-clés

- Les définitions (donnée à caractère personnel, traitement, fichier etc.)
- Les nouveaux concepts du règlement européen Accountability, Privacy by Design, Analyse d'impact...

La Commission Nationale de l'Informatique et Libertés

- Définir les autorités de contrôle
- Identifier le statut de la CNIL
- Lister les missions de la CNIL
- Décrire les pouvoirs de la CNIL
- Collaborer avec la CNIL

Le rôle et les missions du DPO

- Décrire la nomination, la fonction, les responsabilités et les missions du DPO
- Définir le rôle DPO au sein de l'entreprise
- Identifier le cadre juridique du RGPD

Gestion des risques

- Identifier les méthodologies de l'analyse d'impact
- Créer un plan de mesures
- Surveiller la mise en oeuvre de la sécurité des données

Gestion des incidents

- Faire face à un incident de sécurité
- Mettre en place un plan de continuité de l'activité
- Évaluer l'impact sur la protection des données personnelles
- Avertir la CNIL et les personnes concernées

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert en protection de données RGPD, CIL/DPO.

Après cette formation, vous pouvez suivre les formations Explorez la gouvernance des données, Privacy by design, Le RGPD et la sous-traitance, Réaliser son analyse d'impact sur la protection des données, Le RGPD et la norme ISO 27001.

Stratégie de la cybersécurité

Les derniers mois ont montré très concrètement les conséquences désastreuses des cyberattaques mondiales. Les organisations doivent mettre les moyens pour limiter les impacts de telles attaques et intégrer la sécurité dans leur plan stratégique.

Lorsqu'une approche globale de la cybersécurité est mise en place en amont de la stratégie business, les entreprises s'adaptent mieux aux risques, les traitent plus efficacement et protègent leurs actifs. Cela devient une véritable plus-value sur le marché.

Intégrer la cybersécurité à votre stratégie

Systèmes d'informations informatisés, objets connectés, données dans le Cloud, tous vos actifs sont, aujourd'hui, des cibles potentielles aux cyberattaques. Il est donc primordial de concevoir la sécurité de votre entreprise en l'intégrant à vos priorités stratégiques.

Compétences visées

- Concevoir une Cyber stratégie pour son organisation
- Être à l'écoute des nouvelles menaces
- Mettre en place une amélioration continue des process organisationnels et techniques

Objectifs pédagogiques

- Identifier les enjeux de la Cybersécurité
- Lister les atouts business et les responsabilités de la Cybersécurité
- Intégrer la Cybersécurité dans vos processus de conception
- Construire une Cyber veille efficace

Public

Tout manager voulant mettre en place une stratégie en prenant en compte les risques et la conformité liés à son système d'information. DSI, RSSI, consultant, directeur.

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Identifier les enjeux de la Cybersécurité

- Rappeler les différents actifs des systèmes d'informations d'aujourd'hui
- Identifier les grandes typologies d'attaques
- Décrire le cadre juridique de la Cybersécurité
- Lister les acteurs publics : ANSSI, CNIL, etc. et les acteurs privés

Lister les atouts business et les responsabilités de la Cybersécurité

- Évaluer les enjeux business, politiques et économiques
- Dimensionner la mise en place de votre Cybersécurité en fonction de ces enjeux
- Cerner les responsabilités liées à la sécurité de l'information

Intégrer la Cybersécurité dans vos processus de conception

- Cartographier vos processus de conception de vos produits et/ou services
- Définir les risques Cyber et les évaluer
- Gérer les risques de vols, de pertes ou de destructions d'information

Construire une Cyber veille efficace

- Assurer une veille technologique et juridique
- Favoriser la réactivité de votre entreprise face à la cybercriminalité

Communiquer efficacement pour lutter contre les risques Cyber

- Lister les messages à faire passer en interne
- Rédiger la charte d'usage des actifs informatiques en vous mettant à la place des utilisateurs
- Identifier les points clés d'une politique de communication interne en cybersécurité
- Planifier des évènements de communication sur le long terme

Durée
1 jour - 7 heures

Prix inter
850 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine du management de la Cybersécurité.

Après cette formation, vous pouvez suivre les formations Sensibilisation à la Cybersécurité et Les attaques par ingénierie sociale.

Durée
1 jour - 7 heures

Prix inter
850 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert en cybersécurité et en sensibilisation des personnes.

Aprés cette formation, vous pouvez suivre la formation Les attaques par ingénierie sociale.

Sensibilisation à la Cybersécurité

De plus en plus d'entreprises prennent conscience aujourd'hui que la cybersécurité n'est plus une option. Pourtant il reste un maillon faible dans la mise en œuvre de la sécurité : la sensibilisation. Des cyberattaques à grande échelle ont été possibles grâce à une non-connaissance des pièges simples.

Compétences visées

- Appliquer les bonnes pratiques de la cybersécurité
- Rester en veille sur les menaces potentielles

Objectifs pédagogiques

- Appréhender et comprendre les attaques informatiques
- Identifier les menaces informatiques
- Adopter les bonnes pratiques pour se protéger

Public

Toute personne voulant être sensibilisée aux menaces liées aux attaques informatiques et savoir s'en protéger.

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Introduction à la cybersécurité
- Définir les notions d'information et de système d'information
- Identifier la sécurité des systèmes d'information
- Lister les bénéfices de sécuriser les actifs de l'entreprise
- Enumérer les attaques informatiques d'aujourd'hui et leurs motivations
- Identifier les risques pour l'entreprise

Les attaques indoor
- Définir les attaques par clé USB
- Décrire les possibles attaques via le réseau Ethernet
- Identifier les vols ou destructions de matériels
- Identifier une attaque par un employé mal intentionné

Les attaques distantes
- Identifier la portée et la sécurité de son réseau WIFI
- Lister les attaques via le Web

Les attaques par ingénierie sociale
- Décrire la notion d'ingénierie sociale
- Définir la méthode du phishing
- Repérer des personnes malveillantes au téléphone
- Vérifier la provenance de ses mails et pièces jointes
- Exemples d'attaques basées sur l'ingénierie sociale

Les attaques aux mots de passe
- Définir le rôle et les usages des mots de passe
- Lister les attaques via les mots de passe
- Gérer ses mots de passe
- Décrire l'intérêt de la double authentification

Les bonnes pratiques de sécurité au quotidien
- Identifier les réflexes à appliquer dans son travail
- Détecter des menaces potentielles
- Réagir rapidement à un événement de sécurité
- Alerter son entreprise d'un incident

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Les attaques par ingénierie sociale

L'ingénierie sociale ("social engineering") est une technique qui permet d'accéder à des informations par la manipulation de personnes et elle ne s'applique pas seulement au domaine de l'informatique, car elle peut survenir dans la vie de tous les jours et plus particulièrement sur le lieu de travail. Téléphone, émail, réseaux sociaux et bien sûr présence physique sont des moyens employés en ingénierie sociale.

Compétences visées

- Identifier les menaces par ingénierie sociale
- Sensibiliser ses collègues à la menace d'ingénierie sociale

Objectifs pédagogiques

- Définir les pratiques de l'ingénierie sociale
- Identifier les menaces potentielles
- Réagir et alerter son organisation

Public

Toute personne voulant identifier les attaques par ingénierie sociale

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Introduction

- Définir l'ingénierie sociale
- Lister les risques liés à l'ingénierie sociale

Les vulnérabilités humaines

- Identifier les sentiments, comportements et instincts de l'humain
- Lister les vulnérabilités courantes
- Énumérer les modes de perception
- Définir la PNL, programmation neuro-linguistique

Les attaques par ingénierie sociale

- Inciter à faire une action
- Manipuler une personne
- Créer un faux document
- Usurper une identité

Le phishing (hameçonnage)

- Identifier le phishing par émail
- Identifier le phishing via le web
- Identifier le phishing par téléphone
- Signaler un phishing

Sensibilisation du personnel

- Respecter la politique d'accès aux locaux
- Identifier les bonnes pratiques
- Réaliser des audits de sécurité

Études de cas

- Mise en pratique sur des cas d'ingénierie sociale

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans l'ingénierie sociale et les attaques liées.

Management de la sécurité des systèmes d'information

La gestion de l'information et la sécurité des actifs sont aujourd'hui des enjeux de management à part entière. La norme ISO/IEC 27001:2013 permet d'y répondre et place la sécurité de l'information au cœur de l'organisation.

Le management de la sécurité des systèmes d'information demande des compétences multiples et de mettre en place des principes comme la gouvernance, la gestion, la méthodologie et la technologie, l'analyse des risques, la politique, la stratégie, et l'amélioration. Le métier de responsable de sécurité des systèmes d'information (RSSI) devient incontournable pour permettre aux organisations de mettre leur sécurité en avant. Celle-ci devient une plus-value pour leurs clients.

Concevoir la sécurité de votre système d'information

Les conséquences d'une mauvaise sécurité sont multiples. Les organisations, mais aussi la vie privée des personnes peuvent être impactées. Il est évident que la sécurité ne peut être garantie à 100 % et demande donc la mise en œuvre de multiples mesures sur le système d'information.

Compétences visées

- Identifier et analyser les vulnérabilités de votre système d'information
- Gérer la sécurité de votre système d'information

Objectifs pédagogiques

- Décrire la cybercriminalité en 2018
- Identifier la sécurité des applications, du réseau, du cloud, des tablettes et smartphones
- Mettre en oeuvre des processus de vérification de la sécurité de votre système d'information (SI)

Public

Responsable informatique, administrateurs système & réseau, consultant, manager du SI, RSSI, DPO, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Les attaques Cyber en 2018

- Décrire l'évolution de la cybercriminalité
- Identifier les agents de menace
- Lister les nouvelles menaces
- Identifier les failles de sécurité

Les notions fondamentales de la sécurité

- Définir les principes de sécurité
- Lister les éléments clés : risque, menace...
- Décrire les méthodes de gestion de risques
- Mettre en place un SMSI

La sécurité du réseau

- Décrire les fonctions des serveurs proxy
- Créer des périmètres de sécurité via des firewalls
- Mettre en place des sondes IDS / IPS
- Expliquer les zones DMZ
- Sécuriser la virtualisation
- Gérer la sécurité du Cloud

La sécurité des postes clients

- Identifier les menaces sur les postes clients
- Gérer les logiciels anti-virus
- Identifier les vulnérabilités du Web
- Mettre en place de la cryptographie
- Identifier les fonctions de hachage
- Définir les architectures à clés publiques
- Mettre en œuvre l'authentification des personnes

La sécurité d'Internet

- Identifier les attaques sur les protocoles SSL/TLS
- Lister les attaques sur les flux HTTPS
- Définir la sécurité Wifi et ses attaques spécifiques
- Le standard de sécurité IEEE 802.11i.

La sécurité des tablettes et des smartphones

- Lister les menaces sur les appareils mobiles
- Mettre en place des solutions EMM

Surveiller et gérer la sécurité de votre SI

- Identifier les principaux risques selon l'OWASP
- Mettre en œuvre des audits de sécurité
- Mettre en place un plan de continuité de l'activité

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de la sécurité informatique.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager, Sécurité des réseaux sans fil , Sécurité du Cloud et Sécurité des smartphones et des tablettes.

Durée
1 jour - 7 heures

Prix inter
900 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert en droit sur la sécurité des systèmes d'information.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

La Sécurité des SI et le Droit

La sécurité des systèmes d'information et la manipulation de données à caractère personnel sont des principes réglementées par des lois. Les organisations peuvent alors se demander quelle peut être la responsabilité du RSSI ou du directeur SI, quelles réactions et communication mettre en place face à une plainte et quelle marge de manœuvre ont-elles pour sécuriser leurs actifs en respectant les droits des personnes concernées.

Compétences visées

- Gérer la conformité de son SI
- Se tenir informé des lois et règlements concernant les données de son organisation

Objectifs pédagogiques

- Définir le cadre juridique appliqué aux SI
- Faire respecter les règles juridiques au sein de son organisation
- Garantir la conformité de son SI

Public

RSSI, DSI, administrateurs réseaux, chefs de projet, consultant, directeur

Prérequis

Une connaissance de systèmes d'information et des notions de base en sécurité SI sont recommandées.

Programme

Introduction à des notions juridiques

- Décrire la loi Informatique et libertés
- Définir le cadre juridique d'un SI
- Lister les principes fondamentaux du règlement de la protection des données RGPD
- Énumérer les conditions de licéité des traitements
- Lister les sanctions possibles de la CNIL
- Exemples de sanctions

Gérer la communication via Internet

- Décrire les notions fondamentales de cette communication
- Définir le degré de secret des émails
- Mettre en place de chiffrement
- Faire des audits de sécurité des prestataires

Conserver des traces

- Définir le cadre juridique des données de trafic
- Encadrer les procédures de traçabilité
- Avertir les utilisateurs

Gérer le traitement des données à caractère personnel

- Lister les droits des personnes concernées
- Vérifier la mise en application de ses droits
- Réagir à une violation de données avec un cadre juridique

Surveiller les salariés

- Lister les possibilités de l'employeur
- Décrire le respect de la vie privée «résiduelle»
- Gérer les fichiers professionnels et personnels
- Contrôler la navigation web
- Accéder à l'ordinateur du salarié

Mettre en place une charte informatique

- Réglementer les usages informatiques du SI
- Informer des sanctions possibles

Ateliers

- Cas pratiques de réflexion de Droit sur des scénarios de sécurité

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Devenir RSSI : Responsable sécurité des systèmes d'information

Le RSSI est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise. Il doit garantir la disponibilité, la sécurité, et l'intégrité du système d'information et des données. La réalisation de ces missions s'effectue dans le cadre d'un travail d'équipe.

Compétences visées

- Mettre en place des procédures de sécurité du système d'information (SI)
- Garantir le respect des procédures et la sécurité du SI
- Former et informer les utilisateurs du SI

Objectifs pédagogiques

- Concevoir la politique de sécurité du SI
- Analyse les risques et mettre en place des mesures de sécurité
- Documenter son SMSI
- Sensibiliser et former les personnes

Public

Futurs RSSI, directeurs, chefs de projet, ingénieurs en sécurité des systèmes d'information, toute personne souhaitant connaître les fonctions du métier du RSSI.

Prérequis

Une connaissance de systèmes d'information et des notions de base en sécurité SI sont recommandées.

Programme

Introduction

- Définir le métier de RSSI
- Lister les compétences nécessaires au métier

Concevoir la politique de sécurité

- Définir les objectifs et les besoins du SI
- Mettre en place des procédures
- Décrire l'organisation et de sa politique de sécurité

Réaliser l'analyse de risques

- Évaluer les risques et les menaces
- Analyser et aider à la prise de décisions
- Étudier les moyens assurant la sécurité
- Établir un plan de prévention

Sensibiliser et former les personnes

- Sensibiliser la direction générale
- Former les directions opérationnelles et métiers
- Participer à la réalisation de la charte de sécurité
- Animer des séminaires de sensibilisation à la sécurité
- Conseiller et assister les équipes

Mettre en œuvre les procédures

- Réaliser une validation technique des outils de sécurité
- Définir des normes et des standards de sécurité
- Élaborer des règles de sécurité

Auditer et contrôler

- Vérifier que les plans de sécurité ont été bien faits
- Garantir que les équipes suivent les procédures
- Mettre à jour les vulnérabilités de l'entreprise

Faire une veille technologique et prospective

- Suivre les évolutions réglementaires et techniques
- Faire une veille sur la sécurité logique et physique du système d'information

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le management de la sécurité des systèmes d'information.

Après cette formation, vous pouvez suivre les formations La Sécurité des SI et le Droit, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans la sécurité du Cloud Computing.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

Gérer la sécurité du cloud

Le Cloud change profondément les usages de l'Informatique. Quel que soit le contexte opérationnel, toutes les étapes de mise en œuvre d'un service Cloud doivent inclure la gestion de la sécurité.

Compétences visées

- Mettre en conformité le Cloud de son organisation
- Gérer la sécurité du Cloud Computing

Objectifs pédagogiques

- Identifier les risques du Cloud en terme de sécurité de l'information
- Décrire les cadres juridiques et réglementaires des services Cloud
- Définir la sécurité du Cloud Computing

Public

Responsable informatique, consultant, manager du SI, RSSI, DPO, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Identifier les composantes d'une architecture Cloud
- Décrire les contextes d'utilisation

Lister les services de Cloud Computing

- Identifier les différentes offres
- Analyser les déploiements

Analyser la sécurité : opportunités et contraintes

- Identifier les différents niveaux de sécurité
- Lister les vulnérabilités du terminal d'accès au Datacenter du Cloud
- Lister les vulnérabilités des Clouds ouverts

Gérer la conformité

- Identifier les aspects légaux et contractuels
- Lister les niveaux de services
- Mettre en œuvre des audits de sécurité

Organiser les processus

- Identifier les applications éligibles pour le Cloud
- Créer un plan de continuité d'activité
- Gérer la responsabilité de l'entreprise
- Optimiser les contrats de sous-traitance

Gérer l'architecture

- Définir la sécurité des données
- Définir la sécurité des systèmes et des applications
- Gérer les identités et les accès
- Gérer la cryptographie et la virtualisation

Concevoir avec la Security by design

- Cloisonner et isoler des applications
- Combiner des mesures de sécurité
- Mettre en œuvre un trafic IP optimal

Gérer l'utilisation de périphériques personnels (BYOD)

- Identifier les périphériques et leurs contraintes
- Définir les vulnérabilités des périphériques
- Affecter des droits sur le Cloud
- Mettre en place de la surveillance adaptée
- Sensibiliser le personnel à la sécurité

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Visitez notre site 4cysec.io pour les dates
contact@4cysec.io - 09 74 76 85 78

Gérer la sécurité des smartphones et des tablettes

Aujourd'hui, la quantité de terminaux mobiles dépasse celle des PC et le nombre de menace sur ces appareils croit de manière exponentielle. Or beaucoup d'utilisateurs professionnels considèrent leur appareil mobile comme un deuxième ordinateur. Ils consultent leurs messageries et veulent aussi un accès aux données métier. La sécurité mobile devient alors un enjeu stratégique pour les organisations.

Compétences visées

- Identifier les vulnérabilités des smartphones et des tablettes
- Gérer la sécurité par l'EMM (Enterprise Mobile Management)
- Mettre en place une veille de la sécurité mobile

Objectifs pédagogiques

- Identifier les vulnérabilités des appareils mobiles
- Lister les technologies et les solutions pour protéger les plates-formes et les applications mobiles
- Définir la sécurité des usages professionnels dans le cadre du BYOD (Bring Your Own Device)

Public

Responsable informatique, consultant, manager du SI, RSSI, DPO, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Définir les tendances actuelles
- Lister les impacts business

Identifier les vulnérabilités

- Lister les vulnérabilités des smartphones et tablettes
- Définir les risques d'escalade de privilège
- Lister les attaques des systèmes d'exploitation mobiles
- Expliquer les différents niveaux d'attaque

Gérer la sécurité par l'EMM (Enterprise Mobile Management)

- Définir le MDM (Mobile Device Management)
- Définir le MAM (Mobile Application Management)
- Définir le MCM (Mobile Content Management)

Mettre en œuvre un MDM

- Permettre une utilisation limitée à certaine zones géographiques
- Renforcer les couches logicielles et créer une Trust Zone
- Suivre les consommations
- Sécuriser l'accès de l'utilisateur au terminal

Mettre en œuvre un MAM

- Isoler par les containers
- Gérer les stores privés et autorisés
- Cloisonner les interactions entre terminal et serveur

Mettre en œuvre un MCM

- Sécuriser les mobiles contre les fuites des données
- Surveiller les activités
- Mettre en place le chiffrement des données
- Proposer un stockage sécurisé et partagé pour les mobiles

Gérer la sécurité des appareils personnels BYOD

- Insérer le terminal dans l'EMM
- Responsabiliser l'utilisateur
- Fixer un cadre légal d'utilisation

Gérer la sécurité de l'accès aux serveurs

- Lister les solutions : VPN SSL, Firewall
- Mettre en place une authentification forte d'accès aux réseaux
- Sécuriser pour la GSM/4G et le WiFi

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans la sécurité des appareils mobiles.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans la sécurité des réseaux sans fil.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

Gérer la sécurité des réseaux sans fil

Afin de garantir un niveau de sécurité optimal sur un réseau sans fil, il est primordial de mettre à jour ses connaissances sur les vulnérabilités inhérentes à ce type de réseau. Les configurations non sécurisées par défaut des nouveaux équipements tels que les objets connectés facilitent les attaques.

Compétences visées

- Identifier et analyser les vulnérabilités de vos réseaux sans fil
- Gérer la sécurité de vos réseaux sans fil

Objectifs pédagogiques

- Décrire les technologies sans fil
- Identifier les faiblesses des différents systèmes sans fil
- Mettre en œuvre des mesures de sécurité sur les réseaux sans fil

Public

Responsable informatique, administrateurs système & réseau, consultant, manager du SI, RSSI, DPO, chef de projet

Prérequis

Avoir des connaissances en administration système et réseau est nécessaire.

Programme

Introduction
- Décrire les technologies sans fil
- Lister les modes de chiffrement

Gérer un réseau WiFi
- Décrire les techniques d'attaque connues
- Mettre en place des mesures de protection

Mettre en place un VPN
- Lister les différentes technologies et protocoles
- Sécuriser le transport des données
- Décrire les techniques d'attaques connues

Identifier les technologies radio logicielle
- Définir les principes de la software-defined radio (SDR)
- Reconnaître les principaux types de modulation
- Décoder un signal avec des outils open-source

Gérer des connexions Bluetooth
- Identifier les principes du Bluetooth
- Lister les principaux risques
- Exemples d'attaque via des montres connectées

Mettre en place du NFC
- Identifier les principes de la technologie NFC
- Définir les points faibles du NFC
- Lister les attaques connues

Gérer la téléphonie mobile
- Lister les technologies concernées
- Identifier le fonctionnement du SMS
- Définir les faiblesses des méthodes de chiffrement
- Définir les technologies 3G / 4G
- Lister les attaques connues sur ces technologies

Gérer les équipements radio portatifs TETRA
- Définir la technologie associée
- Comparer avec le GSM
- Lister les attaques connues sur cette technologie

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Visitez notre site 4cysec.io pour les dates
contact@4cysec.io - 09 74 76 85 78

Rédiger une PSSI

La politique de sécurité des systèmes d'information (PSSI) doit pouvoir illustrer la vision stratégique de la direction d'une organisation en matière de sécurité des systèmes d'information (SSI) tout en respectant des objectifs concrets. Dans ce but, l'organisation doit appliquer une démarche méthodique.

Compétences visées

- Mettre en œuvre une PSSI
- Piloter une PSSI

Objectifs pédagogiques

- Concevoir la PSSI de son organisation
- Rédiger la PSSI et la communiquer
- Mettre à jour la PSSI

Public

RSSI, DSI, Chefs de projet SMSI, responsables de la gestion de la sécurité de l'information, conseillers experts, consultants

Prérequis

Posséder des connaissances sur les concepts de la sécurité de l'information.

Programme

Identifier les fondamentaux de la SSI

- Décrire les bases de la sécurité des données, des processus et des actifs
- Documenter, vérifier et prouver la mise en œuvre de la sécurité
- Respecter les réglementations et les lois

Initier sa politique de sécurité

- Identifier les besoins des parties prenantes
- Impliquer le Management et les métiers de l'organisation
- Définir les objectifs de la DSI

Décrire les objectifs de la Politique de Sécurité des Systèmes d'Information (PSSI)

- Définir son périmètre et son contenu
- Décrire la communication qui lui est attachée
- Définir son cycle de mise à jour
- Intégrer la PSSI dans le processus global de la SSI

Concevoir la PSSI et la rédiger

- Définir le contexte du SI concerné
- Exprimer les besoins métiers au niveau de la sécurité
- Identifier les menaces et apprécier les risques
- Définir des mesures pour gérer les risques
- Mettre en place une méthode de gestion des risques (ISO 27005, la méthode EBIOS)

Communiquer sur la PSSI

- Concevoir un plan de communication lié aux objectifs de la PSSI
- Gérer le contenu de la communication : pédagogie et objectifs généraux
- Impliquer la direction à la communication

Piloter la PSSI

- Implémenter la PSSI
- Définir des indicateurs à vérifier
- Maintenir à jour sa PSSI

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage.

Validations des acquis
Quizz final et évaluation de la formation.

Formateurs
Formateur expert dans la gestion des risques SI et dans la mise en œuvre d'une PSSI.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans la sécurité du Cloud Computing.

Après cette formation, vous pouvez suivre les formations Sécurité des applications Web, Sécurité des réseaux sans fil et Sécurité des smartphones et des tablettes.

Auditer et contrôler la sécurité de votre SI

Une organisation doit pouvoir prouver qu'elle maitrise les risques et qu'elle améliore en continu le niveau de sécurité de ses données et de ses actifs. L'audit est une démarche efficace pour piloter la sécurité des systèmes d'information (SI).

Compétences visées

- Mettre en œuvre un audit de sécurité
- Surveiller la SSI d'une organisation

Objectifs pédagogiques

- Identifier les enjeux du pilotage de la sécurité
- Concevoir un audit de sécurité
- Réaliser des tableaux de bord efficaces
- Contrôler la sécurité d'un SI

Public

Responsable informatique, consultant, manager du SI, RSSI, DPO, chef de projet, auditeurs

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Rappel sur les principes fondamentaux d'un système de management de la SSI
- Lister les exigences réglementaires et légales en matière de pilotage de la SSI

Piloter la sécurité des systèmes d'information

- Identifier les rôles et responsabilités au sein de la SSI
- Prévoir le pilotage et le suivi de la SSI

Concevoir un audit de sécurité

- Identifier les catégories d'audit
- Lister les recommandations de l'ANSSI
- Préparer un audit et son périmètre
- Prendre en compte les résultats de l'audit et prioriser les actions à mettre en place
- Définir les types de résultats : conformité, non-conformité, remarque

Mettre en place des indicateurs de surveillance de la SSI

- Lister les catégories d'indicateurs SSI de niveau stratégique et opérationnel
- Concevoir et créer des tableaux de bord d'indicateurs
- Identifier des non conformités
- Définir des mesures correctives
- Mettre en place l'amélioration continue sur la SSI

Contrôler la sécurité du SI

- Mettre en place une démarche continue de détections d'intrusion
- Mettre en œuvre la traçabilité du SI : gestion des logs, journalisation, etc.
- Contrôler périodiquement l'efficacité de la SSI
- Planifier et réaliser des revues de direction stratégiques

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Les principes clés des normes ISO 27001 et ISO 27002

La norme ISO 27001 permet une approche processus pour la mise en œuvre, le fonctionnement, la surveillance et l'amélioration du système de management de la sécurité de l'information d'une entreprise. Avec son annexe A, l'ISO 27002, elle détaille les mesures de sécurité qui peuvent être prises. L'application de ces normes permettent aux organisations de satisfaire les parties prenantes aux attentes de bonne gouvernance des données et de responsabilité.

Compétences visées

- Appliquer les normes ISO 27001 et ISO 27002 à son SMSI
- Auditer son SMSI pour vérifier la conformité à la norme ISO 27001

Objectifs pédagogiques

- Identifier les principes fondamentaux de la norme ISO 27001 et de son annexe la norme ISO 27002
- Réaliser l'appréciation des risques au sein d'une organisation
- Mettre en place des mesures de sécurité en corrélation à l'analyse des risques

Public

RSSI, directeurs, chefs de projet, ingénieurs en sécurité des systèmes d'information, toute personne souhaitant connaître les fondamentaux des normes ISO 27001 et ISO 27002.

Prérequis

Une connaissance de systèmes d'information et des notions de base en sécurité SI sont recommandées.

Programme

Introduction

- Définir une norme ISO
- Identifier les normes ISO 2700x
- Rappeler le champ de la sécurité d'un SI
- Définir la gestion de la qualité d'un SM grâce à la roue de Deming (PDCA)

Étudier la norme ISO 27001

- Identifier les exigences de la norme : articles 4 à 10
- Définir les phases du modèle PDCA sur les exigences de la norme ISO 27001

Mettre en œuvre des mesures de sécurité

- Identifier les objectifs de sécurité de l'organisation
- Réaliser une appréciation des risques
- Étudier la norme ISO 27002
- S'appuyer sur la norme ISO 27002 pour identifie les mesures de sécurité à prendre
- Documenter les mesures de sécurité
- Définir la déclaration d'applicabilité (DdA)

Auditer les mesures de sécurité

- Concevoir des audits internes pour vérifier la mise en œuvre des mesures de sécurité
- Analyser et améliorer les processus

Atelier

- Cas pratique sur l'application de la norme ISO 27001 à des exemples de SI

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le management de la sécurité des systèmes d'information

Après cette formation, vous pouvez suivre les formations RSSI, La Sécurité des SI et le Droit, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.

☑CPF formation certifiante ISO 27001 Lead Auditor

Durée
5 jours - 40 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage. Corrections d'exercices. Préparation à l'examen de certification.
Attention cette formation nécessite du travail personnel hors-session. (5 heures)

Validations des acquis
L'examen de certification a lieu le dernier jour du stage.
L'examen est disponible en français et en anglais.

Formateurs
Formateurs experts dans le domaine du management de la Cybersécurité et de l'audit.

La norme ISO/IEC 27001:2013 permet de protéger l'entreprise de toute perte, vol ou altération de données. Elle apporte des principes de conception qui permettent une sécurité globale. L'audit du SMSI fait partie intégrante de ces principes, qu'il soit interne ou externe;

Compétences visées

- Identifier un Système de Management de la Sécurité de l'Information SMSI
- Réaliser un audit de certification ISO 27001
- Manager une équipe d'auditeurs de SMSI

Objectifs pédagogiques

- Identifier les points clés du fonctionnement d'un SMSI selon l'ISO 27001
- Analyser l'environnement interne et externe d'une organisation, et se mettre en condition d'audit du SMSI
- Appliquer les lignes directrices de l'ISO 19011 pour mettre en place un audit ISO 27001
- Mettre en œuvre un audit de certification ISO 27001 avec les spécifications de l'ISO 17021
- Identifier la gestion d'une équipe d'auditeurs de SMSI

Public

Auditeurs internes, consultants, chefs de projets SMSI, toute personne responsable de la sécurité de l'information, conseillers experts

Prérequis

Posséder des connaissances sur les concepts de sécurité de l'information avec de l'expérience dans ce domaine.
Il est fortement recommandé de prendre connaissance de la norme ISO 27001 en amont de la formation.

Programme

Introduction

- Définir les principes fondamentaux d'un SI
- Définir un système de management SMSI
- Lister les objectifs des normes ISO 27001 et ISO 27002
- Présenter le processus de certification ISO 27001
- Identifier les clauses 4 à 10 de la norme ISO 27001
- Définir la gestion de la qualité d'un SM grâce à la roue de Deming (PDCA)

Planifier un audit ISO 27001

- Définir les concepts fondamentaux d'un audit
- Identifier les notions de preuve et de risque
- Préparer un audit de certification ISO 27001
- Définir l'audit documentaire d'un SMSI
- Conduire une réunion d'ouverture

Mettre en oeuvre un audit ISO 27001

- Gérer la communication avec l'audité
- Lister les principes fondamentaux de l'audit
- Rédiger des plans de tests d'audit
- Ecrire des constats d'audit
- Rédiger des rapports de non-conformité
- Mener une réunion de clôture d'un audit

Mener un suivi d'audit ISO 27001

- Évaluer des plans d'action correctifs
- Gérer les audits de surveillance ISO 27001

Examen de certification ISO 27001 Lead Auditor

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

ISO 27001 Lead Implementer

formation certifiante ☑CPF

La certification ISO/IEC 27001:2013 permet à une entreprise de renforcer la confiance de ses clients et constitue une plus-value par rapport à sa concurrence. De plus, la mise en place d'un SMSI permet de formaliser et de mettre en œuvre des processus nécessaires à la sécurité des actifs de l'entreprise.

Compétences visées

- Mettre en œuvre un Système de Management de la Sécurité de l'Information SMSI
- Analyser les risques pour établir un plan de continuité de l'activité dans une organisation
- Manager une équipe à la mise en œuvre d'un SMSI

Objectifs pédagogiques

- Identifier les points clés de la mise en œuvre d'un SMSI conforme à la norme ISO 27001
- Lister les concepts, les démarches, les méthodes, les normes et les techniques pour gérer un SMSI
- Mettre en place une gestion d'équipe efficace dans la mise en œuvre d'un SMSI
- Se préparer à la certification ISO 27001

Public

RSSI, DSI, Chefs de projet SMSI, responsables de la gestion de la sécurité de l'information, conseillers experts, consultants, auditeurs ISO 27001

Prérequis

Posséder des connaissances sur les concepts de la sécurité de l'information avec de l'expérience dans ce domaine. Il est fortement recommandé de prendre connaissance de la norme ISO 27001 en amont de la formation.

Programme

Introduction

- Définir un système de management
- Lister les objectifs des normes ISO 27001 et ISO 27002
- Définir les principes fondamentaux d'un SI
- Initialiser la mise en œuvre du SMSI
- Lister les objectifs de sécurité de l'information
- Analyser un système de management existant
- Définir le domaine d'application du SMSI

Planifier la mise en œuvre d'un SMSI

- Initier la mise en place d'un SMSI
- Intégrer la politique de sécurité
- Structure organisationnelle d'un SMSI
- Documenter l'information
- Gérer les compétences et la sensibilisation
- Analyser les impacts et apprécier les risques

Mettre en place un SMSI basé sur l'ISO 27001

- Définir sa stratégie de sécurité
- Gérer les risques en se basant sur la norme ISO 27005
- Identifier les mesures de sécurité
- Concevoir et rédiger des procédures
- Rédiger la déclaration d'applicabilité (DdA)
- Mettre en place une gestion des incidents

Contrôler et améliorer un SMSI

- Mettre en place des indicateurs (ISO 27004)
- Mettre en place de l'amélioration continue

Certifier un SMSI par la norme ISO 27001

- Réaliser un audit interne ISO 27001
- Produire une revue de direction du SMSI
- Traiter les problèmes et les non-conformités
- Se préparer à l'audit de certification ISO 27001

Examen de certification ISO 27001 Lead Implementer

Durée
5 jours - 40 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage. Corrections d'exercices. Préparation à l'examen de certification.
Attention cette formation nécessite du travail personnel hors-session. (5 heures)

Validations des acquis
L'examen de certification a lieu le dernier jour du stage. L'examen est disponible en français et en anglais.

Formateurs
Formateurs experts dans le domaine du management de la Cybersécurité.

☑CPF formation certifiante EBIOS Risk Manager

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis pendant le stage.
Corrections d'exercices.
Préparation à l'examen de certification.
Attention cette formation nécessite du travail personnel hors-session.

Validations des acquis
L'examen de certification a lieu le dernier jour du stage.

Formateurs
Formateurs experts dans la gestion des risques SI et dans la méthode EBIOS.

EBIOS (Etude des Besoins et Identification des Objectifs de Sécurité) s'est imposée comme la méthodologie phare en France pour apprécier et gérer les risques relatifs à la sécurité des systèmes d'information (SSI) dans les organisations. Créée en 1995 par l'ANSSI et régulièrement mise à jour, la méthode EBIOS permet d'élaborer et d'assurer le suivi de plans d'actions pour la gestion des risques SSI.

Compétences visées

- Appliquer la Méthode EBIOS à un SI
- Piloter la gestion des risques du SI

Objectifs pédagogiques

- Définir la méthode EBIOS
- Concevoir un processus de gestion des risques
- Piloter et réaliser une appréciation des risques EBIOS

Public

RSSI, DPO, DSI, administrateurs réseaux, chefs de projet, consultant, directeur

Prérequis

Une connaissance de systèmes d'information et des notions de base en sécurité SI sont recommandées.

Programme

Introduction

- Définir la méthode EBIOS
- Identifier la naissance de la méthode
- Lister les évolutions de la méthode EBIOS
- Définir les notions fondamentales de la méthode EBIOS 2010

Identifier un risque

- Faire l'estimation des risques
- Identifier la vraisemblance et la gravité d'un risque
- Évaluer des risques et concevoir des mesures
- Définir le risque résiduel

Mettre en œuvre la méthode EBIOS

- Mettre en place des scénarios de menace prenant compte le contexte des traitements
- Surveiller et réexaminer les risques
- Identifier des mesures de sécurité relatives aux risques
- Communiquer autour des risques

Se préparer à l'homologation de sécurité

- Définir sa stratégie d'homologation
- Créer des fiches d'expression rationnelle des objectifs de sécurité (FEROS)
- Rédiger un plan de sécurité (PDS) résumant les mesures de sécurité envisagées
- Concevoir un plan d'action avec des responsables désignés de ses actions
- Présenter un tableau de risques résiduels
- Mettre en place les procédures d'exploitation de sécurité (PES)

Atelier

- Étude de cas pratique de la méthode EBIOS de A à Z

Examen de certification EBIOS Risk Manager

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

ISO 27005 Risk Manager

formation certifiante ☑CPF

Dans la série des normes ISO 2700x, la norme ISO/IEC 27005 détaille une méthode de gestion des risques opérationnelle pour un système de management de la sécurité de l'information (SMSI). En complément d'une mise en place d'un SMSI appliquant les principes de la norme ISO 27001, la norme ISO 27005 permet une gestion des risques sur la durée avec le modèle PDCA (Plan, Do, Check, Act).

Compétences visées

- Mettre en œuvre une méthode d'appréciation des risques
- Appliquer la norme ISO 27005 sur le SMSI d'une organisation

Objectifs pédagogiques

- Identifier les points clés de la mise en œuvre de la norme ISO 27005
- Concevoir un processus de gestion des risques
- Piloter et réaliser une appréciation des risques

Public

RSSI, DSI, Chefs de projet SMSI, responsables de la gestion de la sécurité de l'information, conseillers experts, consultants

Prérequis

Posséder des connaissances sur les concepts de la sécurité de l'information avec de l'expérience dans ce domaine. Il est fortement recommandé de prendre connaissance de la norme ISO 27005 en amont de la formation.

Programme

Introduction

- Identifier les normes ISO 2700x
- Lister les objectifs de la norme ISO 27005
- Énumérer les autres méthodes (EBIOS...)
- Définir les notions fondamentales de l'ISO 27005

Identifier un risque

- Faire l'estimation des risques
- Identifier la vraisemblance et la gravité d'un risque
- Évaluer des risques et concevoir des mesures
- Définir le risque résiduel

Mettre en œuvre la norme ISO 27005

- Gérer le processus de management du risque
- Mettre en place le modèle PDCA
- Prendre en compte le contexte des traitements
- Surveiller et réexaminer les risques
- Identifier des mesures de sécurité relatives aux risques
- Communiquer autour des risques
- Identifier les mesures de sécurité
- Concevoir et rédiger des procédures
- Rédiger la déclaration d'applicabilité (DdA)
- Mettre en place une gestion des incidents

Atelier

- Étude de cas pratique de l'application de la norme ISO 27005 de A à Z

Examen de certification ISO 27005 Risk Manager

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage. Corrections d'exercices. Préparation à l'examen de certification.

Attention cette formation nécessite du travail personnel hors-session.

Validations des acquis
L'examen de certification a lieu le dernier jour du stage. L'examen est disponible en français et en anglais.

Formateurs
Formateurs experts dans la gestion des risques SI et dans la mise en œuvre de la norme ISO 27005.

Hacking éthique et sécurité des systèmes d'information

Dans les années 1980, les hackers étaient des héros de la révolution informatique. Aujourd'hui, les hackers sont souvent associés à la notion de "pirate", voire même de "terroriste". Les cyberattaques font la Une des journaux et les hackers y sont le plus souvent caricaturés. Pourtant, le hacking éthique existe et permet de sécuriser au mieux les systèmes d'informations. La cybersécurité évolue rapidement, les techniques et les technologies changent constamment, des vulnérabilités paraissent quotidiennement. Face à un système d'information, un pentester a beaucoup de travail. Chaque système peut cacher une vulnérabilité qui peut se révéler une voie royale jusqu'à la prise de contrôle du système.

Les bases du hacking et de la cybersécurité

Le hacker éthique (white hat) utilise les mêmes techniques qu'un attaquant malveillant dans le but de sécuriser un système informatique : il étudie ses méthodes, ses principes de fonctionnement, décortique sa manière d'agir. Cela lui permet de renforcer la sécurité là où elle en a besoin.

Compétences visées

- Mettre en place des tests d'intrusion au sein de systèmes d'information (SI)
- Gérer la sécurité de SI

Objectifs pédagogiques

- Découvrir les techniques de base du hacking
- Mettre en place des outils de sécurité

Public

Toute personne travaillant dans la technique souhaitant évoluer vers une mission d'expert technique en cybersécurité

Prérequis

Avoir des connaissances en administration système et réseau est nécessaire.

Programme

Décrire la législation de la sécurité des SI

Définir les tests d'intrusion

- Définir les différentes méthodes d'intrusion et leurs objectifs : boîte noire, boîte grise, boîte blanche
- Lister les techniques d'intrusion
- Identifier la classification des moyens d'intrusion
- Identifier les outils existants

Analyser la cible de l'intrusion

- Lister les méthodes d'analyse de la cible
- Définir l'OSINT, la technique de rensignement d'origine source ouverte
- Localiser un système cible

La sécurité des réseaux

- Mettre en œuvre du scanning avec Nmap
- Analyser le réseau et ses composants
- Identifier les comptes par défaut
- Exploiter les failles de sécurité et les vulnérabilités

La sécurité Web

- Lister les injections SQL
- Définir et identifier les attaques XSS (Cross-site Scripting)
- Définir les attaques LFI-RFI (Local File Inclusion / Remote File Inclusion)
- Identifier la faille CSRF (Cross site request forgery)
- Identifier et exploiter une vulnérabilité RCE (Remote Command Execution)
- Lister les outils d'exploitation

Sécuriser le système d'informations

- Lister les outils de base permettant d'assurer le minimum de sécurité
- Identifier la cryptographie, le chiffrement des données
- Mettre en place la détection d'activité anormale
- Identifier le rôle de la base de registre
- Mettre en place des firewalls

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le hack éthique.

Après cette formation, vous pouvez suivre les formations Hacking éthique et sécurité avancée, Audit de sécurité et tests d'intrusion : Pentest.

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le hack éthique.

Après cette formation, vous pouvez suivre les formations Audit de sécurité et tests d'intrusion : Pentest.

Hacking éthique et sécurité avancée

Cette formation vous permet d'avoir une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Différentes techniques d'attaques sont détaillées et accompagnées de procédures de sécurité applicables sous Windows et Linux.

Compétences visées

- Mettre en place des tests d'intrusion au sein de systèmes d'information (SI)
- Gérer la sécurité avancée d'un SI

Objectifs pédagogiques

- Définir l'impact et la portée d'une vulnérabilité
- Lister les techniques avancées de hacking
- Sécuriser un réseau

Public

Administrateurs réseaux, administrateurs Web, webmaster, hackeur

Prérequis

Avoir suivi la formation Les bases du hacking et de la cybersécurité ou en posséder les connaissances équivalentes.

Programme

La sécurité avancée des réseaux

- Identifier les techniques d'attaque Man-in-the-Middle (MITM)
- Lister les méthodes avancées de recherche de vulnérabilités dans l'infrastructure de la cible

La sécurité avancée du Web

- Définir les méthodes avancées d'exploitation SQLi
- Mettre en œuvre des méthodes avancées d'exploitation XSS

La post-exploitation sous Windows et Linux

- Analyser le système
- Exploiter des vulnérabilités et des erreurs de con figuration
- Contourner des mécanismes de sécurité
- Extraire des mots de passe
- Décrire l'attaque Pass-the-hash et l'exploiter
- Élever ses privilèges

Workshop

- Mettre en œuvre des attaques sur un laboratoire dédié à la formation et appliquer les savoirs théoriques.

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Audit de sécurité et tests d'intrusion : PenTest

L'audit de sécurité est aujourd'hui un moyen permettant d'établir à un instant t une vision de la sécurité d'un système d'information. Le périmètre, les limites légales et la déontologie d'un audit de sécurité sont des éléments à prendre en compte et ils permettent de réaliser un rapport d'audit efficace et de qualité.

Compétences visées

- Concevoir et réaliser un audit de sécurité
- Analyser et synthétiser les résultats d'un audit de sécurité

Objectifs pédagogiques

- Définir un audit de sécurité
- Mettre en œuvre un audit de sécurité
- Rédiger un rapport d'audit

Public

Responsable informatique, administrateurs système & réseau, consultant, manager du SI, RSSI, DPO, auditeur

Prérequis

Avoir des connaissances en administration système et réseau est nécessaire.

Programme

Définir un audit de sécurité et sa mise en place

- Lister les différents types d'audit
- Identifier la réglementation associée
- Définir les responsabilités de l'auditeur
- Mettre en place les précautions appropriées
- Faire preuve de déontologie

Définir le PenTest

- Décrire le PenTest et son cycle de vie
- Identifier les différents types d'attaquants
- Lister les méthodes d'audits : boîte noire, boîte blanche, boîte grise
- Identifier les avantages et les limites du Pen Test
- Décrire les cas particuliers comme le dénis de service ou l'ingénierie sociale

Préparer son audit

- Définir les objectifs de l'audit
- Concevoir le déroulement de l'audit
- Ecrire le cahier des charges de l'audit et le faire valider par l'audité
- Obtenir les habilitations nécessaires

Réaliser son audit

- Documenter son audit
- Récolter les preuves des résultats

Rédiger le rapport d'audit

- Identifier les éléments indispensables d'un rapport d'audit
- Rédiger la synthèse générale et la synthèse technique
- Mettre en forme les informations collectées
- Réaliser une appréciation du risque
- Donner des recommandations de sécurité

Transmettre le rapport

- Identifier la méthode de transmission de rapport
- Faire valider les résultats de l'audit par l'audité

Workshop

- Utiliser Metasploitable pour mener un Pentest de A à Z
- Rédiger un rapport d'audit

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans les audits de sécurité.

Après cette formation, vous pouvez suivre les formations Surveiller, détecter et répondre aux incidents, S'initier à l'analyse inforensique.

Prévention, surveillance, détection et analyse inforensique

Les entreprises et administrations connaissent la nécessité, et parfois l'obligation, de protéger leur patrimoine informationnel et de déployer les moyens de prévention et de défense à la mesure des enjeux. Une organisation défensive doit s'appuyer à la fois sur la prévention, sur la mise en place de moyens de détection et sur des capacités de réaction.

Aprés un incident de sécurité, l'inforensique (dérivé du terme anglais forensics) consiste, en l'application de processus et techniques d'investigation permettant de collecter et d'analyser des éléments ayant valeur de preuves dans un cadre juridique. L'objectif principal d'une analyse inforensique est donc de récupérer et d'analyser des données prouvant un délit numérique. L'analyse inforensique est aussi appelée l'analyse post-mortem. L'analyse inforensique demande de la rigueur et de la précision.

Surveiller, détecter et répondre aux incidents

Il existe des mesures simples sur le plan technique ou organisationnel pour prévenir les risques. La surveillance et la détection sont préconisées pour toute organisation et sont primordiales pour la prise en compte des enjeux de la sécurité de l'information.

Compétences visées

- Identifier les indicateurs de compromission (IOC)
- Mettre en œuvre les différents moyens de surveillance et de détection
- Gérer les incidents de cybersécurité

Objectifs pédagogiques

- Identifier les menaces et les attaques sur votre SSI
- Identifier les indicateurs de compromission (IOC)
- Mettre en œuvre les différents moyens de surveillance et de détection
- Anticiper et limiter l'impact des attaques
- Maîtriser les différentes étapes de gestion des incidents de sécurité

Public

Personne travaillant au sein d'une équipe de sécurité opérationnelle ou d'une équipe de réponse aux incidents, administrateur, RSSI, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Identifier les menaces en 2018
- Lister les familles d'attaques répertoriées
- Identifier les phases du processus d'attaque : Cyber Kill chain
- Comparer les Red Team, Blue Team et Hunt Team
- Définir le principe de compromission préalable

Surveiller et détecter

- Identifier une reconnaissance passive et active
- Détecter des fuites d'informations
- Scanner un réseau
- Mettre en place des pare-feux
- Mettre en place des sondes de sécurité IDS/IPS
- Mettre en place une défense active "honeypot"
- Attaquer pour mieux se défendre

Gérer les failles de sécurité

- Se mettre à jour sur les vulnérabilités du SI
- Corriger les failles web
- Mettre à jour ses applications
- Sensibiliser l'humain avec de la prévention
- Mettre en place une supervision sécurité continue
- Faire de la Security by design

Gérer les incidents

- Identifier les objectifs de l'attaquant
- Déterminer les points d'entrée
- Analyser la timeline de l'incident

Détecter la persistance

- Nettoyer une infrastructure Windows
- Identifier la persistance UNIX/Linux
- Lister les moyens employés

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de la Cybersécurité et de la détection d'attaques.

Après cette formation, vous pouvez suivre la formation S'initier à l'analyse inforensique.

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum.
Un poste par personne.
Alternance d'apports théoriques et pratiques.
Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de l'analyse inforensique.

Après cette formation, vous pouvez suivre la formation Perfectionner son analyse inforensique.

S'initier à l'analyse inforensique

En cas de piratage informatique ou d'incident de sécurité majeur, l'analyse inforensique s'impose. Appelée aussi analyse post-mortem, elle demande beaucoup de rigueur et de précision car les preuves récoltées sont parfois fragiles et volatiles.

Compétences visées

- Mettre en œuvre une analyse inforensique
- Récolter des preuves utilisables dans un cadre juridique

Objectifs pédagogiques

- Identifier les méthodes d'analyse inforensique
- Créer des scénarios d'investigation
- Trier et analyser les informations récoltées
- Rendre une synthèse de son analyse

Public

Toute personne souhaitant se lancer dans l'analyse inforensique

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Définir l'inforensique
- Expliquer l'inforensique
- Identifier le périmètre de l'investigation
- Définir le "First Responder" et sa méthode

Mettre en œuvre une analyse inforensique
- Identifier les éléments à analyser : les disques dur, leurs systèmes de fichiers, la mémoire
- Récupérer des données persistantes et volatiles
- Gérer des supports chiffrés
- Rechercher des données supprimées

Identifier les données des registres Windows
- Définir les structures de registres Windows
- Analyser les journaux d'événements

Mettre en place des scénarios d'investigation
- Identifier les accès à des contenus sécurisés
- Repérer des traces de manipulation de fichiers et de dossiers
- Vérifier la sécurité des réseaux
- Vérifier la sécurité des logiciels
- Étudier la sensibilisation des personnes à l'ingénierie sociale
- Repérer les trous de sécurité via le Web
- Identifier les principaux artefacts des systèmes OSX et Linux

Réaliser de l'inforensique réseau
- Identifier les différents types de preuves réseaux
- Lister les évènements pouvant être trouvés
- Analyser les journaux DNS, DHCP, Proxy, pare-feu
- Analyser des paquets
- Repérer les canaux de contrôle et d'exfiltration

Analyse chronologique
- Créer et analyser une timeline des événements
- Comparer des scénarios d'intrusion

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Perfectionner son analyse inforensique

Dans une attaque simple, le pirate rentre et sort aussi vite que possible. Par contre, une menace persistante avancée, ou APT (Advanced Persistent Threat), est une attaque par laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une période prolongée. Une analyse inforensique poussée peut permettre de repérer les attaques APT.

Compétences visées

- Analyser des systèmes de fichiers corrompus
- Industrialiser ses analyses inforensiques
- Automatiser des opérations

Objectifs pédagogiques

- Identifier les modalités d'une intrusion
- Retrouver des métadonnées effacées
- Analyser les mémoires et les logs
- Mettre en place de l'analyse automatisée

Public

Professionnel de l'inforensique qui souhaite renforcer et développer ses compétences dans ce domaine

Prérequis

Avoir suivi la formation S'initier à l'analyse inforensique ou posséder de l'expérience en analyse inforensique

Programme

Rappel sur l'analyse inforensique

- Définitions et périmètres

Analyser les intrusions

- Identifier les étapes d'une intrusion
- Détecter le périmètre d'une intrusion
- Analyser les impacts d'une intrusion
- Utiliser les indicateurs de compromission pour déceler la présence d'une menace

Analyser les systèmes de fichiers

- Mettre en œuvre l'analyse des systèmes de fichiers NTFS, EXTx, HFS+...
- Recouvrer des informations supprimées
- Reconstruire un système de fichiers

Analyser la mémoire

- Identifier les atouts de l'analyse de la mémoire
- Lister les principales structures de mémoire : Linux / MacOS / Windows
- Choisir des outils d'analyse de mémoire
- Identifier les processus et les processus cachés
- Trouver des traces d'injection de code

Automatiser des opérations

- Concevoir des automates de détection sur les systèmes et la mémoire
- Comparer des scénarios d'intrusion

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de l'analyse inforensique.

Résilience et continuité d'activité

La résilience est devenu un objectif stratégique pour l'entreprise afin de lui permettre de survivre aux nombreuses crises nationales ou mondiales et de continuer son activité.

Afin d'atteindre cet objectif, il faut réaliser un travail de planification, en amont, afin de se préparer et de disposer de plans de secours. C'est l'objet du plan de continuité d'activité. L'analyse et la gestion des risques permet de mettre en place des mesures de sécurité. Une bonne organisation de gestion de crise permet de mieux comprendre la situation et d'élaborer des réponses adaptées. Elle permet la diminution de l'incertitude et une meilleure prise de décisions. Le maintien de l'agilité et une meilleure affectation des ressources en fonction des priorités définies sont les conséquences à un plan de continuité d'activité efficace.

Devenir Responsable du Plan de Continuité d'Activité

La nature, la fréquence et le coût des crises perturbent très fortement le fonctionnement de nombreuses organisations. Les conséquences peuvent être désastreuses allant jusqu'à la cessation définitive d'activité. Les retours d'expérience montrent que les organisations ayant entrepris une démarche visant à garantir la continuité de leur activité sont les plus résilientes.

Compétences visées

- Analyser et apprécier les risques
- Formuler des propositions de stratégie de continuité et de reprise
- Vérifier l'efficacité et l'efficience du Plan de Continuité de l'Activité (PCA)

Objectifs pédagogiques

- Identifier les points clés de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Lister les concepts, les démarches, les méthodes, les normes et les techniques pour gérer un SMCA
- Mettre en place une gestion d'équipe efficace dans la mise en œuvre d'un SMCA
- Améliorer l'analyse et la prise de décision dans la gestion de la Continuité de l'Activité (CA)

Public

Toute personne amenée à exercer la fonction de Responsable du Plan de Continuité d'Activité : RPCA, RSSI, DPO, ingénieurs sécurité, responsables sécurité, managers, chefs de projet

Prérequis

Une expérience dans l'analyse des risques des systèmes d'informations et dans le management des compétences est recommandée.

Programme

Introduction

- Identifier les points clés de la fonction RPCA
- Définir les interactions avec les autres fonctions de l'organisation

La continuité d'activité (CA)

- Définir les principes fondamentaux de la CA
- Identifier les référentiels et les bonnes pratiques
- Décrire les normes sur la CA

La sauvegarde de l'information

- Cartographier l'ensemble des données
- Mettre en place des plans de sauvegardes
- Vérifier la viabilité des restaurations

La gestion des risques

- Analyser et apprécier des risques en CA
- Concevoir son Bilan d'Impact sur l'Activité (BIA)

Le marché de la continuité d'activité

- Gérer les contrats avec les partenaires
- Choisir son prestataire externe

Le Plan de Continuité d'Activité

- Concevoir un PCA
- Identifier les composantes d'un PCA : les différents plans (PGC, PCOM, PRM, PCIT, PRN)

Vérifier la validité d'un PCA

- Mettre en place des tests de vérification
- Réaliser un audit du PCA

Gérer une crise

- Activer le PCA selon les besoins
- Définir une communication de crise
- Gérer la continuité d'activité
- Améliorer le PCA par retour d'expérience

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine du management de la Cybersécurité et de la Continuité d'Activité.

Après cette formation, vous pouvez suivre les formations ISO 22301 Lead Auditor et ISO 22301 Lead Implementer.

☑CPF formation certifiante ISO 22301 Lead Auditor

Durée
5 jours - 40 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage. Corrections d'exercices. Préparation à l'examen de certification.

Attention cette formation nécessite du travail personnel hors-session. (5 heures)

Validations des acquis
L'examen de certification a lieu le dernier jour du stage.
L'examen est disponible en français et en anglais.

Formateurs
Formateurs experts dans le domaine du management de la Cybersécurité, de la Continuité de l'Activité et de l'audit.

La Continuité de l'Activité (CA) est un objectif majeur des entreprises. Une stratégie de résilience permet à l'entreprise de préserver ses actifs en cas d'attaque majeure. La norme ISO 22301:2012 fournit un cadre pour mettre en œuvre un Système de Management de la Continuité de l'Activité (SMCA).

Compétences visées

- Identifier un Système de Management de la Continuité de l'Activité SMCA
- Réaliser un audit de certification ISO 22301
- Manager une équipe d'auditeurs de SMCA

Objectifs pédagogiques

- Identifier les points clés du fonctionnement d'un SMCA selon l'ISO 22301
- Analyser l'environnement interne et externe d'une organisation, et se mettre en condition d'audit du SMCA
- Appliquer les lignes directrices de l'ISO 19011 pour mettre en place un audit ISO 22301
- Mettre en œuvre un audit de certification ISO 22301 avec les spécifications de l'ISO 17021
- Identifier la gestion d'une équipe d'auditeurs de SMCA

Public

Auditeurs internes, consultants, chefs de projets SMCA, toute personne responsable de la gestion de la continuité d'activité, conseillers experts

Prérequis

Posséder des connaissances sur les concepts de continuité d'activité avec de l'expérience dans ce domaine.
Il est fortement recommandé de prendre connaissance de la norme ISO 22301 en amont de la formation.

Programme

Introduction

- Définir les principes fondamentaux de la CA
- Définir un système de management SMCA
- Lister les objectifs des normes ISO 22301, ISO 22313 et ISO 27031
- Présenter le processus de certification ISO 22301
- Identifier les clauses 4 à 10 de la norme ISO 22301

Planifier un audit ISO 22301

- Définir les concepts fondamentaux d'un audit
- Identifier les notions de preuve et de risque
- Préparer un audit de certification ISO 22301
- Définir l'audit documentaire d'un SMCA
- Conduire une réunion d'initialisation

Mettre en œuvre un audit ISO 22301

- Gérer la communication avec l'audité
- Lister les principes fondamentaux de l'audit
- Rédiger des plans de tests d'audit
- Ecrire des constats d'audit
- Rédiger des rapports de non-conformité
- Mener une réunion de clôture d'un audit

Mener un suivi d'audit ISO 22301

- Évaluer des plans d'action correctifs
- Gérer les audits de surveillance ISO 22301

Examen de certification ISO 22301 Lead Auditor

Organisme de formation enregistré sous le numéro 11755723675.
Cet enregistrement ne vaut pas agrément de l'état

Visitez notre site 4cysec.io pour les dates
contact@4cysec.io - 09 74 76 85 78

ISO 22301 Lead Implementer

formation certifiante ☑CPF

La norme ISO/CEI 22301:2012 permet de mettre en œuvre et de gérer un Système de Management de la Continuité de l'Activité (SMCA). Le SMCA est un dispositif organisationnel de gouvernance qui vous permet d'analyser votre situation et exposition aux risques, de vous aider à réaliser des Plans de Continuité de l'Activité (PCA) adaptés à vos objectifs de continuité et de mettre en place des processus de vérification et d'amélioration continue.

Compétences visées

- Mettre en œuvre un Système de Management de la Continuité de l'Activité SMCA
- Analyser les risques pour établir un plan de continuité de l'activité dans une organisation
- Manager une équipe à la mise en oeuvre d'un SMCA

Objectifs pédagogiques

- Identifier les points clés de la mise en oeuvre d'un SMCA conforme à la norme ISO 22301
- Lister les concepts, les démarches, les méthodes, les normes et les techniques pour gérer un SMCA
- Mettre en place une gestion d'équipe efficace dans la mise en oeuvre d'un SMCA
- Améliorer l'analyse et la prise de décision dans la gestion de la Continuité de l'Activité (CA)

Public

Chefs de projet SMCA, responsables de la gestion de la continuité de l'activité, conseillers experts, consultants, auditeurs ISO 22301

Prérequis

Posséder des connaissances sur les concepts de continuité d'activité avec de l'expérience dans ce domaine.
Il est fortement recommandé de prendre connaissance de la norme ISO 22301 en amont de la formation.

Programme

Introduction

- Définir un système de management
- Lister les objectifs des normes ISO 22301, ISO 22313 et ISO 27031
- Définir les principes fondamentaux de la CA
- Initialiser la mise en œuvre du SMCA
- Lister les objectifs de sécurité de l'information
- Analyser un système de management existant
- Définir le domaine d'application du SMCA

Planifier la mise en œuvre d'un SMCA

- Initier la mise en place d'un SMCA
- Intégrer la politique de continuité de l'activité
- Structure organisationnelle de la CA
- Documenter l'information
- Gérer les compétences et la sensibilisation
- Analyser les impacts et apprécier les risques

Mettre en place un SMCA basé sur l'ISO 22301

- Définir sa stratégie de continuité d'activité
- Identifier les mesures de protection et d'atténuation
- Concevoir des PCA et rédiger des procédures
- Analyser des exemples de PCA

Contrôler et améliorer un SMCA

- Mettre en place des mesures de surveillance du SMCA et l'évaluer
- Mettre en place de l'amélioration continue

Certifier un SMCA par la norme ISO 22301

- Réaliser un audit interne ISO 22301
- Produire une revue de direction du SMCA
- Traiter les problèmes et les non-conformités
- Se préparer à l'audit de certification ISO 22301

Examen de certification ISO 22301 Lead Implementer

Durée
5 jours - 40 heures

Prix inter
3500 €HT

Prochaines dates
Visitez notre site 4cysec.io

Examen de certification
inclus

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis pendant le stage. Corrections d'exercices. Préparation à l'examen de certification.

Attention cette formation nécessite du travail personnel hors-session. (5 heures)

Validations des acquis
L'examen de certification a lieu le dernier jour du stage. L'examen est disponible en français et en anglais.

Formateurs
Formateurs experts dans le domaine de la Continuité de l'Activité.

NOTRE DÉMARCHE QUALITÉ

Nos formations intra-entreprise

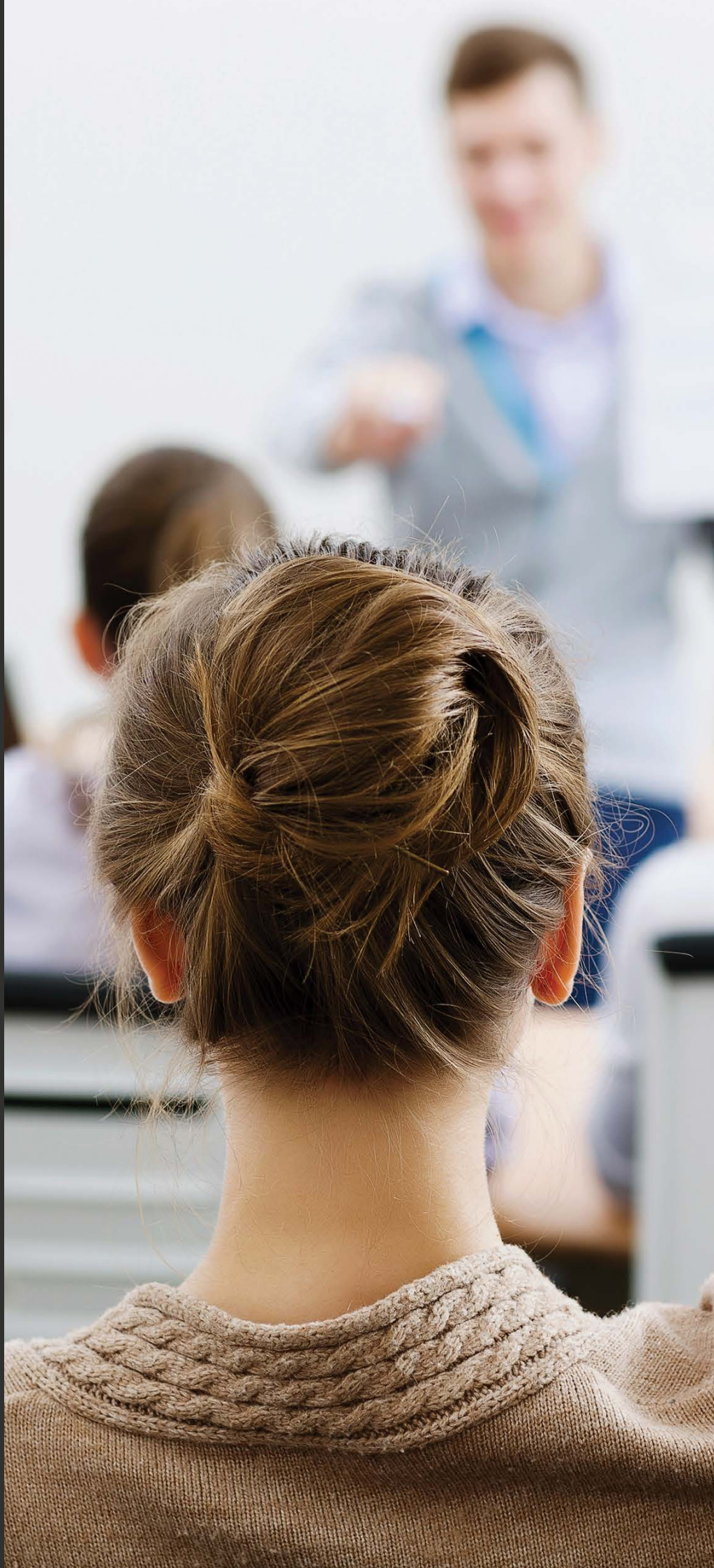
- Nous vous apportons une réponse spécifique à votre besoin au sein de votre entreprise
- Nous appliquons une approche compétence avec un contenu personnalisé et adapté à votre entreprise
- Nous vous proposons un budget optimisé
- Nous réalisons la formation dans vos locaux ou dans nos sites à Paris et en région (Lyon, Marseille, Toulouse, Nantes et Lille)
- Nous convenons avec vous d'une planification adaptée à vos contraintes

Nos formations inter-entreprises

- Nous vous apportons une réponse à un besoin individuel
- Nous visons des compétences métier avec un contenu adapté
- Nous vous proposons une ingénierie pédagogique qualitative
- Nous concevons des supports de formation adaptés
- Nous réalisons la formation dans nos sites à Paris

Trouvez la formation la mieux adaptée à vos besoins opérationnels et à vos objectifs de compétences

Test utilisateur, questionnaire à choix multiples, entretien téléphonique etc., notre protocole d'audit permet de réaliser une analyse pointue de vos prérequis et de vos objectifs. Nous vous proposons le parcours de formation le plus adapté à vos besoins.



CGV
NOS CONDITIONS GÉNÉRALES DE VENTE

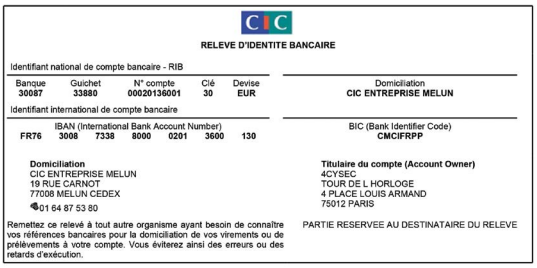
Article 1 - OBJET ET CHAMP D'APPLICATION
Toute commande de formation implique l'acceptation sans réserve par l'acheteur et son adhésion pleine et entière aux présentes conditions générales de vente qui prévalent sur tout autre document de l'acheteur, et notamment sur toutes conditions générales d'achat.

Article 2 - DOCUMENTS CONTRACTUELS
4CYSEC fait parvenir au client une convention de formation professionnelle continue telle que prévue par la loi. Le client s'engage à retourner dans les plus brefs délais à 4CYSEC un exemplaire signé et portant son cachet commercial.
Les attestations de présences peuvent être adressées au client après la formation sur simple demande.

Article 3 - PRÉREQUIS
Des prérequis peuvent être indiqués dans le programme de formation. Le client s'engage à les respecter dans la mesure notamment où cela est susceptible d'affecter la qualité de la formation dispensée.

Article 4 - PRIX, FACTURATION ET RÈGLEMENTS
Nos prix sont établis hors taxes. Ils sont à majorer de la TVA au taux en vigueur. Les repas sont compris dans le prix du stage. Les frais annexes à la formation (les frais de déplacement, de séjour, de coursier,...) sont en sus.
La facture est adressée au client après exécution de la prestation.
En cas de paiement effectué par un Organisme Paritaire Collecteur Agréé (OPCA), il appartient au client de faire la demande de prise en charge avant le début de la formation auprès de l'OPCA dont il dépend. L'accord de financement doit être communiqué au moment de l'inscription.
En cas de prise en charge partielle par l'OPCA, la différence sera directement facturée au client. Si l'accord de prise en charge de l'OPCA ne nous parvient pas au premier jour de la formation, la totalité des frais de formation peut éventuellement être facturée au client. En cas de non-règlement par l'OPCA du client, quelle qu'en soit la cause, la facture devient exigible auprès du client.
Tout stage commencé est considéré comme dû dans son intégralité.

Article 5 - RÈGLEMENT
Le règlement des factures peut s'effectuer :
- par chèque
- par virement bancaire :



CIC

RELEVE D'IDENTITE BANCAIRE

Identifiant national de compte bancaire - RIB

Banque	Guichet	N° compte	Clé	Devise
30087	33880	00020136001	30	EUR

Domiciliation
CIC ENTREPRISE MELUN

Identifiant international de compte bancaire

IBAN (International Bank Account Number)
FR76 3008 7338 8000 0201 3600 130

BIC (Bank Identifier Code)
CMCIFRPP

Domiciliation
CIC ENTREPRISE MELUN
19 RUE CARNOT
77008 MELUN CEDEX
01 64 87 53 80

Titulaire du compte (Account Owner)
4CYSEC
TOUR DE L HORLOGE
4 PLACE LOUIS ARMAND
75012 PARIS

Remettez ce relevé à tout autre organisme ayant besoin de connaître vos références bancaires pour la domiciliation de vos virements ou de prélèvements à votre compte. Vous éviterez ainsi des erreurs ou des retards d'exécution.

PARTIE RESERVEE AU DESTINATAIRE DU RELEVE

Les factures sont payables à 30 jours, net et sans escompte sauf autre échéance indiquée sur la facture. Tout retard de paiement par rapport à cette échéance entraînera de plein droit :
- des frais financiers de 1,5 % par mois au prorata temporis,
- l'application d'une clause pénale égale à 20 % du prix de vente hors taxes,
- l'exigibilité immédiate des factures non échues.

4CYSEC se réserve le droit de suspendre ou d'annuler les prestations en cours, sans pouvoir donner lieu à dommages et intérêts pour le Client. Tous droits et taxes applicables sont facturés en sus, conformément aux lois et règlements en vigueur.

Article 6 - CONVOCATIONS
4CYSEC ne peut être tenue responsable de la non-réception de la convocation quel qu'en soient le ou les destinataires chez le client, notamment en cas d'absence du ou des stagiaires à la formation. Dans le doute, il appartient au client de s'assurer de l'inscription de ses stagiaires et de leur présence à la formation.

Article 7 - ANNULATION, ABSENCE, REPORT D'INSCRIPTION PAR LE CLIENT
Tout stage commencé est dû en totalité, de même si le participant ne s'est pas présenté.
Les remplacements de stagiaires sont admis à tout moment, sans frais, en communiquant par écrit le nom et les coordonnées du remplaçant sous réserve de remplir les conditions d'acceptation à la formation.
Toute annulation d'inscription doit être signalée par téléphone et confirmée par écrit.
- Une annulation intervenant plus de deux semaines avant le début du stage ne donnera lieu à aucune facturation.
- Une annulation intervenant entre une et deux semaines avant le début du stage donnera lieu à la facturation au client de 50 % du coût de la totalité du stage.
- Une annulation intervenant moins d'une semaine avant le début du stage donnera lieu à la facturation de la totalité du coût du stage.
- Un report intervenant moins de deux semaines avant le début du stage est considéré comme une annulation.

Cependant, si simultanément à son annulation, le participant se réinscrit à une formation, aucune indemnité forfaitaire ne sera retenue, à moins qu'il annule cette nouvelle participation et ce, quelle que soit la date d'annulation. Ce dédit ne peut en aucun cas être imputé sur le montant de la participation au développement de la formation professionnelle.

Article 8 - ANNULATION D'UN STAGE PAR 4CYSEC
4CYSEC se réserve la possibilité d'annuler une formation en cas de force majeure. Sont considérés comme tels, outres les cas habituels de force majeure ou de cas fortuit, sans que cette liste soit exhaustive : la grève des transports, la maladie de l'intervenant, l'interruption des télécommunications. (...) 4CYSEC organisera alors une nouvelle session dans les meilleurs délais et aucun dédommagement ne pourra être demandé. En cas d'impossibilité du client de participer à la session à la date ultérieurement proposée, 4CYSEC, proposera une formation équivalente. En cas de session inter-entreprises notamment, 4CYSEC se réserve le droit d'annuler une formation si le nombre de 3 stagiaires n'est pas atteint ou en cas de problème technique ou logistique et ce sans aucun dédommagement. Dans ce cas, les stagiaires seront prévenus au moins une semaine avant le début du stage. De nouvelles dates leur seront proposés. Le nombre de participants maximum est indiqué sur les programmes de formation.

Article 9 – RÈGLEMENT INTÉRIEUR
Le participant s'engage à respecter les conditions du règlement intérieur affiché sur les lieux de formation, dont il déclare avoir pris connaissance et accepter les termes.

Article 10 - INFORMATIQUE ET LIBERTÉ et RGPD
Les données à caractère personnel du client sont traitées conformément à la Loi du 14 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et à la réglementation européenne relative à la protection des données à caractère personnel ainsi que dans les conditions prévues par notre Politique de confidentialité des données à caractère personnel. (document PDF téléchargeable sur notre site web 4cysec.io)

Article 11 - CITATION ET RÉFÉRENCES CLIENT
Le client autorise expressément, sauf avis contraire, 4CYSEC à citer son nom (enseigne commerciale et/ou raison sociale pour les professionnels) comme référence client de 4CYSEC.

Article 12 - LOI APPLICABLE
Les CGV et tous les rapports entre 4CYSEC et ses clients relèvent de la Loi française.

Article 13 - ATTRIBUTION DE COMPÉTENCES
Tous litiges qui ne pourraient être réglés à l'amiable seront de la COMPÉTENCE EXCLUSIVE DU TRIBUNAL DE COMMERCE DE PARIS quel que soit le siège ou la résidence du client, nonobstant pluralité de défendeurs ou appel en garantie. Cette clause attributive de compétence ne s'appliquera pas au cas de litige avec un Client non professionnel pour lequel les règles légales de compétence matérielle et géographique s'appliqueront. La présente clause est stipulée dans l'intérêt de la société 4CYSEC qui se réserve le droit d'y renoncer si bon lui semble.

Article 14 - ÉLECTION DE DOMICILE
L'élection de domicile est faite par 4CYSEC à son siège social à Tour de l'horloge 4 place Louis Armand 75012 Paris.

4CYSEC

CYBER SECURITY EXPERT

4cysec.io

Tour de l'horloge
4 place Louis Armand
75012 Paris

Tél: 09 74 76 85 78

Email: contact@4cysec.io