Deloitte.

CyberAcademy

Catalogue Cyber Academy 2023
Formations & Sensibilisation

Sécurité technique, juridique, organisationnelle et continuité d'activité

MAKING AN IMPACT THAT MATTERS since 1845

La qualité au cœur de nos offres

Formation et sensibilisation : combinaison incontournable de la sécurité de votre entreprise

01

Un contenu de qualité

Des supports et prestations en évolution permanente pour répondre aux exigences de nos clients.

02

Une expertise reconnue

Un centre de formation et des cours certifiés par les plus grands acteurs du marché.

03

Des formateurs qualifiés

Des experts cyber certifiés sur les sujets dispensés, partageant leur expertise et leurs retours d'expérience.

04

Une offre à 360°

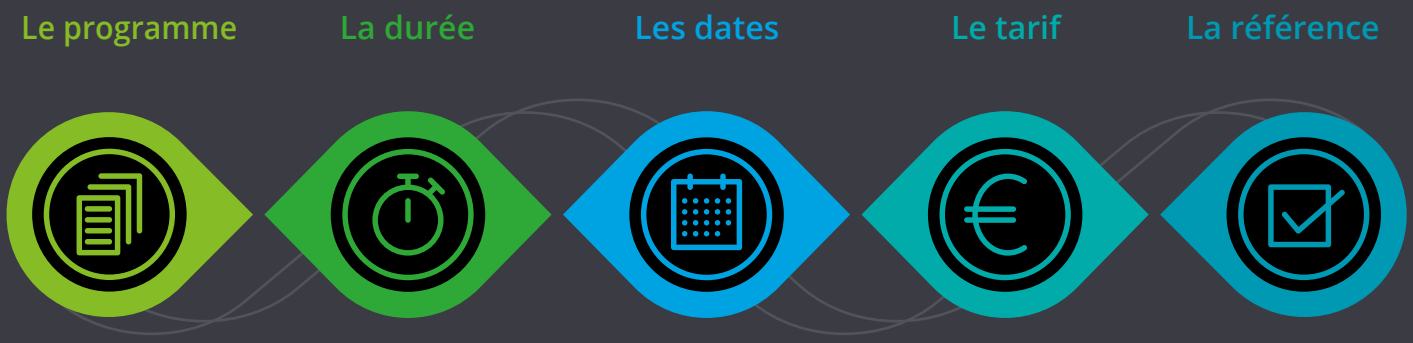
Une sélection de formations sur étagère complétée par une offre de sensibilisation sur-mesure.

Le centre de formation Deloitte Cyber Academy

Deloitte Cyber Academy propose et conçoit un ensemble de formations et de plans de sensibilisation à la pointe de l'état de l'art dans le domaine de la cybersécurité.

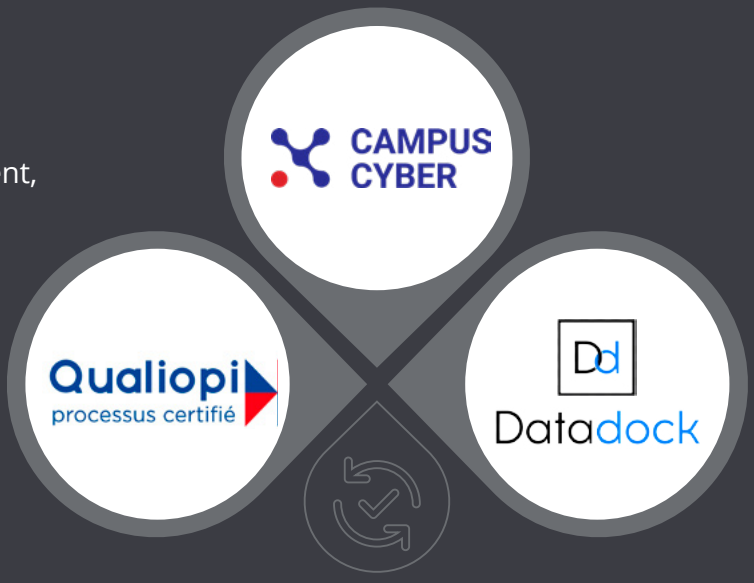
Vous trouverez au sein de ce catalogue l'ensemble de notre offre pour l'année 2023 avec :
- des formations de sécurité organisationnelle, juridique et technique ;
- des plans de sensibilisation adaptables au contexte de votre entreprise.

Ainsi pour chaque prestation, ce catalogue vous fournira les informations suivantes :

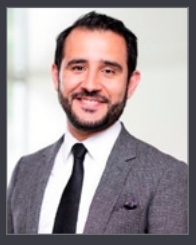


Un centre de formation reconnu pour son professionnalisme et sa qualité d'enseignement, certifié par le label de qualité Qualiopi depuis 2022.

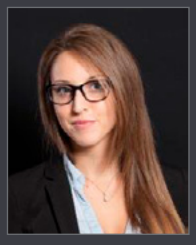
En accord avec sa vision et ses ambitions, la Cyber Academy a intégré le Campus Cyber depuis septembre 2022. L'ensemble de ses formations y est dispensé.



L'équipe Deloitte Cyber Academy se tient à votre disposition pour élaborer votre projet.



Imade Elbaraka
Associé Cyber Risk
ielbaraka@deloitte.fr
+33 (0)1 55 61 74 64



Emilie Bozzolo
Responsable Formation
ebozzolo@deloitte.fr
+33 (0)1 40 88 71 46

Toutes nos formations sont accessibles aux personnes en situation de handicap.

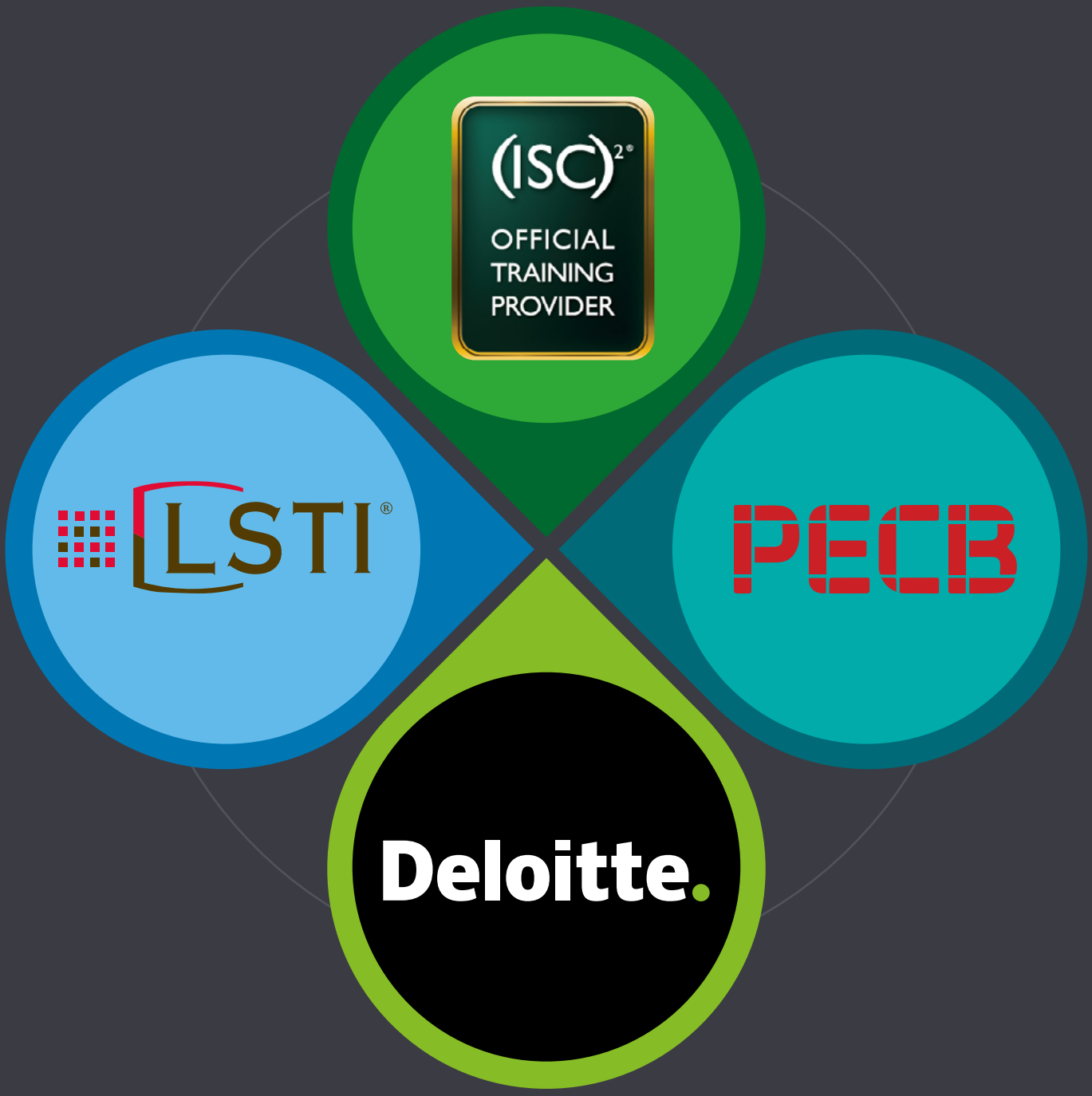
Sommaire

Vous avez identifié des **besoins** en **cybersécurité** ?

Nos **experts** vous accompagnent pour **adapter** ce catalogue et répondre à vos enjeux de **formation**.

Organismes de certification

Grâce au soutien de quatre organismes renommés, Deloitte Cyber Academy propose aux stagiaires de présenter les certifications les plus reconnues dans le monde :



Certified in Cybersecurity (ISC)²

New

La certification Certified in Cybersecurity prouvera aux employeurs que les candidats possèdent les connaissances, les compétences et les aptitudes fondamentales nécessaires pour occuper un poste en cybersécurité de niveau junior. Elle témoignera de leur compréhension des bonnes pratiques, politiques et procédures fondamentales en matière de sécurité, ainsi que de leur volonté et leur capacité d'en apprendre d'avantage et de se perfectionner dans ce domaine. Cette certification permet aux candidats de prendre confiance et d'accéder à leur premier poste en cybersécurité tout en disposant d'un bagage initial de connaissances.

Vous allez apprendre à

- Comprendre les concepts de sécurité et de protection de l'information, le processus de gestion des risques, les contrôles de sécurité, le code d'éthique (ISC)² et les processus de gouvernance.
- Comprendre la continuité des activités, la reprise après incident et la réponse aux incidents.
- Comprendre les contrôles d'accès physiques.
- Comprendre les réseaux informatiques, les menaces et les attaques de réseaux, ainsi que l'infrastructure de sécurité des réseaux.
- Comprendre la sécurité des données, le renforcement des systèmes, les politiques de sécurité.
- Comprendre les bonnes pratiques, ainsi que l'importance de la formation et de la sensibilisation.

Public visé

- Upskillers : Étudiants et jeunes diplômés
- Reskillers : Professionnels de l'informatique ou non, souhaitant se reconvertir dans le domaine de la cybersécurité.

Pré-requis

Aucun prérequis n'est nécessaire. Il est cependant recommandé aux candidats d'avoir des connaissances de base en technologie de l'information (TI). Aucune expérience professionnelle dans le domaine de la cybersécurité ni aucun diplôme ou grade officiel ne sont requis.

Certification

Cette formation prépare à l'examen de certification « Certified in Cybersecurity »
Trouver votre centre d'examen Pearson VUE pour vous inscrire à l'examen en suivant le lien : www.pearsonvue.com/isc2.

Méthode pédagogique

- Dispense en français
- Cours théorique
- QCM d'entrainement pour chaque chapitre

Matériel

- Supports de cours en anglais

Programme

Le programme traite de cinq domaines de sécurité :

Domaine 1 : Security Principles
- Concepts de sécurité et protection de l'information
- Concepts de gestion des risques
- Contrôles de sécurité
- Processus de gouvernance
- Code éthique (ISC)²

Domaine 2 : Incident Response, Business Continuity (BC), and Disaster Recovery (DR)
- Réponse aux incidents
- Continuité des opérations (BC)
- Reprise après sinistre (DR)

Domaine 3 : Access Controls Concepts
- Concepts de contrôles d'accès
- Contrôles d'accès physiques
- Logique des contrôles d'accès

Domaine 4 : Network Security
- Réseau informatique
- Menaces et attaques de réseau
- Infrastructure de sécurité des réseaux

Domaine 5 : Security Operations
- Sécurité des données
- Renforcement du système
- Les bonnes pratiques en matière de politiques de sécurité
- Formation à la sécurité

Résumé du cours et détails de l'examen
- Exigences en matière d'expérience professionnelle
- Programmation de l'examen
- Avant l'examen
- Après l'examen
- Conseils pour l'examen
- Explication des attentes de l'examen

2 jours / 14 heures

Réf. : CC1

2 000€ hors taxes

- 16 au 17 janvier
- 3 au 4 juillet
- 11 au 12 septembre

CISSP (ISC)²

CISSP (Certified Information Systems Security Professional) est la certification professionnelle internationale la plus connue dans le monde de la sécurité des systèmes d'information. Le programme de certification géré par ISC² (International Information Systems Security Certification Consortium) est réparti en 8 thèmes couvrant tous les aspects de la sécurité des systèmes d'information.

Vous allez apprendre à

- Connaître le Common Body of Knowledge de la sécurité IT
- Développer une vision globale des enjeux de sécurité IT
- Approfondir les connaissances des huit domaines du CISSP
- Se préparer à l'examen de certification du CISSP

Public visé

- Toute personne souhaitant obtenir une certification reconnue en sécurité
- Consultants en sécurité devant démontrer leur expertise acquise et enrichir leur CV
- Juristes

Pré-requis*

- Avoir lu le CBK (Common Body of Knowledge), livre officiel de l'ISC²
- Disposer de 5 ans d'expérience dans au moins 2 des 8 domaines traités par la formation CISSP. Un CV vous sera demandé afin de valider ce prérequis.

Méthode pédagogique

- Des questions et des explications à chaque réponse inexacte
- Formation dispensée en français

Matériel

- Support officiel de l'(ISC)² en anglais
- Livre CBK officiel de l'ISC² envoyé sur demande uniquement à réception des documents de confirmation d'inscription
- Un livre de révision de l'ISC² pour l'ensemble des chapitres comprenant :
  - Des fiches de révision et résumés des chapitres
  - Des questions d'entraînement
  - Un examen blanc

Certification

- Cette formation prépare à l'examen de certification CISSP de l'ISC². Partenaire officiel d'ISC² en France, Deloitte Cyber Academy est un des rares organismes de formation à être habilité à vendre l'examen CISSP. L'examen se déroule dans un centre Pearsonvue en suivant le lien : www.pearsonvue.com.

Programme

Les 8 thèmes officiels du CBK :

- Security & Risk Management
- Asset Security
- Security Engineering
- Communications & Network Security
- Identity & Access Management
- Security Assessment & Testing
- Security Operations
- Security in the Software Development Life Cycle

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures

Réf. : CISSP

4 100€ hors taxes dont 650€ hors taxes de coupon d'examen

- 6 au 10 mars
- 22 au 26 mai
- 26 au 30 juin
- 18 au 22 sept.
- 13 au 15 nov.
- 11 au 15 déc.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

CCSP (ISC)²

Le cloud computing bouscule les organisations, d'une part par son approche technique, d'autre part par la démarche organisationnelle qu'il implique. Ainsi, le Cloud permet à de nombreuses organisations de développer leurs activités en termes d'efficacité, de rentabilité et de croissance, tout en contribuant à réduire les coûts de production et le time to market. Cependant, suite au succès du Cloud, il est indispensable de comprendre et d'étudier ses implications en termes de sécurité, pour réussir sa mise en œuvre et la rentabilité de la démarche sur le long terme d'une entreprise. Pour cela, les entreprises doivent s'appuyer sur des professionnels expérimentés et compétents, dotés de connaissances et compétences solides en matière de sécurité du Cloud. La certification CCSP (Cloud Computing Security Professional) apporte une réponse, en attestant de connaissances et de compétences approfondies dans tout l'éco système Cloud (organisationnel, technique, juridique). Cette certification est soutenue par la Cloud Security Alliance (CSA) et l'(ISC)².

Vous allez apprendre à

- Connaître le Common Body of Knowledge de la sécurité du Cloud
- Développer une vision globale des enjeux de sécurité Cloud
- Approfondir les connaissances des six domaines du CCSP
- Se préparer à l'examen de certification du CCSP

Public visé

- Architecte d'entreprise ; RSSI, officier de sécurité ; administrateur sécurité ; architecte sécurité ; consultant en sécurité ; ingénieur sécurité ; chef de projet et manager sécurité; architecte système, ingénieur système

Pré-requis*

Avoir lu le CBK (Common Body of Knowledge), livre officiel de l'ISC²

Matériel

- Support officiel de l'(ISC)² en anglais
- Livre CBK officiel de l'ISC² envoyé sur demande uniquement à réception des documents de confirmation d'inscription
- Un livre de révision de l'ISC² pour l'ensemble des chapitres comprenant : des fiches de révision et résumés des chapitres ; des questions d'entraînement et un examen blanc

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Certification

- Pour être titulaire de la certification CCSP, les candidats doivent d'une part réussir l'examen CCSP, d'autre part, disposer de cinq années d'expérience professionnelle en technologies de l'information, dont trois ans en sécurité de l'information, ainsi qu'au moins une année dans un ou plus des six domaines du CCSP Common Body of Knowledge (CBK®) de (ISC)².

Les six domaines couverts par le CCSP

Domaine 1 - Exigences et concepts en termes de conception en architecture Cloud computing

- Les concept du Cloud computing
- Les architectures de référence du Cloud computing
- Les concepts de sécurité associés au cloud computing
- Les principes de conception de sécurité du Cloud de Computing
- L'identification des services de cloud computing de confiance

Domaine 2 - La sécurité des données dans le cloud computing

- Le cycle de vie des données du cloud computing
- Conception et déploiement des architectures de stockage en cloud computing
- Conception et application des stratégies de sécurité des données
- Connaissances et déploiement des technologies de classification et de découverte des données
- Conception et mise en œuvre des exigences légales de sécurité des données concernant l'identification des informations personnelles (PII)
- Conception et déploiement du Data Rights Management
- Planification et mise en œuvre des politiques de rétention, de suppression et d'archivage des données
- Conception et déploiement des démarches d'audit, de détection et de démontrabilité

Domaine 3 - La sécurité des infrastructures et des plateformes de cloud computing

- Les composants de l'infrastructure du cloud computing
- Evaluation des risques de l'infrastructure du cloud computing
- Conception et planification des contrôles de sécurité
- Conception et déploiement de plan de reprise et de continuité des services et des métiers

Domaine 4 - La sécurité des applications de cloud computing

- Formation et sensibilisation de la sécurité autour des services du Cloud computing
- Validation et assurance des solutions logicielles du Cloud computing
- Utilisation des logiciels vérifiés, approbation des API
- SDLS : cycle de vie du développement de la sécurité logicielle
- Les architectures applicatives du Cloud computing
- Conception et déploiement d'une solution d'IAM (Identity & Access Management)

Domaine 5 - Gestion des opérations

- Planification des processus de conception du data Center
- Développement et mise en œuvre d'une infrastructure physique du Cloud
- Gestion opérationnelle et maintenance d'une infrastructure physique de Cloud computing
- Conception, maintenance et gestion d'une infrastructure logique de Cloud computing
- Conformité avec les normes de type ISO 20000-1 ou des référentiels comme ITIL
- Evaluation des risques d'une infrastructure logique et physique du Cloud Computing
- Collecte et conservation des preuves numériques (forensic)
- Communication avec les parties prenantes

Domaine 6 - Les exigences légales et la conformité

- Risques et exigences légales d'un environnement de Cloud Computing
- La gestion de la vie privée, diversité des exigences légales en fonction des pays
- Méthodes et processus d'audit d'un environnement de cloud computing
- La gestion des risques au niveau de l'entreprise d'un écosystème cloud computing
- Conception et gestion des contrats, notamment dans le cadre d'une démarche d'externalisation
- Gestion des fournisseurs du Cloud Computing

5 jours / 35 heures	Réf. : CCSP	4 100€ hors taxes dont 650€ hors taxes de coupon d'examen	• 3 au 7 avril	• 20 au 24 novembre

RSSI

La formation RSSI Deloitte Cyber Academy apporte au nouveau responsable sécurité des SI ou au nouveau manager d'un RSSI un panorama complet de ses fonctions et des attentes des organisations sur son rôle. Les connaissances indispensables à la prise de fonction du RSSI, un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par des consultants expérimentés et d'anciens RSSI.

Vous allez apprendre à

- Les bases pour la mise en place d'une bonne gouvernance de la sécurité des systèmes d'information
- Les connaissances techniques de base indispensables à la fonction de RSSI
- Pourquoi et comment mettre en œuvre un SMSI en s'appuyant sur la norme ISO 27001
- L'état du marché de la sécurité informatique
- Les méthodes d'appréciation des risques
- Les enjeux de la SSI au sein des organisations
- Les stratégies de prise de fonction et des retours d'expérience de RSSI
- Identifier et évaluer les principaux risques juridiques pesant sur un système d'information
- Réduire concrètement les non-conformités juridiques affectant un système d'information

Public visé

- Nouveaux ou futurs RSSI souhaitant se mettre à niveau et échanger
- RSSI expérimentés souhaitant se remettre à niveau et échanger sur les bonnes pratiques du métier avec d'autres RSSI
- Ingénieurs en sécurité des systèmes d'information souhaitant rapidement acquérir toutes les compétences leur permettant d'évoluer vers la fonction de RSSI
- Directeurs des systèmes d'information ou auditeurs en systèmes d'information souhaitant connaître les contours de la fonction et les rôles du RSSI

Pré-requis*

- Expérience au sein d'une direction informatique en tant qu'informaticien ou bonne connaissance générale des systèmes d'information
- Des notions de base en sécurité appliquée aux systèmes d'information constituent un plus

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Méthode pédagogique

- Cours magistral dispensé par des consultants et des experts de chaque domaine: organisationnel, technique, commercial et juridique
- Formation dispensée en français

Matériel

- Support de cours en français

Certification

- Cette formation n'est pas certifiante
- Cette formation donne lieu à une évaluation des connaissances et le cas échéant un certificat de réussite.

Programme

Introduction

- Accueil
- Présentation de la fonction de RSSI avec mise en perspective par rapport à tous les aspects de son environnement
- Production, direction, métiers, conformité, juridique, etc.

Aspects organisationnels de la sécurité

- Panorama des référentiels du marché
- Politiques de sécurité
- Rédaction
- Politiques globales, sectorielles, géographiques
- Conformité
- Gouvernance de la sécurité
- Indicateurs sécurité
- Gestion des incidents
- Aspects techniques de la sécurité
- Sécurité du système d'exploitation
- Sécurité des applications (sessions, injections SQL, XSS)
- Sécurité réseau (routeurs, firewalls)
- Sécurité du poste de travail

Systèmes de management de la sécurité de l'information (norme ISO 27001)

- Bases sur les SMSI
- Panorama des normes de type ISO 27000
- Bases sur ISO 27001 et ISO 27002

Préparation à l'audit

- Formation et communication
- Audit à blanc
- Documents à préparer
- Considérations pratiques
- Réception des auditeurs (SoX, Cour des comptes, Commission bancaire, etc.)

Gestion des risques

- Méthodologies d'appréciation des risques :
  - EBIOS
  - MEHARI
  - ISO 27005
- Analyse des risques
- Evaluation des risques
- Traitement des risques
- Acceptation des risques

Aspects juridiques de la SSI

- Informatique et libertés
- Communications électroniques
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Charte informatique
- Administrateurs

Acteurs du marché de la sécurité

- Gestion des relations avec les partenaires
- Infogérance
- Prestataires en sécurité

Stratégies de prise de fonction du RSSI

- Rôles du RSSI
- Relations avec les métiers, la DSI, la DG, les opérationnels
- Retour d'expérience
- Questions / Réponses avec les stagiaires

Intervention d'un RSSI selon disponiblité

5 jours / 35 heures

Réf. : RSSI

3 500€ hors taxes

- 27 au 31 mars
- 12 au 16 juin
- 2 au 6 octobre
- 27 nov. au 1er déc.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Préparation à l'examen CISA

Préparation à l'examen

Le CISA (Certified Information Systems Auditor) est la certification internationale des auditeurs des systèmes d'information. Cette certification est régulièrement exigée auprès des auditeurs informatiques et sécurité. Elle est éditée par l'Association internationale des auditeurs informatique ISACA (*www.isaca.org/*).

Objectif

- Préparer à la réussite de l'examen CISA de l'ISACA

Public visé

- Consultants en organisation, consultants en systèmes d'information, consultants en sécurité
- Auditeurs
- Informaticiens
- Responsables informatique
- Chefs de projets, urbanistes, managers

Pré-requis*

- Connaissance générale de l'informatique, de ses modes d'organisation et de son fonctionnement
- Connaissance des principes généraux des processus SI et des principes de base de la technologie des SI et des réseaux
- Au moins 5 ans d'expérience dans les domaines de l'audit, le contrôle, l'assurance ou la sécurité des IS/IT

Méthode pédagogique

- Cours magistraux
- Exercices pratiques par des questions à l'issue de chaque exposé
- Examen blanc de 100 questions et explications à chaque réponse inexacte
- Formation dispensée en français

Matériel

Supports de cours en français

Certification

Cette formation prépare à l'examen de certification CISA de l'ISACA. Coupon d'examen disponible uniquement sur le site de l'ISACA.

Programme

Le stage est organisé sur 4 journées de révision des 5 thématiques de la certification CISA associées à des séries de questions illustratives.

Les 5 domaines abordés (repris dans le CRM et le support de cours) :

- Le processus d'audit des SI : méthodologie d'audit, normes, référentiels, la réalisation de l'audit, les techniques d'autoévaluation
- La gouvernance et la gestion des SI : pratique de stratégie et de gouvernance SI, politiques et procédures, pratique de la gestion des SI, organisation et comitologie, gestion de la continuité des opérations
- L'acquisition, la conception et l'implantation des SI : la gestion de projet, l'audit des études et du développement, les pratiques de maintenance, contrôles applicatifs
- L'exploitation, l'entretien et le soutien des SI : l'audit de la fonction information et des opérations, l'audit des infrastructures et des réseaux
- La protection des actifs informationnels : audit de sécurité, gestion des accès, sécurité des réseaux, audit de management de la sécurité, sécurité physique, sécurité organisationnelle.
- La dernière journée du stage est consacrée à un exposé de pratiques destiné à la préparation de l'examen (QCM de 4h), suivi d'un examen blanc de 100 questions (2h) et d'une revue des réponses des stagiaires.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures	Réf. : CISA	3 500€ hors taxes	• 17 au 21 avril	• 20 au 24 novembre

Préparation à l'examen de certification Certified Information Security Manager (CISM)

Ce cours permet de préparer l'examen CISM® (Certified Information Security Manager) en couvrant la totalité du cursus CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défini par l'ISACA®.
La formation aborde de manière claire des notions avancées de gestion du risque ainsi que les mises en conformités spécifiques et la gestion de la sécurité grâce à un support développé par nos experts, incluant des diagrammes ainsi que des questionnaires pour s'entrainer.

Vous allez apprendre à

- Maîtriser les concepts des quatre grands domaines sur lesquels porte la certification CISM.
- Assimiler le vocabulaire et les idées directrices de la certification CISM.
- Acquérir les connaissances de bases sur les standards internationaux dans le domaine de la gestion de la sécurité des systèmes d'information.
- Comprendre les pratiques de gestion des risques pour gérer le programme de sécurité de l'information d'une organisation.
- Préparer l'examen de certification CISM, Responsable Sécurité certifié ISACA.

Public visé

Cette formation s'adresse aux professionnels expérimentés dans la gestion de la sécurité et ceux qui sont responsables de la sécurité et de la confidentialité des informations incluant : les consultants IT, les auditeurs, les managers, les rédacteurs en charge des règles de sécurité, les administrateurs et ingénieurs réseau/sécurité.

Prérequis *

- Connaissances de base du fonctionnement des Systèmes d'Information
- Bonne compréhension de l'anglais

Méthode pédagogique

- 5 jours de revue du contenu théorique – en français
- Examens blancs avec corrigé détaillé – en anglais
- Support de cours en anglais

Matériel

- Support de cours extrait du livre officiel en anglais
- Livre officiel en anglais

Certifications

Cette formation n'est pas certifiante. Elle donne lieu à une évaluation des connaissances et, le cas échant, à un certificat de réussite.

Pour la certification officielle :

- Inscription à faire sur le site www.isaca.org, la clôture des inscriptions est faite 2 mois avant la date de l'examen.
- Déroulement de l'examen : 4 heures de QCM avec 200 questions (examen disponible uniquement en anglais).
- Trois années ou plus d'expérience en sécurité de l'information et en contrôle des SI sont nécessaires pour prétendre à la certification. Aucune dispense ou substitution d'expérience n'est possible.

Programme

DOMAINE 1 - Gouvernance de la sécurité de l'information - 17%
- Chapitre 1 : Gouvernance d'entreprise
- Chapitre 2 : Stratégie de sécurité de l'information

DOMAINE 2 - Gestion des risques de l'information et conformité - 20%
- Chapitre 3 : Evaluation des risques de sécurité de l'information
- Chapitre 4 : Réponse aux risques de sécurité de l'information

DOMAINE 3 - Implémentation, gestion de programme sécurité de l'information - 33%
- Chapitre 5 : Développement d'un programme de sécurité de l'information
- Chapitre 6 : Management d'un programme de sécurité de l'information

DOMAINE 4 - Gestion des incidents de sécurité de l'information - 30 %
- Chapitre 7 : Préparation à la gestion des incidents
- Chapitre 8 : Opérations de gestion des incidents

Travaux pratiques pour chaque module : questions issues des précédentes sessions du CISM (ou d'examens comparables).

Examen blanc et procédure de certification

Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

3 jours / 21 heures

Réf. : CISM

3 500€ hors taxes

- 6 au 8 février
- 3 au 5 juillet
- 4 au 6 septembre
- 6 au 8 novembre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Préparation à l'examen de certification Certified in Risk and Information Systems Control (CRISC)

CRISC vise à préparer les professionnels de l'informatique à relever les défis que présente la gestion des risques informatiques. Elle leur permet d'être capable d'aider les entreprises à atteindre leurs objectifs commerciaux en concevant, en mettant en œuvre, en surveillant et en maintenant des contrôles des SI basés sur les risques, efficients et efficaces. La formation CRISC fera donc des participant des acteurs stratégiques et essentiels au sein d'une organisation.

Vous allez apprendre à

- Identifier une stratégie de gestion des risques informatiques alignés avec la stratégie globale de l'entreprise.
- Analyser et évaluer les risques informatiques pour déterminer la probabilité et l'impact sur les objectifs de l'entreprise afin de permettre une prise de décision basée sur les risques.
- Déterminer les options de réponse aux risques et évaluer leur efficience et leur efficacité pour gérer les risques en conformité avec les objectifs commerciaux.
- Suivre en permanence les risques et les contrôles informatiques et en rendre compte aux parties prenantes concernées afin de garantir l'efficacité et l'efficience de la stratégie de gestion des risques informatiques et son alignement sur les objectifs commerciaux.

Public visé

Ce cours s'adresse aux personnes qui cherchent à mieux comprendre l'impact des risques informatiques et la façon dont ils sont liés à leur organisation. Et tout particulièrement aux professionnels de l'audit, du risque et de la sécurité des TI/SI en milieu de carrière.

Prérequis*

- Connaissance de base du fonctionnement d'un SI.
- Des expériences de l'informatique et de la gestion des risques d'entreprise sont un plus.
- Bonne compréhension de l'anglais.

Méthode pédagogique

- 5 jours de cours intensifs
- Cours théorique dispensé en français
- Exercices pratiques et QCM d'entrainement
- Corrections détaillées et expliquées

Matériel

- Support de cours extrait du livre officiel en anglais
- Livre officiel en anglais

Certification

- Cette formation prépare à la certification CRISC - Certified in Risk and Information Systems Control - examen passé ultérieurement, elle n'est donc pas certifiante. Elle donne lieu à une évaluation des connaissances et le cas échant d'un certificat de réussite.
- Il n'y a pas de conditions préalables pour passer l'examen CRISC ; cependant, pour obtenir la certification CRISC, vous devez remplir les conditions d'expérience requises par l'ISACA.
- Trois années ou plus d'expérience en gestion des risques informatiques et en contrôle des SI sont nécessaire pour obtenir la certification.
- Frais d'examen et démarche d'inscription auprès de l'ISACA à la charge du candidat sur : https://www.isaca.org/credentialing/crisc/crisc-exam

Programme

DOMAINE 1 - Gouvernance - 26%
- Gouvernance organisationnelle
- Gouvernance des risques

DOMAINE 2 - Evaluation des risques informatiques - 20%
- Identification des risques informatiques
- Analyse er évaluation des risques informatiques

DOMAINE 3 - Réponse aux risques et rapports - 32%
- Réponse aux risques
- Conception et mise en œuvre du contrôle des risques
- Suivi des risques et rapports

DOMAINE 4 - Technologie et sécurité de l'information - 22 %.
- Principe de technologies de l'information
- Principes de sécurité de l'information

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

3 jours / 21 heures	Réf. : CRISC	3 500€ hors taxes	• 23 au 27 janvier • 22 au 26 mai	• 18 au 22 décembre

Gestion de crise IT/SSI

Les méthodes proactives demeurent limitées et quiconque est confronté un jour à une crise due à des incidents informatiques ou un problème de sécurité. Il faut donc maîtriser cette réaction d'urgence et s'y préparer.

Vous allez apprendre à

- Acquérir les connaissances et l'expertise pour la mise en œuvre et la gestion d'un dispositif de crises en entreprise.
- Développer ses compétences pour maitriser les concepts, les approches et les techniques nécessaires pour la préparation, la conduite, et le conseil de l'entreprise dans un processus de gestion de crises.
- Améliorer son comportement et attitudes lors d'un processus de gestion de crise pour pouvoir gérer et conduire une cellule de crise.

Public visé

- Professionnels de la sécurité physique, de la cybersécurité et de la continuité d'activité
- Délégués à la protection de données
- Responsables communication
- DRH et managers d'entreprises

Pré-requis

- Aucun prérequis n'est nécessaire. Des connaissance de base de l'entreprise et de la gestion des incidents sont un plus.

Méthode pédagogique

- Slides de cours
- Questions-Réponses
- Ateliers
- Exercice de simulation de crise

Certification

Cette formation n'est pas certifiante

Programme

Jour 1

1. Architecture d'un dispositif de crise
- Pourquoi un dispositif de gestion de crise ?
- Les fondements de la gestion de crise
- Système de veille et alerte
- Evaluer la situation et escalade
- L'organisation pour piloter la crise
- Composition d'une cellule de crise
- Leader et relais de gestion de crise
- Le guide de gestion de crise

2. Les processus de remontée d'alertes
- Capteurs internes
- Capteurs externes

3. Anticipation à la gestion de crise
- Scénarii de crise
- Scénarii d'indisponibilité
- Préparation du dispositif de gestion crise
- La cellule de crise
- Le maillage préventif

4. Évaluation de la crise
- Première évaluation
- Les indicateurs d'alerte
- Les niveaux d'alerte
- Pilotage de la gestion de crise

5. Gestion de la crise
- Activation d'une cellule de gestion de crise
- Articulation des cellules de crise
- La logistique et les moyens dédiés à la gestion de crise
- Plan d'action adapté à chaque niveau de crise
- Prise de décision

Jour 2

6. Cas pratiques – Fiches réflexes
- Pandémie
- Incident de Sécurité Informatique et cybersécurité
- Virus Informatique
- Violation de données personnelles
- Confinement réseau informatique
- Indisponibilité d'un bâtiment
- PCA : Activation du Site de Repli
- Evacuation d'un immeuble
- Catastrophe naturelle
- Autres sinistres

7. La communication de crise
- Mettre en œuvre un plan de communication de crise
- Les conditions de succès d'une communication de crise
- Les outils de communication en crise
- La mallette de communication
- ATELIER – Elaborer une communication de crise

8. Les Outils de management de crise
- Les arbres d'appels
- Les fiches d'analyse de l'événement
- La chaine d'alerte
- Fiche de rôles
- La carte des acteurs de la crise
- Questionnaire d'autoévaluation des cellules de gestion de crise
- Le livre de bord (main courante)
- Le Pocket Mémo
- Le Numéro de crise – Numéro vert
- Gestion des notifications
- Localiser ses employés
- Trackers GPS, suivi de flottes
- Maintenance des outils de gestion de crise

Jour 3

9. La sortie de crise
- Evoluer le dispositif pour sortir de la crise
- Débriefing de crise à chaud
- Mener une démarche de retour d'expérience
- Les comptes-rendus de crise
- ATELIER – Evaluer la crise

10. Maintenance du dispositif de crise
- Capitaliser sur la gestion de crise
- Assurer l'amélioration continue de la gestion de crise

11. Atelier – Notification de crise

12. Atelier - Exercice de crise (1/2 journée)
- Efficacité du dispositif de gestion de crise
- Mise en place d'une culture de gestion de crise
- Organiser l'exercice de crise
- Préparation du scénario de crise
- Composition de la cellule de crise
- Déroulement de l'exercice de crise
- Débriefing et évaluation de l'exercice de crise

3 jours / 21 heures	Réf. : Crise IT/SSI	2 100€ hors taxes	• 6 au 8 mars	• 16 au 18 octobre

Formation NIS

MANIKA

Adoptée par les institutions européennes le 6 juillet 2016, la directive Network and Information Security ou NIS est la première initiative de l'Union européenne sur la cybersécurité, qui poursuit l'objectif majeur d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.
La directive instaure des obligations pour les opérateurs de services essentiels (OSE), catégorie distincte des « opérateurs vitaux » (OIV) qui sont déjà soumis à des obligations depuis la loi de programmation militaire (LPM). Les opérateurs essentiels offrent « des services essentiels au fonctionnement de la société ou de l'économie », services qui sont susceptibles d'être gravement affectés par des incidents touchant les réseaux. Ces opérateurs seront désignés par le premier ministre, dans une liste qui sera réactualisée au moins tous les deux ans.
La France à promulguée la directive NIS le 27 février 2018 et en a finalisé la transposition en droit français avec la publication, le 29 septembre 2018, du dernier arrêté d'application portant sur les mesures de sécurité s'appliquant aux OSE.

Vous allez apprendre à

- Maîtriser les enjeux et les exigences de la directive
- Réaliser un état des lieux de la conformité NIS
- Appréhender un projet de mise en conformité

Public visé

- Les personnes souhaitant acquérir des connaissances relatives aux principales règles de la directive
- Responsable de la sécurité de l'information ou équivalent
- Consultant / prestataire intervenant sur les domaines de la gouvernance SSI

Pré-requis*

- Des connaissances en SSI sont un plus

Méthode pédagogique

- Cours magistral basé sur les normes et bonnes pratiques
- Exercices pratiques individuels et collectifs basés sur une étude de cas

Matériel

- Un manuel de cours contenant plus de 100 pages d'informations et d'exemples pratiques est fourni aux participants

Certification

- Cette formation n'est pas certifiante

Programme

- Qu'est-ce-que la directive européenne NIS ?
- Terminologie
- Historique de la directive européenne NIS
- Les grands objectifs de la directive NIS
- Structure de la directive NIS : Procédure de gestion des incidents, alerter des incidents, surveillance du réseau et correction, système de gestion des risques cyber, sensibilisation
- Qu'est-ce-que la sécurité des SI ?
- Qu'est-ce-que la sécurité des réseaux ?
- Les 23 règles de sécurité à appliquer par les OSE et FSN
- Les limites de la directive
- Retour d'expérience / Cas pratique (Analyse des différences / correspondances entre ISO 27001/27002 – Directive NIS)

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

1 jour / 7 heures	Réf. : NIS	700 € hors taxes	• 9 mai	• 6 novembre

Présentation des formations ISO

Vous souhaitez		Vous devez suivre	Page
• Avoir une introduction au SMSI • Acquérir les fondamentaux de la norme ISO 27001 • Comprendre les mesures de sécurité et apprendre à les gérer (élaborer, améliorer et créer des enregistrements et des indicateurs)		**Fondamentaux des normes ISO 27001 & ISO 27002**	16
Appréhender la mise en œuvre des mesures de sécurité de l'information de la norme ISO/CEI 27002 : 2022			17
• Auditer un SMSI • Devenir auditeur interne ou auditeur de certification pour les SMSI		**ISO 27001 Lead Auditor**	18
• Implémenter un SMSI • Devenir responsable de mise en œuvre d'un SMSI	Available in English	**ISO 27001 Lead Implementer**	19
• Apprendre à réaliser une gestion des risques avec la méthode ISO 27005	Available in English	**ISO 27005 Risk Manager**	21
• Apprendre à réaliser une gestion de risque avec la méthode EBIOS		**EBIOS Risk Manager : 2018**	23
• Protéger les données et la confidentialité d'une organisation contre les menaces cybernétiques • Renforcer vos compétences dans la mise en place et la maintenance d'un programme de cybersécurité • Développer les bonnes pratiques pour gérer les politiques de cybersécurité • Améliorer le système de sécurité de l'organisation et assurer sa continuité d'activité • Réagir et récupérer plus rapidement en cas d'incident		**ISO 27032 Lead Cybesecurity Manager**	24
• Accompagner une organisation lors de la mise en œuvre d'un plan de gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035		**ISO 27035 Lead Incident Manager**	25
• Comprendre le processus de mise en œuvre du système de management de la protection de la vie privée • Acquérir les compétences nécessaires pour aider une organisation à mettre en œuvre un système de management de la protection de la vie privée conforme à la norme ISO/IEC 27701 • Soutenir le processus d'amélioration continue du système de management de la protection de la vie privée dans les organisations • Protéger la réputation de l'organisation • Augmenter la transparence des processus et procédures de l'organisation • Maintenir l'intégrité des informations des clients et des autres parties intéressées		**ISO 27701 Lead Implementer**	26
• Acquérir des connaissances approfondies sur les principes fondamentaux, le cadre et les processus de management du risque conforme à la norme ISO 31000		**ISO 31000 Risk Manager**	27
• Comprendre le fonctionnement d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301 • Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011 • Savoir diriger un audit et une équipe d'audit • Savoir interpréter les exigences d'ISO 22301 dans le contexte d'un audit du SMCA • Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011		**ISO 22301 Lead Auditor**	28
• Étendre votre connaissance sur la façon dont un système de management de la continuité des activités vous aidera à atteindre vos objectifs opérationnels • Obtenir les connaissances suffisantes pour gérer une équipe pendant la mise en œuvre de l'ISO 22301 • Renforcer la gestion de votre réputation • Identifier les risques et minimiser l'impact des incidents		**ISO 22301 Lead Implemeter**	29

Fondamentaux ISO 27001 & 27002

La formation d'introduction à la norme ISO/IEC 27001 vous permettra d'appréhender les concepts fondamentaux d'un Système de management de la sécurité de l'information.
La formation d'introduction à la norme ISO/IEC 27002 vous permettra d'appréhender les systèmes de management de la sécurité de l'information et les mesures de sécurité de l'information telles que définies par la norme ISO/IEC 27002.
En participant à la formation d'introduction ISO/IEC 27001 & 27002, vous allez comprendre l'importance d'un SMSI et des mesures de la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

Vous allez apprendre à

- Connaître les concepts, approches, méthodes et techniques permettant de mettre en œuvre un Système de management de la sécurité de l'information
- Comprendre les éléments fondamentaux d'un Système de management de la sécurité de l'information
- Connaître les normes relatives à la sécurité de l'information et les bonnes pratiques de management de la sécurité de l'information permettant de mettre en œuvre et de gérer les mesures de la sécurité de l'information
- Comprendre les mesures de sécurité nécessaires pour gérer les risques de la sécurité de l'information

Public visé

- Les personnes intéressées par le management de la sécurité de l'information
- Les personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information

Pré-requis

- Aucun

Certification

Cette formation n'est pas certifiante

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Programme

Jour 1

- Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/CEI 27001

Jour 2

- Introduction aux mesures de sécurité de l'information, telles que définies par la norme ISO/IEC 27002

2 jours / 14 heures

Réf. : 27001 & 27002

1 500€ hors taxes

• 11 au 12 mai

• 9 au 10 novembre

Formation à la transition entre la norme ISO/IEC 27001:2013 et ISO 27001:2022

La nouvelle version d'ISO/IEC 27001 a été publiée récemment et est maintenant alignée sur la nouvelle version d'ISO/IEC 27002, qui a été publiée en février 2022. Les changements majeurs entre ISO/IEC 27001:2022 et ISO/IEC 27001:2013 portent notamment sur les contrôles de sécurité de l'information de l'annexe A, ainsi que sur clauses de la norme. De plus, le titre de l'ISO/IEC 27001:2022 diffère de celui de l'ISO/IEC 27001:2013, puisque la norme est désormais intitulée *Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences.*

Vous allez apprendre à

- Expliquer les différences entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022.
- Interpréter les nouveaux concepts et exigences de l'ISO/IEC 27001:2022
- Planifier et mettre en œuvre les changements nécessaires à un SMSI existant conformément à la norme ISO/IEC 27001:2022.

Pubic visé

- Les personnes qui souhaitent rester à jour avec les exigences d'ISO/IEC 27001 pour un SMSI.
- Les personnes qui cherchent à comprendre les différences entre les exigences d'ISO/IEC 27001:2013 et d'ISO/IEC 27001:2022.
- Les personnes responsables de la transition d'un SMSI d'ISO/IEC 27001:2013 à ISO/IEC 27001:2022.
- Les managers, formateurs et consultants impliqués dans le maintien d'un SMSI.
- Professionnels souhaitant mettre à jour leur certificat ISO/IEC 27001.

Prérequis

Les participants qui suivent cette formation doivent avoir une compréhension fondamentale des concepts de sécurité de l'information et des exigences de la norme ISO/IEC 27001.*

Méthode pédagogique

- Cette formation est basée sur la théorie et les meilleures pratiques utilisées dans le processus de transition d'un SMSI d'ISO/IEC 27001:2013 à ISO/IEC 27001:2022.
- Les sessions de cours sont illustrées par des quiz qui ont une structure similaire à celle de l'examen de certification.

Matériel

- Support de cours en français
- Dispense en français
- Cours théoriques
- Quizz

Certification

Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO/IEC 27001:2022 ».

Programme

Jour 1

Introduction à ISO/IEC 27001:2022 et comparaison avec ISO/IEC 27001:2013

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Aperçu des changements entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022 et ISO/CEI 27001:2022
- Modifications des clauses 4 à 10 d'ISO/CEI 27001

Jour 2

Comparaison entre les contrôles de l'annexe A de l'ISO/CEI 27001:2013 et de l'ISO/CEI 27001:2022

- Annexe A - Contrôles organisationnels
- Annexe A - Contrôles des personnes
- Annexe A - Contrôles physiques
- Annexe A - Contrôles technologiques

Clôture de la formation

**L'atteinte des prérequis sera validée au moyen d'un QCM envoyé au moment de l'inscription.*

14 heures / 2 jours

Réf. : TRANSI

1 500 € hors taxes

- 30 au 31 janvier
- 3 au 4 avril
- 4 au 5 septembre
- 8 au 19 décembre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ISO 27001 Lead Auditor

La formation ISO/CEI 27001 Lead Auditor vous permettra d'acquérir l'expertise nécessaire pour réaliser des audits de Systèmes de Management de la sécurité de l'information (SMSI) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues. Durant cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes, en conformité avec la norme ISO 19011 et le processus de certification d'ISO/CEI 17021-1.
Grâce aux exercices pratiques, vous serez en mesure de maîtriser les techniques d'audit et disposerez des compétences requises pour gérer un programme d'audit, une équipe d'audit, la communication avec les clients et la résolution de conflits.
Après avoir acquis l'expertise nécessaire pour réaliser cet audit, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Lead Auditor ». Le certificat PECB atteste que vous avez acquis les capacités nécessaires pour l'audit des organismes selon les meilleures pratiques d'audit.

Vous allez apprendre à

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Public visé

- Auditeurs SMSI
- Responsables ou consultants SMSI
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Experts techniques désirant préparer un audit du Système de management de la sécurité de l'information
- Conseillers spécialisés SMSI

Pré-requis*

Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit.

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Certification

Cette formation prépare à l'examen de certification « PECB Certified ISO/CEI 27001 Lead Auditor ».

Programme

Jour 1 – Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Système de management de la sécurité de l'information
- Principes et concepts fondamentaux du Système de management de la sécurité de l'information
- Initialisation de la mise en œuvre du SMSI
- Compréhension de l'organisation et clarification des objectifs de sécurité de l'information
- Analyse du système de management existant

Jour 2 – Planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet du SMSI
- Périmètre du SMSI
- Politiques de sécurité de l'information
- Appréciation du risque
- Déclaration d'applicabilité et décision de la direction pour la mise en œuvre du SMSI
- Définition de la structure organisationnelle de la sécurité de l'information

Jour 3 – Mise en œuvre d'un SMSI

- Définition d'un processus de gestion de la documentation
- Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
- Plan de communication
- Plan de formation et de sensibilisation
- Mise en œuvre des mesures de sécurité
- Gestion des incidents
- Gestion des activités opérationnelles

Jour 4 – Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Compétence et évaluation des « implementers »
- Clôture de la formation

Jour 5 – Examen de certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures

Réf. : 27001 LA

3 500€ hors taxes

- 13 au 17 mars
- 5 au 9 juin
- 9 au 13 octobre
- 4 au 8 décembre

ISO 27001 Lead Implementer

La formation ISO/CEI 27001 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la sécurité de l'information pour sécuriser les informations sensibles, améliorer l'efficacité et la performance globale de l'organisation.
Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

Vous allez apprendre à

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance, et la tenue à jour du SMSI
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information

Public visé

- Responsables ou consultants impliqués dans le management de la sécurité de l'information
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Membres d'une équipe du SMSI

Pré-requis*

Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre.

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées pour la mise en œuvre du SMSI
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Certification

Cette formation prépare à l'examen de certification « PECB Certified ISO/CEI 27001 Lead Implementer »

Programme

Jour 1 – Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Système de management de la sécurité de l'information
- Principes et concepts fondamentaux du Système de management de la sécurité de l'information
- Initialisation de la mise en œuvre du SMSI
- Compréhension de l'organisation et clarification des objectifs de sécurité de l'information
- Analyse du système de management existant

Jour 2 – Planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet du SMSI
- Périmètre du SMSI
- Politiques de sécurité de l'information
- Appréciation du risque
- Déclaration d'applicabilité et décision de la direction pour la mise en œuvre du SMSI
- Définition de la structure organisationnelle de la sécurité de l'information

Jour 3 – Mise en œuvre d'un SMSI

- Définition d'un processus de gestion de la documentation
- Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
- Plan de communication
- Plan de formation et de sensibilisation
- Mise en œuvre des mesures de sécurité
- Gestion des incidents
- Gestion des activités opérationnelles

Jour 4 – Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Compétence et évaluation des « implementers »
- Clôture de la formation

Jour 5 Examen de certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures

Réf. : 27001 LI

3 500€ hors taxes

- 6 au 10 fév.
- 3 au 7 avril
- 19 au 23 juin
- 25 au 29 sept.
- 13 au 17 nov.
- 11 au 15 déc.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ISO 27001 Lead Implementer

ISO/IEC 27001 Lead Implementer training course enables participants to acquire the knowledge necessary to support an organization in effectively planning, implementing, managing, monitoring, and maintaining an information security management system (ISMS). Information security threats and attacks increase and improve constantly. The best form of defense against them is the proper implementation and management of information security controls and best practices. Information security is also a key expectation and requirement of customers, legislators, and other interested parties. This training course is designed to prepare participants in implementing an information security management system (ISMS) based on ISO/IEC 27001. It aims to provide a comprehensive understanding of the best practices of an ISMS and a framework for its continual management and improvement. After attending the training course, you can take the exam. If you successfully pass it, you can apply for a "PECB Certified ISO/IEC 27001 Lead Implementer" credential, which demonstrates your ability and practical knowledge to implement an ISMS based on the requirements of ISO/IEC 27001.

Learning objectives

- Explain the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001
- Interpret the ISO/IEC 27001 requirements for an ISMS from the perspective of an implementer
- Initiate and plan the implementation of an ISMS based on ISO/IEC 27001, by utilizing PECB's IMS2 Methodology and other best practices
- Support an organization in operating, maintaining, and continually improving an ISMS based on ISO/IEC 27001
- Prepare an organization to undergo a third-party certification audit

Who can attend

- Project managers and consultants involved in and concerned with the implementation of an ISMS
- Expert advisors seeking to master the implementation of an ISMS
- Individuals responsible for ensuring conformity to information security requirements within an organization
- Members of an ISMS implementation team

Prerequisites*

- General knowledge of the ISMS concepts and ISO/IEC 27001

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Educational approach

- This training course contains essay-type exercises, multiple-choice quizzes, examples, and best practices used in the implementation of an ISMS.
- The participants are encouraged to communicate with each other and engage in discussions when completing quizzes and exercises.
- The exercises are based on a case study.
- The structure of the quizzes is similar to that of the certification exam.

Course material

- Course material in English in paper and/or digital format
- Associated annexes in French and/or English

Certification

This course prepares for the "PECB Certified ISO/IEC 27001 Lead Implementer" certification exam

Programme

Day 1 – Introduction to ISO/IEC 27001 and initiation of an ISMS

- Training course objectives and structure
- Standards and regulatory frameworks
- Information Security Management System (ISMS)
- Fundamental information security concepts and principles
- Initiation of the ISMS implementation
- Understanding the organization and its context
- ISMS scope

Day 2 – Planning the implementation of an ISMS

- Leadership and project approval
- Organizational structure
- Analysis of the existing system
- Information security policy
- Risk management
- Statement of Applicability

Day 3 – Implementation of an ISMS

- Documented information management
- Selection and design of controls
- Implementation of controls
- Trends and technologies
- Communication
- Competence and awareness
- Security operations management

Day 4 – ISMS monitoring, continual improvement, and preparation for the certification audit

- Monitoring, measurement, analysis, and evaluation
- Internal audit
- Management review
- Treatment of nonconformities
- Continual improvement
- Preparing for the certification audit
- Certification process and closing of the training course

Day 5 Certification Exam

** The learner undertakes to meet the necessary prerequisites. A written statement and/or CV may be required. A successful MCQ to validate that the prerequisites have been met may be required to confirm registration.*

5 days / 35 hours

Ref. : 27001 LI EN

3 500€ VAT excl.

- 16 au 20 janvier
- 4 au 8 septembre

ISO 27005 Risk Manager

La formation « ISO/CEI 27005 Risk Manager » vous permettra de développer les compétences pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/CEI 27005 comme cadre de référence. Au cours de cette formation, nous présenterons également d'autres méthodes d'appréciation des risques telles qu'OCTAVE, EBIOS, MEHARI et la méthodologie harmonisée d'EMR. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre SMSI selon la norme ISO/CEI 27001.

Vous allez apprendre à

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information

Public visé

- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation
- Tout individu mettant en œuvre ISO/CEI 27001, désirant se conformer à la norme ISO/CEI 27001 ou impliqué dans un programme de gestion des risques
- Consultants des TI
- Professionnels des TI
- Agents de la sécurité de l'information
- Agents de la protection des données personnelles

Pré-requis*

Des connaissances fondamentales de la norme ISO/IEC 27005 et des connaissances approfondies sur l'appréciation du risque et la sécurité de l'information

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans la gestion des risques liés à la sécurité de l'information
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Certification

Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO 27005 Risk Manager »

Pack 1 semaine : ISO 27005 RM + Ebios RM 2018

Tarif : 3 500€ hors taxes

Dates :
• 12 au 16 juin
• 27 nov. au 1er déc.

Programme

Jour 1 – Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005

- Objectifs et structure de la formation
- Concepts et définitions du risque
- Cadres normatifs et règlementaires
- Mise en œuvre d'un programme de gestion des risques
- Compréhension de l'organisation et de son contexte

Jour 2 – Mise en œuvre d'un processus de gestion des risques conforme à la norme ISO/CEI 27005

- Identification des risques
- Analyse et évaluation des risques
- Appréciation du risque avec une méthode quantitative
- Traitement des risques
- Acceptation des risques et gestion des risques résiduels
- Communication et concertation relatives aux risques en sécurité de l'information
- Surveillance et revue du risque

Jour 3 – Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

- Méthode OCTAVE
- Méthode MEHARI
- Méthode EBIOS
- Méthodologie harmonisée d'EMR
- Clôture de la formation
- Passage de la certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

3 jours / 21 heures

Réf. : 27005 RM

2 150€ hors taxes

• 30 jan. au 1er fév. • 30 mai au 1er juin • 6 au 8 nov.
• 11 au 13 avril • 20 au 22 sept. • 4 au 6 déc.

ISO 27005 Risk Manager

ISO/IEC 27005 Risk Manager training enables you to develop the competence to master the risk management process related to all assets of relevance for Information Security using the ISO/IEC 27005 standard as a reference framework. During this training course, you will also gain a thorough understanding of best practices of risk assessment methods such as OCTAVE, EBIOS, MEHARI and harmonized TRA. This training course corresponds with the implementation process of the ISMS framework presented in the ISO/IEC 27001 standard.
After understanding all the necessary concepts of Information Security Risk Management based on ISO/IEC 27005, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27005 Risk Manager" credential. By holding a PECB Risk Manager Certificate, you will be able to demonstrate that you have the necessary skills and knowledge to perform an optimal Information Security Risk Assessment and timely manage Information Security risks.

Learning objectives

- Acknowledge the correlation between Information Security risk management and security controls
- Understand the concepts, approaches, methods and techniques that enable an effective risk management process according to ISO/IEC 27005
- Learn how to interpret the requirements of ISO/IEC 27001 in Information Security Risk Management
- Acquire the competence to effectively advise organizations in Information Security Risk Management best practices

Who can attend

- Information Security team members
- Individuals responsible for Information Security, compliance, and risk within an organization
- Individuals implementing ISO/IEC 27001, seeking to comply with ISO/IEC 27001 or involved in a risk management program
- IT consultants
- IT professionals
- Information Security officers
- Privacy officers

Prerequisites*

A fundamental understanding of ISO/IEC 27005 and comprehensive knowledge of Risk Assessment and Information Security.

Educational approach

- This training is based on both theory and best practices used in Information Security Risk Management
- Lecture sessions are illustrated with examples based on cases studies
- Practical exercises are based on a case study which includes role playing and discussions
- Practice tests are similar to the Certification Exam

Course material

- Course material in English
- Associated annexes in French and/or in English

Certification

This course prepares for the examination of "PECB Certified ISO/IEC 27005 Risk Manager".

Program

Day 1 – Introduction to ISO/IEC 27005 and implementation of a risk management program

- Course objectives and structure
- Standard and regulatory framework
- Concepts and definitions of risk
- Risk management program
- Context establishment

Day 2 – Information security risk assessment, risk treatment and acceptance as specified in ISO/IEC 27005

- Risk identification
- Risk analysis
- Risk evaluation
- Risk assessment with a quantitative method
- Risk treatment
- Information security risk acceptance

Day 3 – Risk communication, consultation, monitoring, review, and risk assessment methods

- OCTAVE method
- MEHARI method
- EBIOS method
- Harmonized Threat and Risk Assessment (TRA) method
- Applying for certification and closing the training

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

** The learner undertakes to meet the necessary prerequisites. A written statement and/or CV may be required. A successful MCQ to validate that the prerequisites have been met may be required to confirm registration.*

3 days / 21 hours

Ref. : 27005 RM EN

2 150€ VAT excl.

- 9 au 11 janvier
- 3 au 5 juillet

Ebios Risk Manager : 2018

Cette formation vous permettra d'acquérir les connaissances et développer les compétences nécessaires pour maîtriser les concepts et les éléments de management des risques liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la méthode EBIOS. Grâce aux exercices pratiques et aux études de cas, vous acquerrez les connaissances et les compétences nécessaires pour réaliser une appréciation optimale des risques liés à la sécurité de l'information et pour gérer les risques dans les temps par la connaissance de leur cycle de vie. Cette formation s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/CEI 27001.

Vous allez apprendre à

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude EBIOS
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme
- Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS

Public visé

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnel participant aux activités d'appréciation des risques selon la méthode EBIOS
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode EBIOS

Pré-requis*

Une connaissance en gestion du risque est recommandée

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les bonnes pratiques d'appréciation du risque avec la méthode EBIOS
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Certification

Cette formation prépare à l'examen de certification Ebios Risk Manager par Deloitte Cyber Academy et labélisé par l'ANSSI

La liste nominative de nos formateurs Ebios Risk Manager est disponilbe sur notre site internet.
Chacun d'eux est signataire de la Charte Ebios.

Programme

Jour 1
Introduction à la méthode d'appréciation des risques EBIOS

Jour 2
Réaliser l'appréciation des risques selon la méthode EBIOS

Jour 3
Atelier avec études de cas et examen de certification

Pack 1 semaine : ISO 27005 RM + Ebios RM 2018

Tarif : 3 500€ hors taxes

Dates :
• 12 au 16 juin
• 27 nov. au 1er déc.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

3 jours / 21 heures	Réf. : EBIOS RM	2 150€ hors taxes	• 17 au 19 avril	• 16 au 18 octobre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ISO 27032 Lead Cybersecurity Manager

La formation ISO/IEC 27032 Lead Cybersecurity Manager vous permet d'acquérir l'expertise et les compétences nécessaires pour soutenir un organisme dans la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST. Au cours de cette formation, vous acquerrez des connaissances approfondies sur la cybersécurité, la relation entre la cybersécurité et d'autres types de sécurité informatique, ainsi que le rôle des parties prenantes dans la cybersécurité.
Après avoir maîtrisé toutes les notions de cybersécurité nécessaires, vous pouvez vous présenter à l'examen et postuler pour une attestation « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ». En étant titulaire d'un certificat PECB Lead Cybersecurity Manager, vous serez en mesure de démontrer que vous possédez les connaissances pratiques et les capacités professionnelles nécessaires pour soutenir et diriger une équipe dans le management de la cybersécurité.

Vous allez apprendre à

- Acquérir des connaissances approfondies sur les éléments et les activités d'un programme de cybersécurité, conformément à la norme ISO/IEC 27032 et au cadre de cybersécurité du NIST
- Reconnaître la corrélation entre la norme ISO/CEI 27032, le cadre de cybersécurité du NIST et d'autres normes et cadres d'exploitation
- Maîtriser les notions, les approches, les normes, les méthodes et les techniques utilisées pour concevoir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les lignes directrices de la norme ISO/IEC 27032 dans le contexte particulier d'un organisme
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité, comme spécifié dans la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST
- Acquérir l'expertise nécessaire pour conseiller un organisme sur les pratiques d'excellence du management de la cybersécurité

Pré-requis*

Des connaissances fondamentales de la norme ISO/IEC 27032 et des SI sont recommandés

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Public visé

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels cherchant à gérer un programme de cybersécurité
- Personnes responsables de la conception d'un programme de cybersécurité
- Spécialistes de la TI
- Conseillers-experts en technologie de l'information
- Professionnels de la TI qui cherchent à améliorer leurs compétences et leurs connaissances techniques

Examen

- L'examen « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager » satisfait entièrement les exigences du programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :
- Domaine 1 - Principes fondamentaux et notions de la cybersécurité
- Domaine 2 - Rôles et responsabilités des parties prenantes
- Domaine 3 - Management du risque en cybersécurité
- Domaine 4 - Mécanismes d'attaque et mesures de contrôle de cybersécurité
- Domaine 5 - Partage et coordination de l'information
- Domaine 6 - Intégration du programme de cybersécurité dans le management de la continuité des activités
- Domaine 7 - Management des incidents de cybersécurité et mesure de la performance

Certification

- Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ».

Programme

Jour 1
Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032
- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

Jour 2
Politiques de cybersécurité, management du risque et mécanismes d'attaque
- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

Jour 3
Mesures de contrôle de cybersécurité, partage et coordination de l'information
- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

Jour 4
Gestion des incidents, suivi et amélioration continue
- Continuité des activités
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

Jour 5
Examen de certification

5 jours / 35 heures | Réf. : 27032 LCM | 3 500€ hors taxes | • 13 au 17 février | • 23 au 27 octobre

ISO 27035 Lead Incident Manager

La formation ISO/CEI 27035 Lead Incident Manager vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de la mise en œuvre d'un plan de gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035. Durant cette formation, vous acquerrez une connaissance approfondie sur le modèle de processus permettant de concevoir et de développer un plan de gestion des incidents des organisations. La compatibilité de cette formation avec l'ISO/CEI 27035 prend également en charge l'ISO/CEI 27001 en offrant des lignes directrices pour la gestion des incidents de sécurité de l'information. Après avoir maîtrisé l'ensemble des concepts relatifs à la gestion des incidents de sécurité de l'information vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27035 Lead Incident Manager ». En étant titulaire d'une certification Lead Incident Manager de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles nécessaires pour soutenir et diriger une équipe dans la gestion des incidents de sécurité de l'information.

Vous allez apprendre à

- Maîtriser les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/CEI 27035
- Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres réglementaires
- Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en œuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information
- Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
- Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
- Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

Pré-requis*

Des connaissances fondamentales de la norme ISO/IEC 27035 et des SI sont recommandés

Public visé

- Gestionnaires des incidents de sécurité de l'information
- Responsables des TIC
- Auditeurs des technologies de l'information
- Responsables souhaitant mettre en place une équipe de réponse aux incidents
- Responsables souhaitant apprendre davantage sur le fonctionnement efficace d'une équipe de réponse aux incidents
- Responsables des risques liés à la sécurité de l'information
- Administrateurs professionnels des systèmes informatiques
- Administrateurs professionnels de réseau informatique
- Membres de l'équipe de réponse aux incidents
- Personnes responsables de la sécurité de l'information au sein d'une organisation

Examen

- L'examen « PECB Certified ISO/CEI 27035 Lead Incident Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :
  - Domaine 1 - Principes et concepts fondamentaux relatifs à la gestion des incidents liés à la sécurité de l'information
  - Domaine 2 - Meilleures pratiques de la gestion des incidents liés à la sécurité de l'information selon la norme ISO/CEI 27035
  - Domaine 3 - Conception et développement d'un processus de gestion des incidents organisationnels selon l'ISO/CEI 27035
  - Domaine 4 - Préparation aux incidents de sécurité de l'information et mise en œuvre d'un plan de gestion des incidents
  - Domaine 5 - Lancement du processus de gestion des incidents et traitement des incidents liés à la sécurité de l'information
  - Domaine 6 - Surveillance et mesure de la performance
  - Domaine 7 - Améliorer les processus et les activités de gestion des incidents

Certification

- Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO/CEI 27035 Lead Incident Manager ».

Programme

Jour 1 - Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035

- Objectifs et structure de la formation
- Cadres normatifs et réglementaires
- Gestion des incidents liés à la sécurité de l'information
- Processus de base de la norme ISO/CEI 27035
- Principes fondamentaux de la sécurité de l'information
- Corrélation avec la continuité des activités
- Questions légales et déontologiques

Jour 2 - Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- Lancement d'un processus de gestion des incidents de sécurité de l'information
- Compréhension de l'organisation et clarification des objectifs de la gestion des incidents de sécurité de l'information
- Planifier et préparer
- Rôles et fonctions
- Politiques et procédures

Jour 3 - Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information

- Planification de la communication
- Premières étapes de la mise en œuvre
- Mise en place des éléments de support
- Détection et rapport
- Évaluation et décisions
- Réponses
- Leçons apprises
- Transition aux opérations

Jour 4 - Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information

- Analyse supplémentaire
- Analyse des leçons apprises
- Mesures correctives
- Compétence et évaluation des gestionnaires d'incidents
- Clôture de la formation

Jour 5 - Examen de certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures

Réf. : 27035 LIM

3 500€ hors taxes

• 13 au 17 février

• 2 au 6 octobre

ISO 27701 Lead Implementer

Cette formation est conçue pour préparer les participants à mettre en œuvre un système de management de la protection de la vie privée (Privacy Information Management System – PIMS) conformément aux exigences et aux directives d'ISO/IEC 27701. De plus, vous acquerrez une compréhension globale des meilleures pratiques de gestion des données personnelles et apprendrez comment gérer et traiter les données tout en respectant les différents régimes de confidentialité de ces données.

Vous allez apprendre à

- Maîtriser les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS
- En savoir plus sur la corrélation entre ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Comprendre le fonctionnement d'un PIMS selon ISO/IEC 27701 et ses principaux processus
- Apprendre à interpréter les exigences d'ISO/IEC 27701 dans le contexte spécifique d'une organisation
- Développer l'expertise nécessaire pour aider une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et le maintien efficaces d'un PIMS

Public visé

- Directeurs et consultants impliqués dans la confidentialité et la gestion des données
- Experts-conseils cherchant à maîtriser la mise en œuvre d'un système de management de la protection de la vie privée
- Responsables des informations personnellement identifiables (IPI) au sein des organisations
- Responsables de la conformité aux exigences des lois sur la protection des données
- Membres de l'équipe PIMS

Pré-requis*

Compréhension fondamentale de la sécurité de l'information et connaissance approfondie des principes de mise en œuvre du SMSI.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Méthode pédagogique

- Ce cours de formation s'appuie à la fois sur la théorie et sur les meilleures pratiques utilisées dans la mise en œuvre du PIMS
- Les sessions de cours sont illustrées par des exemples basés sur des études de cas
- Les exercices pratiques sont basés sur une étude de cas qui comprend des jeux de rôle et des discussions
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours

Certification

Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO 27701 Lead Implementer »

Programme

Jour 1 – Introduction à l'ISO/IEC 27701 et initiation au PIMS

- Objectifs et structure de la formation h Normes et cadres réglementaires
- Système de management de la protection de la vie privée (PIMS)
- Concepts et principes fondamentaux de la sécurité de l'information et de la protection de la vie privée
- Démarrage de la mise en œuvre du PIMS
- Analyse du domaine d'application du SMSI et de la déclaration d'applicabilité
- Domaine d'application du PIMS
- Approbation de la direction
- Politique de protection de la vie privée
- Appréciation du risque d'atteinte à la vie privée

Jour 2 – Planification de la mise en œuvre d'un PIMS

- Appréciation de l'impact sur la vie privée
- Déclaration d'applicabilité du PIMS
- Gestion de la documentation
- Sélection des mesures
- Mise en œuvre des mesures

Jour 3 – Mise en œuvre d'un PIMS

- Mise en œuvre des mesures (suite)
- Mise en œuvre des mesures spécifiques aux contrôleurs IPI
- Mise en œuvre des mesures spécifiques aux processeurs IPI

Jour 4 – Surveillance du PIMS, amélioration continue et préparation d'un audit de certification

- Sensibilisation, formation et communication
- Surveillance, mesure, analyse, évaluation et revue de direction
- Audit interne
- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

Jour 5 Examen de certification

5 jours / 35 heures	Réf. : 27701 LI	3 500€ hors taxes	• 20 au 24 mars	• 20 au 24 novembre

ISO 31000 Risk Manager

La formation ISO 31000 Risk Manager vous permettra d'acquérir des connaissances approfondies sur les principes fondamentaux, le cadre et les processus de management du risque conforme à la norme ISO 31000. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de management du risque et à développer vos aptitudes pour les mettre en œuvre dans un organisme afin de mettre en œuvre efficacement un processus de management du risque.
Après avoir appréhendé les concepts nécessaires du management du risque, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 31000 Risk Manager ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances et des compétences pratiques pour gérer efficacement un processus du risque dans un organisme.

Vous allez apprendre à

- Comprendre les concepts et les processus fondamentaux relatifs au management du risque
- Connaître la corrélation entre la norme ISO 31000 et la norme CEI/ISO 31010, ainsi qu'avec d'autres normes et cadres règlementaires
- Comprendre les approches, les méthodes et techniques utilisées pour gérer le risque dans un organisme
- Savoir interpréter les principes et les lignes directrices de la norme ISO 31000

Public visé

- Gestionnaires ou consultants chargés du management efficace du risque dans un organisme
- Toute personne désirant acquérir des connaissances approfondies sur les concepts, processus et principes de management du risque
- Conseillers impliqués dans le management du risque

Pré-requis*

Des connaissances fondamentales de la norme ISO/IEC 31000 et de la gestion des risques sont recommandés

Examen

- L'examen « PECB Certified ISO 31000 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1- Principes et concepts fondamentaux relatifs au management du risque
- Domaine 2 - Processus et cadre organisationnel de management du risque
- Domaine 3 - Techniques d'évaluation des risques conformes à la norme CEI/ISO 31010

Certification

- Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified ISO 31000 Risk Manager ».

Programme

Jour 1
Introduction aux principes et au cadre organisationnel de l'ISO 31000

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Introduction aux principes et aux concepts de la norme ISO 31000
- Cadre organisationnel de management du risque
- Mise en œuvre du processus de management du risque
- Établissement du contexte

Jour 2
Processus de management du risque conforme à la norme ISO 31000
Identification des risques

- Analyse du risque
- Évaluation du risque
- Traitement du risque
- Acceptation du risque
- Communication et concertation relatives aux risques
- Surveillance et revue du risque

Jour 3
Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010 et examen de certification

- Méthodologies de gestion du risque, conformes à la norme ISO 31010 (partie 1)
- Méthodologies de gestion du risque, conformes à la norme ISO 31010 (partie 2)
- Compétence, évaluation et clôture de la formation

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

3 jours / 21 heures

Réf. : 31000 RM

2 150€ hors taxes

- 23 au 25 janvier
- 23 au 25 octobre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ISO 22301 Lead Auditor

La formation ISO 22301 Lead Auditor vous permettra d'acquérir l'expertise nécessaire pour réaliser des audits de Système de management de la continuité d'activité (SMCA) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues. Durant cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes, en conformité avec la norme ISO 19011 et le processus de certification d'ISO/CEI 17021-1.
Grâce aux exercices pratiques, vous serez en mesure de maîtriser les techniques d'audit et disposerez des compétences requises pour gérer un programme d'audit, une équipe d'audit, la communication avec les clients et la résolution de conflits.
Après avoir acquis l'expertise nécessaire pour réaliser cet audit, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 Lead Auditor ». Le certificat PECB atteste que vous avez acquis les capacités nécessaires pour l'audit des organisations selon les meilleures pratiques d'audit.

Vous allez apprendre à

- Comprendre le fonctionnement d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301
- Expliquer la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO 22301 dans le contexte d'un audit du SMCA
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Public visé

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la continuité d'activité
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la continuité d'activité
- Toute personne responsable du maintien de la conformité aux exigences du SMCA
- Experts techniques désirant préparer un audit du Système de management de la continuité d'activité
- Conseillers spécialisés en management de la continuité d'activité

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Pré-requis*

- Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMAC
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Certification

- Cette formation prépare à l'examen de certification « PECB Certified ISO 22301 Lead Auditor »

Programme

Jour 1 – Introduction au Système de management de la continuité d'activité et à la norme ISO 22301

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Processus de certification
- Principes fondamentaux du Système de management de la continuité d'activité
- Système de management de la continuité d'activité

Jour 2 – Principes, préparation et déclenchement de l'audit

- Principes et concepts fondamentaux d'audit
- Approche d'audit fondée sur les preuves
- Déclenchement de l'audit
- Étape 1 de l'audit
- Préparation de l'étape 2 de l'audit (audit sur site)
- Étape 2 de l'audit (première partie)

Jour 3 – Activités d'audit sur site

- Étape 2 de l'audit (deuxième partie)
- Communication pendant l'audit
- Procédures d'audit
- Rédaction des plans de tests d'audit
- Rédaction des constats d'audit et des rapports de non-conformité

Jour 4 – Clôture de l'audit

- Documentation de l'audit et revue de qualité de l'audit
- Clôture de l'audit
- Évaluation des plans d'actions par l'auditeur
- Avantages de l'audit initial
- Management d'un programme d'audit interne
- Compétence et évaluation des auditeurs
- Clôture de la formation

Jour 5 – Examen de certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures	22301 LA	3 500€ hors taxes	• 11 au 15 septembre

ISO 22301 Lead Implementer

La formation ISO 22301 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la continuité d'activité et à développer vos aptitudes à fournir un cadre qui permet à l'organisation de continuer ses activités durant les crises.
Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la continuité d'activité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 Lead Implementer ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO 22301 dans une organisation.

Vous allez apprendre à

- Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA
- Savoir interpréter les exigences de la norme ISO 22301 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMCA
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la continuité d'activité

Public visé

- Responsables ou consultants impliqués dans le management de la continuité d'activité
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la continuité d'activité
- Toute personne responsable du maintien de la conformité aux exigences du SMCA
- Membres d'une équipe du SMCA

Pré-requis*

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de sa mise en œuvre

Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées pour la mise en œuvre du SMCA
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification

Matériel

- Support de cours en français
- Annexes associées en français et/ou anglais

Certification

Cette formation prépare à l'examen de certification « PECB Certified ISO 22301 Lead Implementer »

Programme

Jour 1 – Introduction à la norme ISO 22301 et initialisation d'un SMCA

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Système de management de la continuité d'activité
- Principes et concepts fondamentaux du Système de management de la continuité d'activité
- Initialisation de la mise en œuvre du SMCA
- Compréhension de l'organisme
- Analyse du système de management existant
- Périmètre du SMCA

Jour 2 – Planification de la mise en œuvre d'un SMCA

- Leadership et engagement
- Politiques du SMCA
- Structure organisationnelle
- Informations documentées
- Compétences et sensibilisation
- Analyse d'impacts sur les activités (BIA)
- Appréciation du risque

Jour 3 – Mise en œuvre d'un SMCA

- Stratégie de continuité d'activité
- Mesures de protection et d'atténuation
- Procédures et plans de la continuité d'activité
- Plan de réponse aux incidents
- Plan d'intervention d'urgence
- Plan de gestion de crise
- Plan de reprise informatique
- Plan de restauration
- Plan de communication

Jour 4 – Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA

- Tests et exercices
- Mesure et surveillance du SMCA
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Compétence et évaluation des « implementers »
- Clôture de la formation

Jour 5 – Examen de certification

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures	22301 LI	3 500€ hors taxes	• 27 au 31 Mars	• 16 au 20 octobre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Droit de la SSI

La conformité juridique est aujourd'hui un aspect essentiel de la sécurité de l'information. Or, les obligations à respecter sont nombreuses et pas toujours faciles à comprendre et à respecter.
« Droit de la SSI » propose aux professionnels d'acquérir une connaissance pratique, concrète et pragmatique de la matière. La formation leur permettra d'évaluer et de renforcer le niveau de conformité de leur organisme.

Vous allez apprendre à

- Connaître la signification pratique des règles juridiques
- Appliquer les règles juridiques de façon concrète et pragmatique
- Renforcer efficacement le niveau de conformité de votre organisme

Public visé

Toutes les personnes impliquées dans la sécurité informatique :

- RSSI
- DSI
- Administrateurs systèmes et réseaux
- Astreintes opérationnelles
- Maîtrises d'oeuvre de la SSI
- Chefs de projet
- Responsables de comptes
- Consultants

Pré-requis

- Aucun. Il n'est pas nécessaire de disposer de connaissances en droit ou en informatique pour suivre cette formation.

Méthode pédagogique

- Explication des notions juridiques en langage courant
- Cours totalement interactif
- Formation dispensée en français

Matériel

- Support de cours en français au format papier

Certification

- Cette formation n'est pas certifiante

Programme

Enjeux de la conformité

Sources d'information

Informatique et libertés (RGPD)

- Découverte et notions essentielles
- Principes fondamentaux
- Démarche de conformité
- Sécurité des données personnelles
- Relations avec les personnes concernées
- Relations avec les sous-traitants
- Transferts en dehors de l'Union européenne
- Registre et PIA
- Contrôles et sanctions

Communications électroniques

- Notions fondamentales
- Sources d'information
- Secret des correspondances
- Cryptologie
- Brouillage des communications
- Contrôles de sécurité sur les opérateurs
- Filtrage

Conservation des traces (logs)

- Données relatives au trafic
- Données d'identification des créateurs de contenus
- Autres traces

Atteintes aux systèmes informatiques

- Cadre juridique des intrusions et dénis de service
- Réagir à une atteinte
- Conséquences en droit social

Surveillance des salariés

- Pouvoir de contrôle de l'employeur
- Respect de la vie privée « résiduelle »
- Courriers électroniques et SMS
- Fichiers
- Navigation sur Internet
- Accès à l'ordinateur du salarié

Administrateurs systèmes et réseaux

- Obligation de confidentialité renforcée
- Accès étendus
- Responsabilité

Charte informatique

- Cibles, fonctions et enjeux
- Contenu et rédaction
- Opposabilité et formalisme

3 jours / 21 heures	Réf. : Droit SSI	2 250€ hors taxes	• 30 mai au 1er juin	• 4 au 6 décembre

RGPD : essentiel de la conformité

Le règlement européen sur la protection des données personnelles est venu refondre le cadre juridique en matière « informatique et libertés ». Le RGPD couvre tout un panel d'obligations pour les responsables de traitement et les sous-traitants. Il touche également tous les métiers au sein des organismes, aussi bien la sécurité de l'information que la maîtrise des risques.
RGPD : essentiel de la conformité est une formation indispensable pour connaître tous les points clés du RGPD. Elle appréhende le texte d'un point de vue pratique et opérationnel, elle s'adresse aussi bien aux profils techniques que juridiques et peut être suivie par toute personne curieuse de la matière.

Vous allez apprendre à

- Les principaux points clés du RGPD et leurs implications opérationnelles
- Les chantiers à mettre en place pour la mise en conformité
- Les bons réflexes dans la pratique quotidienne de la protection des données

Public visé

- Futurs DPO ou DPO débutants
- Directions
- Juristes souhaitant se spécialiser et/ou avoir une vision globale du RGPD
- RSSI ou techniciens souhaitant renforcer leurs connaissances juridiques en la matière
- Chefs de projet et MOE/maîtrise d'œuvre
- Auditeur ou toute personne impliquée dans la réalisation d'un audit
- Relais ou référents RGPD au sein des directions et travaillant dans la maitrise des risques

Pré-requis

- Aucun pré-requis, néanmoins avoir déjà parcouru le RGPD est un plus

Certification

- À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification " RGPD : essentiel de la conformité " de Deloitte Cyber Academy.

Programme

Introduction
- Fondamentaux juridiques
- Historique et avenir du règlement européen
- Enjeux de la protection des données personnelles

Quelles sont les enjeux fondamentaux du RGPD ?
- Champ d'application du règlement
- Principes fondamentaux
- Notions essentielles et acteurs
- Responsabilités (responsabilité du DPO, du sous-traitant, responsabilité conjointe, etc.)
- Les risques de non-conformité

Comment assurer la conformité de son organisme ?
- Piloter la protection des données personnelles avec un DPO
- Gérer les risques avec l'analyse d'impact (PIA : Privacy impact assessment)
- Cartographier avec le registre des activités de traitements
- Veiller aux données particulières (données sensibles, judiciaires, protection des mineurs, etc.)
- Assurer la sécurité des données
- Gérer les droits des personnes concernées
- Veiller aux transferts de données en dehors de l'UE
- Se préparer à un contrôle
- Coopérer avec les autorités

Quels sont les outils permettant d'assurer la conformité ?
- Certifications et codes de conduite
- Methodologies de conformité
- Veille
- Références

Perspectives du renforcement du nouveau cadre européen data (Intelligence Artificial Act, DSA, DGA, DMA..) et articulations avec le RGPD

2 jours / 14 heures | Réf. : RGPD | 1 400€ hors taxes | • 9 au 10 mai | • 9 au 10 octobre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Certification des Compétences du DPO conformément au référentiel de certification de la CNIL

La formation certifiante PECB « Data Protection Officer » vous permettra d'acquérir les connaissances et compétences nécessaires pour mettre en œuvre et gérer de façon efficace un cadre de conformité visant la protection des données à caractère personnel. Après avoir maîtrisé les concepts liés au Règlement général sur la protection des données (RGPD), vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified Data Protection Officer ». En détenant un certificat « PECB Certified Data Protection Officer », vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour aider les organismes à appliquer les lois et les règlements en matière de protection des données.

Vous allez apprendre à

- Acquérir une compréhension approfondie des concepts fondamentaux et des éléments du Règlement sur la protection des données.
- Comprendre l'objectif, le contenu et la corrélation entre le Règlement général sur la protection des données et les autres cadres réglementaires.
- Acquérir une compréhension approfondie des concepts, des approches, des méthodes et des techniques permettant une protection efficace des données à caractère personnel.
- Savoir interpréter les exigences relatives à la protection des données dans le contexte particulier d'un organisme.
- Acquérir l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir un cadre de conformité en ce qui concerne le RGPD.

Public visé

- À des responsables de projets et consultants qui désirent préparer et aider un organisme à mettre en œuvre les nouvelles procédures et à adopter les nouvelles exigences présentées dans le RGPD.
- Aux délégués à la protection des données et membres de la direction générale responsables de la protection des données à caractère personnel d'une entreprise et de la gestion de ses risques.
- Aux membres d'équipes de sécurité de l'information, de gestion des incidents et de continuité des activités.
- Aux conseillers spécialisés en sécurité des données à caractère personnel
- Aux spécialistes des questions techniques et de conformité qui désirent se préparer à occuper un poste de délégué à la protection des données.

Pré-requis*

Une compréhension fondamentale du RGPD et des connaissances de base sur les exigences légales actuelles en matière de protection des données.

Méthode pédagogique

- Cette formation est basée sur le règlement et les meilleures pratiques.
- Les séances de cours sont illustrées par des exemples basés sur des études de cas.
- Les exercices pratiques sont basés sur des études de cas qui inclut des jeux de rôle et discussions.
- Les tests pratiques sont similaires à l'examen de certification.

Certification

- Après avoir réussi l'examen, les participants peuvent demander la qualification « PECB Certified Data Protection Officer ».
- Certification agrée par la CNIL.

Programme

Jour 1 – Introduction au RGPD et mise en œuvre de la conformité au RGPD

- Objectifs et structure du cours
- Règlement général sur la protection des données
- Principes fondamentaux du RGPD
- Débuter la mise en place du RGPD
- Comprendre l'organisme et clarifier les objectifs de la protection des données
- Analyse du système actuel

Jour 2 – Planification de la mise œuvre du RGPD

- Direction et approbation du projet de conformité du RGPD
- Politique de protection des données
- Définition de la structure organisationnelle de la protection des données
- Classification des données
- Évaluation des risques en vertu du RGPD

Jour 3 – Déploiement du RGPD

- Analyse d'impact sur la protection des données
- Conception des mesures de sécurité et rédaction de politiques et de procédures spécifiques
- Mise en œuvre des mesures de sécurité
- Définition du processus de gestion des documents
- Plan de communication

Jour 4 – Surveillance et amélioration continue de la conformité au RGPD

- Plan de formation et de sensibilisation
- Gestion des opérations
- Gestion des incidents
- Surveillance, mesure, analyse et évaluation
- Audit interne
- Violation des données et actions correctives
- Amélioration continue
- Compétence, évaluation et fin de la formation

Jour 5 – Examen de certification

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures

Réf. : Cert DPO

3 500€ hors taxes

- 20 au 24 mars
- 11 au 15 décembre
- 11 au 15 septembre

Test d'intrusion et sécurité offensive

L'intérêt des tests d'intrusion pour évaluer la sécurité d'un système informatique n'est aujourd'hui plus à démontrer. Ils permettent de découvrir des vulnérabilités majeures, montrent comment un attaquant peut progresser au sein du réseau ciblé. Enfin ils permettent de répondre aux exigences de nombreuses normes.

Vous allez apprendre à

Mettre en pratique les techniques d'intrusion les plus récentes sur les principales technologies du marché (systèmes d'exploitation, bases de données, applications Web, etc.)

Public visé

- Experts en sécurité, consultants ou auditeurs internes dont le rôle est de vérifier la sécurité des systèmes informatiques
- Administrateurs systèmes ou réseaux, chefs de projets, ou responsables sécurité souhaitant mieux appréhender les techniques d'attaque pour renforcer la sécurisation de leurs systèmes

Pré-requis*

- Avoir une expérience dans l'utilisation des systèmes Windows et UNIX/Linux
- Avoir une connaissance des principaux protocoles de la suite TCP/IP
- Avoir des connaissances dans l'administration de bases de données ainsi que dans le développement d'application Web est un plus

Méthode pédagogique

- Cours magistral
- Travaux pratiques
- Formation dispensée en français

Matériel

- Ordinateurs portables mis à disposition des stagiaires
- Supports papier en français

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Programme

- Introduction aux tests d'intrusion
- Présentation de l'architecture des travaux pratiques
- Méthodologie des tests d'intrusion
- Préparation et gestion d'un test d'intrusion
- Législation et déontologie

Découverte réseau et qualification des cibles

- Rappels TCP/IP
- Découverte/fuite d'information
- Analyse de l'environnement
- Génération de paquets
- Scan de port
- Présentation de Nessus

Attaque réseau

- Ecoute du réseau local
- Attaque des interfaces d'administration
- Attaque "Man-in-the- middle"/ARP spoofing
- Attaque des routeurs
- Tunneling

Sécurité WiFi

- Présentation des protocoles d'authentification
- Attaques Wi-Fi (e.g. De-Auth, faux access point / Man in the Middle, écoute et craquage d'un handshake).

Intrusion sur les applications web

- Infrastructure Web
- Rappels HTTP
- Prise d'empreinte
- Présentation des webshells
- Injection de code SQL, de commande, inclusion de fichier
- XSS et CSRF

Découverte des mots de passe

- Généralités
- Génération des empreintes
- Méthodes et outils de cassage d'empreinte

Utilisation de Metasploit

- Présentation du framework
- Méthodologie d'intrusion avec Metasploit
- Présentation de Meterpreter

Reconnaissance (OSINT)

- Identification des actifs exposés, nslookup, etc.
- Présentation d'outils utilisés pour la reconnaisance (TheHarverster, recon-ng)
- Présentation de Shodan
- Google Dorks
- Sécurité des boîtes mail / SMTP

Intrusion sur les bases de données

- Introduction et rappels SQL
- Intrusion MySQL
- Intrusion SQL Server
- Intrusion Oracle

Intrusion sur les systèmes Windows

- Identification machines et services
- Récupération d'informations à distance/ sessions nulles
- Récupération d'informations locales
- Authentification sous Windows et récupération des empreintes
- Attaque hors ligne
- Elévation de privilèges Intrusion sur les systèmes Unix/Linux
- Sécurité sous Unix/Linux
- "Sortir de la cage"
- Attaque par le réseau
- Attaque locale

5 jours / 35 heures	Réf. : INTRU1	3 600€ hors taxes	• 9 au 13 octobre

Essentiels techniques de la SSI

MANIKA

Formation théorique à la sécurité des systèmes d'information, ce cours apportera au personnel technique et aux chefs de projet une approche d'un système d'information sous l'angle des attaquants et donnera les bonnes pratiques pour sécuriser et maintenir un niveau de sécurité correct dans vos systèmes d'information. Connaître les principales attaques et les contre-mesures adéquates est devenu primordial pour toute entreprise utilisant l'informatique et les réseaux comme support de travail.

Vous allez apprendre à

- Identifier les points faibles des systèmes d'information
- Définir les règles de sécurité fondamentales pour sécuriser un périmètre
- Comprendre la portée des attaques informatiques

Public visé

- Personnel ayant besoin d'engranger de nouvelles connaissances en sécurité
- Administrateurs systèmes ou réseaux

Pré-requis*

Une connaissance informatique de base ainsi que des bases en réseaux TCP/IP

Méthode pédagogique

- Cours magistral
- Démonstrations

Matériel

- Supports au format papier en français

Certification

- Formation non certifiante

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Programme

Jour 1

Introduction
- Contexte, objectifs et enjeux
- Initiation au framework Metasploit

Risque impact et métiers
- Fuite d'information
- Atteinte à l'image
- Risques juridiques

Typologie des attaques, sources de menaces
- Cybercriminalité
- Espionnage

Sécurité : concepts fondamentaux
- inventaire et connaissance de son SI
- principes de moindre privilège et de défense en profondeur
- la détection : maillon indispensable

Rappels sur les réseaux IP
- Protocoles réseau (IP, TCP, UDP, ICMP, IPsec)
- Protocoles "lien" (Ethernet, ARP, 802.1X, LAN, VPN, MPLS)
- Exemple de protocole applicatif : HTTP
- scan de ports (nmap), Man-in-the-Middle (MitM)

Cryptographie
- chiffrement symétrique/asymétrique
- fonctions de hachage (ex : SHA512)
- protocole de transport TLS
- certificats et signature

Contrôle d'accès
- Gestion des utilisateurs (procédures arrivée/départ)
- Gestion des mots de passe (base de données de leak sur internet, politique de mot de passe, cassage par brute-force)
- Comptes privilégiés : securité spécifique

Jour 2

Sécurité des réseaux et firewalls (grands principes)
- Segmentation (vlans, routeurs, pare-feu, 802.1Q, vlan hopping, VPN)
- Filtrage (pare-feu, DMZ, proxy)
- Relayage applicatif
  - proxy et reverse proxy
  - attaques web courantes : SQLi et XSS
- Critères de choix d'une solution de sécurité

Sécurité des systèmes
- Principes de base (minimisation, réduction de surface d'attaque, antivirus, durcissement d'OS)
- Mise à jour (gestion de parc, WSUS, CVEs)
  - Veille en vulnérabilité
  - Gestion des vulnérabilités techniques
  - Risques spécifiques pour les navigateurs (plugins, addons, ActiveX, interpréteur, etc.)
- Journalisation (syslog, SIEM)
- Sauvegarde

Sécurité des applications web
- OWASP & TOP 10 OWASP (2021) - attaques classiques et retour d'expérience : injections SQL/LDAP, XSS, directory listing, IDOR, XXE, SSRF, etc.
- Stockage des mots de passe : bonnes pratiques de développement
- Intégration de la sécurité dans le développement

Conclusion

2 jours / 14 heures	Réf. : ESSI	1 400€ hors taxes	• 15 au 16 mai	• 13 au 14 novembre

Socle technique de la cybersécurité

Formation initiale à la sécurité des systèmes d'information, la SECU1 permettra d'apporter au personnel technique les connaissances nécessaires à l'implémentation et au maintien de la sécurité dans vos systèmes d'information.
Savoir implémenter les bonnes mesures de sécurité est devenu pour tout ingénieur ou administrateur système ou réseau un enjeu primordial permettant d'assurer la sécurité des SI.

Vous allez apprendre à

- Maîtriser le vocabulaire et la théorie de la sécurité de l'information
- Elaborer la sécurité des réseaux informatiques
- Capitaliser sur de nombreux concepts de défense
- Maîtriser la sécurité des systèmes d'exploitation et des applications

Public visé

- Personnel technique souhaitant se reconvertir dans la sécurité des systèmes d'information
- Administrateurs systèmes ou réseaux
- Professionnels de la sécurité

Pré-requis*

Une réelle connaissance informatique est nécessaire.

Méthode pédagogique

- Cours magistral
- Travaux pratiques

Matériel

- Ordinateurs portables mis à disposition des stagiaires
- Supports en français

Programme

Jour 1
Introduction
- Contexte
- Sources de menaces
- Anatomie d'une attaque
- Risques et impacts métiers
- Concepts fondamentaux

Rappels sur les réseaux IP
- Couches OSI
- Adressage
- ARP
- DNS

Equipements réseaux

Jour 2
Cryptographie
- Symétrique et modes, asymétrique : hashage, signature, VPN, PKI, TLS, PGP, IPSec
- Contrôle d'accès : gestion des utilisateurs, authentification et autorisation

Jour 3
Sécurité des réseaux
- Equipements réseau
- Segmentation
- Filtrage
- Relayage
- Architecture (ANSSI)

Gestion d'incidents
- Processus
- Veille
- Journalisation
- Investigation

Jour 4
Linux
- Système de fichiers
- Authentification et comptes utilisateurs
- Sécurisation des services
- Journalisation
- Pare-feu local
- Modules de sécurité

Windows
- Active directory
- PowerShell
- Scénarios d'attaques classiques
- Solutions pratiques
- Durcissement réseau

Jour 5
Sécurité des applications
- HTTP
- Gestion de l'authentification
- Gestion des cookies
- Gestion des sessions
- Présentation des principales attaques : SQLI, XSS, CSRF, Directory traversal, RCE, RFI/LFI

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

5 jours / 35 heures	Réf. : SECU1	3 600€ hors taxes	• 25 au 29 septembre

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Formation cybersécurité industrielle

Les systèmes industriels ne sont plus isolés, bien au contraire. Ils se retrouvent de plus en plus exposés, car digitalisés et connectés avec d'autres actifs informationnels, souvent du monde « IT » (ou bureautique), de l'organisation. Partant de ce constat, cette formation est conçue pour vous apporter les connaissances fondamentales s'agissant des enjeux, des vecteurs de risque, des vulnérabilités et des techniques et moyens afin de sécuriser les environnements industriels – également dits « OT ».

Objectifs

- Acquérir les notions fondamentales de la cybersécurité industrielle et des systèmes associés
- Pouvoir identifier les composants d'un écosystème d'automates de gestion et de contrôle, les protocoles et architectures OT courantes
- Comprendre les vulnérabilités majeures de cybersécurité industrielle, et les risques associés
- Pouvoir déterminer les risques inhérents à une architecture, solutions ou situations basées sur des contextes techniques ou organisationnels réels, par des exercices et travaux pratiques
- Pouvoir mettre en œuvre un programme de sécurité OT par le biais d'une méthodologie exhaustive et adaptée au contexte technique et organisationnel

Public visé

- RSSI
- Professionnel de la cybersécurité, des TI ou de la sécurité OT (consultant, expert, référent, etc.)
- Responsable des risques opérationnels
- Ingénieur ou utilisateur OT

Pré-requis*

Cette formation nécessite une connaissance générale de la sécurité des systèmes d'information. La connaissance des systèmes industriels n'est pas un pré-requis.

Méthode pédagogique

- Cours magistral, questions/réponses, cas d'usage

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Matériel

- Supports de cours et annexes éventuelles en anglais. La dispense se fait en français.

Examen/ Certification

Un examen de type QCM vous sera proposé lors de la 3e journée de formation. La réussite à cet examen donne droit à la certification **« Cybersécurité industrielle – Foundation » par Deloitte France.**

Programme

Jour 1

- Objectifs et structure du cours
- Principes et notions fondamentales des réseaux OT et de leur sécurité
- État de l'art de la sécurité OT
- Les protocoles et leurs vulnérabilités (S7, Modbus, DNPS, ICCP/TASE, etc.)
- Automates et IHM (systèmes d'exploitation Windows)
  - Services courants
  - Vulnérabilités rencontrées
  - Top 10 OWASP
  - Déni de service et résilience

Jour 2

- Les normes de sécurité applicables aux environnements industriels
  - IEC 62443-x
  - NIST SP800-82
- Les systèmes OT distants
  - VPN
  - Boîtiers de télétransmission
  - Sans-fil (Wifi, liaisons radio)
  - Exposition sur internet : risques et vulnérabilités
- Les architectures OT
- Sécurité organisationnelle d'un réseau OT
- Points sensibles, niveaux de classification ANSSI
- Organisation d'un programme de cybersécurité OT
- Mise en place d'un modèle opérationnel (organisation) pour la cybersécurité OT, interaction avec les organisations type RSSI/ groupe
- Approche par les risques, études d'impact métier du risque Cyber OT
- Exercices et travaux pratiques

Jour 3 – matin

- Révisions générales
- Passage de l'examen

2,5 jours / 17,5 heures	Réf. : INDUS	2 250 € hors taxes	• 22 au 24 mai	• 27 au 29 novembre

Architectures réseaux sécurisées

MANIKA

Wi-Fi, Cloud, BYOD, IoT. Derrière chacune de ces vagues marketing successives, il y a des choix de conception à faire. Des choix qui doivent tenir compte des nouvelles possibilités et des contraintes spécifiques à ces technologies. Les concepteurs sont confrontés aux problématiques d'authentification et de gestion des accès utilisateurs, de résilience de l'infrastructure et de son maintien.

Vous allez apprendre à

- Les caractéristiques d'une architecture sécurisée et comment les prendre en compte dans le cadre d'architectures spécifiques
- A sécuriser les architectures communément mises en œuvre dans les entreprises
- A évaluer la sécurité d'une architecture donnée
- A identifier les choix structurant l'architecture de vos prochaines solutions
- A prendre en compte la sécurité dans les choix d'architecture et connaître les points d'attention qui y sont liés

Public visé

- Toutes les personnes confrontées à la sécurité des architectures des systèmes d'information : architectes des réseaux, architectes applicatifs, chefs de projets informatiques, responsables informatique ou sécurité, équipes informatique ou sécurité, consultants et auditeurs techniques ou de SMSI, gestionnaires de risques

Pré-requis*

- Avoir une culture générale en informatique avec une connaissance de base des réseaux et du fonctionnement des TCP/IP
- Disposer d'un ordinateur pouvant accéder à Google Form pour le test de connaissances final

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques sur la conception et l'évaluation d'architectures

Matériel

- Supports intégralement en français

Certification

- Cette formation prépare à l'examen de certification SECARC. Toutes les questions de l'examen sont issues des supports de cours de la formation. L'examen se déroule le dernier jour de la formation.

En partenariat avec Manika

Programme

Introduction

Principes de sécurisation, éléments sensibles, objectifs de sécurité

Architecture d'administration et d'authentification

- Protocoles d'administration et usages : RDP, WinRM, SSH, VNC
- Authentification centralisée : LDAP, NTLM, RADIUS, Kerberos
- Référentiels centralisés : OpenLDAP, Active Directory
- Authentification forte : principes, OAuth, U2F, ActivCard
- Administrateurs et services : Forêts, LAPS, bastions

Réseaux et segmentation

- IPv4, IPv6
- Composants : concentrateur, pare-feu, diode, NIDS/NIPS...
- Segmentation physique : ports RJ45 et consoles, 802.1x
- Segmentation réseau, découpage vertical : VLAN, 802.1Q, VxLAN, VRF, PVLAN
- Routage : statique vs dynamique, OSPF, RIPE, BGP, BATMAN
- Filtrage : règles fondamentales, matrice de flux, local vs central
- Software-defined network
- Relais applicatifs et inverses

Architecture générale

- Systèmes autonomes
- Segmentation horizontale et administration "out-of-band"
- Positionnement des éléments de sécurité

Connexion distante

Connexion à distance et interconnexion multi-sites : MPLS, VPN IPSec, TLS

Postes de travail

Virtualisation, VDI, BYOD vs. COPE

Architecture Windows

Architecture de domaines, DC et RODC, approbation et délégation

Architectures applicatives

- Accès Internet
- Architectures 2-tiers, 3-tiers ; requêtes RPC
- Stockage : SAN, NAS, partages réseaux SMB, NFS

Architecture des fonctions d'infrastructure et de sécurité

- DHCP et usage
- DNS : interne, public, DNSSEC
- SMTP : émission interne, réception
- Journalisation et SIEM / supervision
- Mise à jour ; configuration et déploiement : GPO, Puppet, Ansible
- Cryptographie : PKI, authentification des serveurs, CRL vs OCSP, HSM

Continuité et haute disponibilité

- Notion de SPOF
- Réseau : agrégation, clusters, adresses IP virtuelles, boucles
- Equipements simples : répartition de charge, réplication de données
- Sauvegarde
- Continuité d'activité : interdépendance des composants, infrastructure de crise, architectures temporaires, reprise et bascule

Réaliser des choix d'architecture

- Loi et réglementation : classifié défense, PDIS, LPM et SIIV, PCI DSS
- Cloud : IAAS / PAAS / SAAS et intégration à l'architecture existante
- Virtualisation
- Existant et rétro-compatibilité
- Utilisation de cadriciels

Architectures spécifiques

- Environnements (hors) production
- Imprimantes et scanneurs
- Audio (VoIP) et vidéo
- Interconnexion filiales / partenaires
- Infrastructure virtuelle
- Réseaux wi-fi
- Réseaux libre-service
- Architectures industrielles
- IoT ; appareils mobiles
- Grid, architectures n-tiers, distribuées : Hadoop, P2P
- Mainframes / Sécurité physique
- Exploration des limites du cloisonnement

Examen

3 jours / 21 heures	Réf. : SECARC	2 250€ hors taxes	• 13 au 15 mars	• 18 au 20 septembre

Investigation numérique réseaux

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

Public visé

- Administrateur, analyste SOC, ingénieur sécurité

Pré-requis*

- Connaissance sur l'OS Windows, TCP/IP, Linux

Programme

Jour 1

Section 1 - Introduction à la cybersécurité
- La "cybersécurité" d'avant
- Présentation du programme Creeper
- Présentation du projet Rabbit
- La cybersécurité d'aujourd'hui et ses risques (Wannacry, Stuxnet)
- La dangerosité des données numériques
- Qui sont les responsables ? quelles motivations ont-ils?
- Classification des risques selon le gouvernement français

Section 2 - Le monde de l'investigation
- Introduction et approche du forensique
- Présentation de la timeline historique
- Les objectifs en infosec
- Définition et étymologie du terme
- Présentations des dérivés de la discipline
- Les organismes référents en la matière, tels que l'ENISA et le SANS
- Présentation des cinq principes fondamentaux
- Définition de la méthodologie OSCAR
- Liaisons avec le computer forensic
- Liaisons avec le memory forensic
- Liaisons avec le mobil forensic

Section 3 - Enregistrement et surveillance
- Sources utiles d'analyse basées sur l'hôte
- Sources utiles d'analyse basées sur le réseau
- La technologie SIEM (SEM / SIM)

Section 4 - Les différents types de données
- Définitions des données volatiles et non volatiles
- Les données complètes
- Les données de session
- Les données d'alerte
- Les Métadonnées

Section 5 - Acquisition des preuves et sondes
- Approche légale
- Les différents types d'acquisitions
- Les acquisitions par câble et les sondes
- Les acquisitions sans fil et les modes de capture
- Les acquisitions offensives

Section 6 - Rappel des bases réseau
- Rappels sur le modèle OSI
- Rappels sur le modèle TCP/IP
- Les différents matériels réseau
- Définitions et exemples d' IPS / IDS / WIDS
- Rappels sur les protocoles DHCP, DNS, ARP, HTTP / HTTPS

Section 7 - Présentation des outils connus
- Les outils de capture de paquets, tels que TCPDump / Dumpcap
- SIEM : Détection prévention d'intrusion tel que AlienVault
- Les analyseurs de flux, tels que Argus
- Network Incident Detection System, tel que Snort
- Les outils d'analyse à grande échelle, tels que Moloch et Wireshark

Section 8 - TD / WireShark
- Présentation de l'interface de Wireshark
- Les différentes options de capture
- Présentation de la barre d'outil Wireshark
- Les règles de coloration sous Wireshark
- Exercice / Créer ses propres règles de coloration
- Les filtres d'affichage
- Exercice / créer ses propres filtres rapides
- Les profils sous wireshark
- Exercice / créer de profils adaptés aux besoins
- Effectuer des recherches avancées
- Les filtres de capture
- Les filtres Berkeley Packets Filter
- Les boutons raccourcis de Wireshark
- Exercice / Créer ses propres boutons
- Export des données et enregistrement de fichier
- Le bouton de pré-analyse WireShark
- Utilisation des statistiques

Jour 2

Section 9 - TD / Mise en pratique
- Exercice / Prise en main Wireshark
- Exercice / Lancement des investigations (TP1, TP2)

Section 10 - Le rapport d'investigation
- Comprendre le déroulé d'une attaque avec le MITRE - ATT&CK
- Rédaction du contexte
- Création de schéma de la typologie réseau
- Présentation des preuves et hash d'intégrité
- Rédaction des processus d'analyse
- Edition de la timeline des événements
- Rédaction de la conclusion
- Émettre des recommandations

Section 11 - TP / Analyse réseau
- Identifier une erreur de type ARP Storm
- Identifier une attaque DHCP Starvation
- Identifier une attaque ARP spoofing
- Identifier un Scan réseau
- Identifier une exfiltration de données
- Identifier un téléchargement via torrent

Jour 3

Section 12 - Cas réels d'entreprise TP
- Etude de cas réels d'entreprise
- Analyse de captures réseau
- Utilisations des outils, méthodes et techniques
- Rédaction d'un rapport forensique en réponse aux problèmes posés

Section 13 - TD / Installation / Utilisation et détection via SIEM
- Mise en place du LAB ;
- Installation de AlienVault ;
- Configuration de l'OSSIM ;
- Détection / configuration des hôtes ;
- Mise en place d'agents sur les clients ;
- Détection de vulnérabilités ;
- Détection d'une attaque par exploit
- Examen pour l'obtention d'un badge ESD academy (https://badges.esdacademy.eu)

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

3 jours / 21 heures

Réf. : INVRES

1 980€ hors taxes

• 17 au 19 avril

• 16 au 18 octobre

Investigation numérique Windows

L'objectif pédagogique est d'acquérir les compétences et la méthodologie pour une investigation numérique sur le système d'exploitation Windows. La méthodologie et l'étude des différents artefacts sont développées et mises à jour régulièrement afin que le candidat puisse pratiquer ce qu'il a vu en formation sur les dernières versions des systèmes Windows.

Public visé

- Administrateur
- Analyste SOC
- Ingénieur sécurité

Pré-requis*

- Avoir des connaissances sur les OS Windows, TCP/IP, Linux

Programme

Jour 1

Section 1 – Etat de l'art de l'investigation numérique

- Objectif du cours
- Introduction à l'investigation numérique
- Lien entre les différentes disciplines Forensics
- Méthodologie d'investigation légale (Chaîne de custody, Chaîne des évidences)
- Présentation du framework ATT & CK du MITRE et points d'entrée des Cyberattaques
- Arbres d'attaque
- Les signes de compromissions (Corrélation ATT&CK)
- Vocabulaire, taxonomie
- Les différents OS Windows

Section 2 – Les fondamentaux Windows

- Fondamentaux Windows
  - Système de fichiers / Arborescence
  - Séquence de boot Windows
  - Base de registre
  - Logs (evtx, log pilotes, etc.)
  - Variables d'environnements
- Services et les différents accès (services.exe, Powershell)
- Fondamentaux FAT32
- Fondamentaux NTFS
- TD 1 / Analyse d'un disque
- TP 1 / Analyse d'un disque
- TP2 / Questionnaire de connaissance

Section 3 – Collecte des données

- Les outils du marché (Kape, Arsenal, FTKimager, Plaso,Hindsight..)
- Collecte des données physiques et virtualisation
- Présentation du Lab
- TD / Collecte de données (En continu)

Jour 2

Section 4 – Artefacts

- Différents artefacts internet
  - Pièces jointes
  - Open/Save MRU
  - Flux ADS Zone.Identifier
  - Téléchargements
  - Historique Skype
  - Navigateurs internet
  - Historique
  - Cache
  - Sessions restaurées
  - Cookies
- Différents artefacts exécution
  - UserAssist
  - Timeline Windows 10
  - RecentApps
  - Shimcache
  - Jumplist
  - Amcache.hve
  - BAM/DAM
  - Last-Visited MRU
  - Prefetch
- Différents artefacts fichiers/dossiers
  - Shellbags
  - Fichiers récents
  - Raccourcis (LNK)
  - Documents Office
  - IE/Edge Files
- Différents artefacts réseau
  - Termes recherchés sur navigateur
  - Cookie
  - Historique
  - SRUM (ressource usage monitor)
  - Log wifi
- Différents artefacts comptes utilisateur
  - Dernières connexions
  - Changement de mot de passe
  - Echec/Réussite d'authentification
  - Évènement de service (démarrage)
  - Evènement d'authentification
  - Type d'authentification
  - Utilisation du RDP
- Différents artefacts USB
  - Nomination des volumes
  - Evénement PnP (Plug & Play)
  - Numéros de série
- Différents artefacts fichiers supprimés tools
  - Récupération de la corbeille
  - Thumbcache
  - Thumb.db
  - WordWheelQuery
- Spécificités Active Directory
- TP 3 / Première investigation

Jour 3

Section 5 – Techniques avancées

- VSS
- Carving
- Anti-forensic et Timestomping
- TP 4 / Deuxième investigation

Section 6 – Introduction à volatility

- Données volatiles
- Analyse d'un dump mémoire
- Extraction et analyse des process
- TP / Recherche d'un malware à l'aide de Volatility

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

3 jours / 21 heures

Réf. : INVWIN

1 980€ hors taxes

- 12 au 14 juin
- 27 au 29 novembre

Analyste SOC (Security Operation Center)

Aujourd'hui, les utilisateurs sont de plus en plus mobiles et un grand nombre d'applications et de données migrent vers le Cloud, ce qui a pour effet d'exposer davantage les ressources IT aux différentes menaces. Les entreprises ont donc besoin d'un dispositif de contrôle de la sécurité des données dans le Cloud comme sur site et de personnels aptes à le gérer.

Vous allez apprendre à

- Décrire l'état de l'art du SOC (Security Operation Center)
- Répondre aux besoins des enjeux liés à la cybersécurité et des menaces par le métier d'analyste SOC

Public visé

- Consultant en cybersécurité
- Administrateur système
- Ingénieur en informatique
- Développeur

Pré-requis*

- Avoir des bases de la sécurité des systèmes d'information
- Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell

Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques
- Evaluation des acquis en continu

Matériel

Supports intégralement en français

Programme

Jour 1 : SOC et métier d'analyste
Section 1 – Etat de l'art du Security Operation Center

- Définition du SOC
- Les avantages, l'évolution du SOC
- Les services intégrés au SOC, les données collectées, playbook
- Le modèle de gouvernance du SOC (approche SSI, type de SOC, CERT, CSIRT)
- Pré-requis et rôles d'un analyste SOC (techniques, soft skills, rôles, modèles)

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

- Les référentiels (ATT&CK, DeTT&CT, Sigma, MISP)
- Démonstration 1 – utilisation du framework ATT & CK via Navigator (attaque et défense)

Section 2 – Focus sur l'analyste SOC

- Quel travail au quotidien
- Triage des alertes
- Révision et état de sécurité
- Identification et rapport
- Threat hunting
- Démonstration 2 – utilisation de l'outil SYSMON

Section 3 – Les sources de données à monitorer

- Indicateur Windows (processus, firewall, etc.)
- Service WEB (serveur, WAF, activité)
- IDS/IPS
- EDR, XDR
- USB
- DHCP, DNS
- Antivirus, EPP
- DLP, whitelist
- Email
- Exercice 1 / cas d'usage et ligne de défense

Jour 2 : Découverte & mise en place du SIEM
Section 4 – Tour d'horizon du SIEM

- Contexte du SIEM
- Solution existante
- Principe de fonctionnement d'un SIEM
- Les objectifs d'un SIEM
- Solution de SIEM

Section 5 – Présentation de la suite Elastic

- Les agents BEATS, sysmon
- Découverte de Logstash
- Découverte de Elasticsearch
- Découverte de Kibana
- TP 1 / mise en place d'ELK et première remontée de log

Jour 3 : (Analyse, Logstash, Elastic search)
Section 6 – Logstash (ETL)

- Fonctionnement de Logstash
- Les fichiers input & output
- Enrichissement : Les filtres Groks et sources externes

Section 7 – ElasticSearch

- Terminologie
- Syntax Lucene
- Alerte avec ElasticAlert et Sigma
- TP 2 / création d'alertes, alarmes
- Démonstration 3 / utilisation d'Elastalert et Sigmac

Section 8 – Kibana

- Recherche d'événements
- Visualisation des données
- Démonstration 4 / création d'un filtre sur Kibana
- Ajout de règles de détection, IoC
- Allez plus loin dans l'architecture ELK avec HELK

Jour 4 : Cyber entraînement
Section 9 – Mise en situation

À travers des outils ESD Academy, l'analyste SOC est en situation et doit identifier plusieurs scénarios d'attaque lancés par le formateur

- TP 3 / Configurer un SIEM et l'exploiter

Jour 5 : Rapport
Section 10 – Rapport

l'analyste SOC doit rapporter les attaques détectées et identifier les menaces, impacts, vérifier si son système d'information est touché.

- TP 4 / Créer un rapport des attaques interceptées et évaluer l'impact

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

5 jours / 35 heures

Réf. : SOC

3 750€ hors taxes

- 23 au 27 janvier
- 24 au 28 avril
- 24 au 28 juillet
- 23 au 27 octobre

Sécurité des serveurs et applications web

MANIKA

Les applications web constituent le point le plus vulnérable au sein des entreprises. Il n'est pas rare que des failles de sécurité donnent lieu, par exemple, à des vols de millions de numéros de cartes de crédit, à des dommages financiers, à d'importants impacts sur l'image, voire même à la compromission de milliers de machines d'internautes consultant le site web piraté. Cette formation présente les vulnérabilités classiques du Web à travers les tests d'intrusion et les moyens d'y remédier.

Vous allez apprendre à

- Les enjeux de la sécurité web
- Les méthodes d'attaque sur le web et comment s'en protéger
- Les bases de la cryptographie, quand et comment l'utiliser
- Les méthodes d'authentification web
- Les bonnes pratiques de développement sécurisé
- Les techniques de protection des serveurs

Public visé

- Développeur web
- Architecte d'application web ou de solutions de sécurité web (pare-feu applicatif...)
- Administrateur systèmes
- Pentester débutant

Pré-requis*

- Avoir une expérience dans le développement web ou des connaissances en réseaux et systèmes sont un plus

Méthode pédagogique

- Cours magistral illustré et approfondi par des travaux pratiques. Formation dispensée en français

Matériel

- Supports de cours papier en français

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECWEB Deloitte Cyber Academy.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Programme

Introduction

- La sécurité informatique
- Cadre normatif et législatif
- Les différents types de menace et leurs évolutions
- Comprendre l'attaquant pour mieux se protéger

L'infrastructure web

- Architecture matérielle
- Architecture applicative
- Découverte de l'environnement

Travaux pratiques : collecte d'information, scan réseau, transfert de zone, protection

Les protocoles du web

- Le protocole HTTP :
  - Les méthodes de base
  - Les entêtes
  - Cookie et session
  - Les failles du HTTP
- Les autres protocoles sur HTTP

Travaux pratiques : Proxy, exploitation d'un analyseur de réseau, configuration d'entêtes, attaques sur sessions

Sécurisation des données et des flux

- Eléments de cryptographie
- Chiffrement des flux de données
- Signature électronique, certificats
- Chiffrement des données

Travaux pratiques : récupération de mots de passes

L'authentification

- Méthodes d'authentification http :
  - Basic
  - Digest
  - Formulaire HTML
- Méthodes d'authentification forte :
  - Token PKI
  - Certificat
  - Autres méthodes
- Modèles de délégation
- Principes d'infrastructure Single Sign On

Les applications Web

- Les attaques par injection :
  - Côté serveur (Commandes, LDAP, SQL...)
  - Côté client (XSS)
- Les attaques par inclusion :
  - Inclusions de fichiers locaux
  - Inclusions de fichiers distants
- Durcissement des serveurs et des OS :
  - Principes généraux sous Windows
  - Principes généraux sous Linux
- Développement sécurisé

Travaux pratiques : configuration d'un serveur web, attaques courantes et contremesures

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

5 jours / 35 heures	Réf. : SECWEB	3 600€ hors taxes	• 23 au 27 octobre

Durcissement sécurité Windows

Le durcissement des infrastructures Microsoft Windows est indispensable à la protection des systèmes d'information. Cette formation aborde la configuration des services Windows pour la sécurité et les différentes bonnes pratiques à adopter.

Public visé

- Consultant en cybersécurité
- Administrateur système
- Ingénieur en informatique
- Développeur

Pré-requis*

- Avoir des bases de la sécurité des systèmes d'information
- Connaître le fonctionnement d'un des systèmes Windows et Linux ainsi que les langages Shell

Programme

Jour 1

Section 1 – Introduction sur l'écosystème actuel

- L'évolution des systèmes d'information et de leurs menaces
- Segmentation et études des phases d'un attaquant (CyberKill Chain & MITRE ATT&CK)
- Chronologie et évolutions majeures des systèmes d'exploitation Windows
- Les attaques courantes dans un domaine Windows
- TP 1 / Mener une étude Cyber Kill-Chain

Section 2 – Durcissement des domaines Windows

- Cohérence et défauts de conception Active Directory (AGDLP, GPO, Relations approbations, délégation)
- Sécurité des droits d'administrations (ACL, Red Forest ESAE, Silo, Bastion, délégation)
- Sécurité des comptes à privilèges (AdminSDHolder, LAPS, PAM)
- Utilisation d'une infrastructure de clés publiques PKI (NPS, Radius, WIFI, carte à puce...)
- Sécurisation des protocoles d'administration (RPC, WMI, WinRM)
- Sécurité des services et comptes de services managés
- TP 2 / Implémenter LAPS

Jour 2

- Système de prévention de perte de données (Classification, Marquage, DLP)
- Surveillance et journaux d'événements (Surveillance en profondeur, Sysmon)
- Microsoft ATA et Threat Intelligence
- TP 3 /Appliquer les règles de classification et de surveillance sur des données confidentielles
- TP 4 / Renforcer la journalisation (Sysmon + Journalisation WMI pivoting)

Section 3 – Durcissement des serveurs et postes clients

- Sécurisation du démarrage (UEFI, Bitlocker, ...)
- Sécurité des applications (Applocker, Device Guard)
- Sécurité de l'authentification (SSP, credential guard)
- Contrôler l'élévation de privilèges (UAC)
- Fonctionnalité antivirale (Defender, AMSI, SmartScreen)
- Sécurité de Powershell (Politique de restriction, JEA, Journalisation)
- Réduction de la surface d'attaque (Serveur Core / Nano)
- TP 5 / Déployer Bitlocker
- TP 6 / Configurer powershell JEA

Jour 3

Section 4 – Durcissement des protocoles réseaux

- L'authentification Microsoft (NTLM, NET-NTLM, Kerberos)
- Les protocoles microsoft (WPAD, SMB, RDP, LLMNR...)
- Etude et recherche de vulnérabilités protocolaires
- TP 7 / Sécuriser LLMNR & SMB Introduction sur l'écosystème actuel

Section 5 – Mécanisme de défense avancé

- Détection des attaques avancées
- Auditer son architecture
- TP 8 / Auditer son architecture et préparer un plan de contre mesure

Jour 4

Section 6 – Durcissement des domaines Azure

- Rappel sur Azure et IAM
- Authentification et autorisation Azure
- Zoom sur les attaques Azure
- Renforcement des défenses Azure
- Auditer son architecture cloud

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

4 jours / 28 heures

Réf. : SECWIN

2 400€ hors taxes

- 30 janvier au 2 février
- 26 au 29 juin
- 11 au 14 septembre
- 6 au 9 novembre

Développement sécurisé

Chaque année, des vulnérabilités logicielles sont exploitées par des attaquants. Les logiciels sont au cœur de nos systèmes informatiques et sont une cible de choix. Il est possible d'éviter de nombreuses vulnérabilités en adoptant de bons réflexes de développement sécurisé.

Vous allez apprendre à

- Comprendre les différentes vulnérabilités web et applicatives utilisées par les attaquants
- Connaitre les outils de développement sécurisé
- Acquérir les bonnes pratiques de développement d'application pour développer de façon sécurisée

Public visé

- Développeurs
- Équipes informatique ou sécurité
- Chefs de projet
- Consultants
- Gestionnaires de risques

Pré-requis*

- Avoir une culture générale en informatique
- Connaitre un langage de programmation

Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques sur le développement d'applications sécurisées

Matériel

- Supports intégralement en français

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

Programme

Introduction aux enjeux de la sécurité logicielle

- Définition de la cybersécurité
- Analyse d'attaques récentes et de leurs conséquences
- Le logiciel : vecteur d'attaque
- Concepts de sécurité : confidentialité, intégrité et disponibilité, sécurité par défaut, défense en profondeur…
- Les acteurs de la sécurité des développements logiciels
- Les standards de la sécurité en développement logiciel

Les pratiques recommandées

- La formation à la sécurité des personnes
- L'analyse de risques intégrée dans un cycle de développement
- Les spécifications des exigences de sécurité liées aux spécifications du logiciel
- Les choix de design du logiciel
- L'implémentation du logiciel
- La vérification : l'importance du test dans le développement et la maintenance
- Le déploiement sécurisé des applications
- Protéger la confidentialité des échanges : introduction au chiffrement

Les principales failles de sécurité et contre-mesures

- Classement du MITRE CWE/SANS des erreurs logicielles les plus dangereuses
- Les principales sources de vulnérabilités : gestion des entrées/sorties (chaines de caractères, fichiers, entiers)
- Cas pratiques : analyse de codes vulnérables, exploitation et application de correctifs :
  - attaques de type injection ;
  - inclusion de fichiers arbitraires ;
  - injection de contenu dans une page ;
  - exploitation de fonctionnalités dangereuses ;
  - attaques sur une authentification non sécurisée ;
  - attaques exploitant le parsing XML ;
  - attaques basées sur le temps (« timing attacks ») ;
  - attaques cryptographiques ;
  - attaques exploitant les dépendances d'un projet.

Les pratiques de développement

- Tests lors du développement
- La pratique des tests d'intrusion
- Les tests statiques et dynamiques
- Audit de code
- Cas pratique : déroulé de tests
- Les outils existants intégrables dans une chaine de développement (DevSecOps)

3 jours / 21 heures	Réf. : DEVSEC	2 150€ HT	• 11 au 13 avril	• 2 au 4 octobre

Sécurité Active Directory

L'annuaire Active Directory est un élément critique permettant la gestion centralisée d'un parc Windows. Les annuaires Active Directory sont une cible de choix pour les attaquants, car leur compromission entraîne la prise de contrôle complète de tous les systèmes Windows ainsi administrés. Cette formation permet de comprendre les principaux modes opératoires des attaquants, de s'en protéger et d'administrer de façon sécurisée un Active Directory.

Vous allez apprendre à

- Comprendre les différentes vulnérabilités exploitées par les attaquants
- Détecter et corriger les vulnérabilités liées à l'Active Directory
- Connaitre les outils et architectures permettant une administration sécurisée
- Acquérir les bonnes pratiques d'administration sécurisé

Public visé

- Administrateurs système
- Équipes informatique ou sécurité
- Auditeurs techniques
- Consultants

Pré-requis*

- Avoir une expérience dans l'utilisation des systèmes Windows
- Connaissances générales en système et réseau

Méthode pédagogique

- Cours magistral
- Travaux pratiques
- Formation dispensée en français

Matériel

- Supports intégralement en français

Programme

Architecture Active Directory

- Structure d'un AD
- Les principaux services
- Relations d'approbation
- Naming Context LDAP
- Niveaux fonctionnels
- Utilisateurs et groupes
- Authentification
- Gestion des mots de passe
- Déploiement d'une politique de sécurité (GPO)

Les points de contrôle sécurité Active Directory

- Définition
- Classement de l'ANSSI des points de contrôle les plus importants
- Les outils existants
- Cas pratiques : identification, exploitation et correction des principales vulnérabilités d'un Active Directory :
  - membres de groupes à privilèges ;
  - droits sur des comptes privilégiés ;
  - droits sur des comptes de DC ;
  - droits sur des GPO ;
  - droits sur des templates de certificats ;
  - délégations Kerberos ;
  - absence de pré-authentification Kerberos (AS-REP Roasting) ;
  - comptes avec SPN (Kerberoasting).
- Backdoors (post-compromission) d'un attaquant :
  - Golden ticket ;
  - rebond vers d'autres domaines via une relation d'approbation.

Modèle d'administration sécurisé

- Les principaux risques :
  - mise en cache des authentifiants Windows ;
  - faiblesses de NTLM ;
  - pass-the-hash / pass-the-ticket.
- Atelier de réflexion sur les mesures de protection à mettre en œuvre
- Le modèle d'administration en Tiers
  - architecture du Tiers 0 : la « pierre angulaire » d'un Active Directory ;
  - la PAW, station d'administration sécurisée ;
  - les serveurs du Tiers 0 ;
  - les autres Tiers.
- Mesures de sécurité permettant la mise en place du modèle en Tiers :
  - Kerberos Armoring ;
  - politiques d'authentification et silos ;
  - RDP Restricted admin ;
  - délégations d'administration pour les Tiers 1 et 2.

** L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandé(s). Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.*

4 jours / 27 heures	Réf. : SECUAD	2 850€ HT	• 19 au 22 juin	• 11 au 14 décembre

Vous souhaitez **sensibiliser** vos collaborateurs aux bonnes pratiques de **cybersécurité** ? Nos **experts** développent pour vous des **parcours** de sensibilisation **sur-mesure**.

L'équipe Deloitte Cyber Academy vous accompagne dans la co-construction d'un plan de sensibilisation adapté à votre contexte, à la maturité de vos employés et à votre exposition aux différents risques cyber en mettant à votre disposition un ensemble d'outils d'apprentissage (micro-learning, e-learning, jeux, etc.).

Pour tout renseignement, contactez notre équipe à l'adresse suivante : formations-cyber@deloitte.fr.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Notre approche de la sensibilisation

Rendre l'humain maillon fort de la chaîne de sécurité

01

Le risque cyber est présent en permanence, auprès de tous

- La digitalisation grandissante de notre environnement implique un nombre croissant de vulnérabilités.
- L'évolution rapide des menaces cyber devance la maturité des usagers, engendrant un risque pour l'entreprise et ses tiers.

02

La sensibilisation de tous les acteurs est primordiale

- Toutes les populations d'une entreprise doivent être sensibilisées aux enjeux cyber actuels.
- Nos sensibilisations s'adaptent en fond et forme aux différents publics afin de garantir l'application des bonnes pratiques de cybersécurité.

03

Une sensibilisation peut être construite sur-mesure

- Nous proposons des plans de sensibilisation que nous adaptons au contexte de votre entreprise.
- Nos actions de sensibilisation s'intègrent dans des plans de montée en sécurité globale de votre entreprise.

Deloitte Cyber Academy s'engage à travailler conjointement avec vous pour construire un plan de sensibilisation adapté à votre besoin et à vos contraintes.

Nos actions s'appuient sur des outils d'apprentissage tels que la gamification, des e-learnings, etc. afin de capter l'intérêt du plus grand nombre, de faire intégrer les bonnes pratiques et ainsi de garantir le meilleur niveau de sécurité pour votre organisation.

Introduction à la cybersécurité

L'interconnexion de notre monde actuel représente une menace constante pour les entreprises et leurs employés. Quand plus de 60% des attaques sont dues à une erreur humaine, les collaborateurs doivent être considérés comme un facteur de risque majeur.
Il apparait donc primordial de les sensibiliser aux bonnes pratiques d'hygiène informatique.

Vous allez apprendre à

- Développer une vision globale de la cybersécurité, de sa définition à son évolution récente, des enjeux de la SSI avec des exemples d'incidents parlants.
- Découvrir les attaques les plus répandues (social engineering, malware, etc.) ainsi que les bonnes pratiques à adopter pour y faire face.
- Contrôler le niveau de maturité de la sécurité IT d'une entreprise.
- Obtenir des connaissances fondamentales sur l'ensemble de la cybersécurité.

Méthode pédagogique :

- Cours magistral
- Démonstrations

Matériel :

- Support de cours au format pdf en français

Public visé :

- Tout public

Les objectifs du client :

- **Objectif 1** : Connaitre les principaux risques informatiques ou a minima financier avec des exemples d'incidents parlants
- **Objectif 2** : Connaitre la réglementation en matière de sécurité IT
- **Objectif 3** : Connaitre les bonnes pratiques en matière de sécurité IT : gouvernance, organisation, dispositif de contrôle permanent, outils
- **Objectif 4** : Disposer des principaux tests d'audit permettant de contrôler le niveau de maturité de la sécurité IT d'une entreprise

Programme :

- Introduction à la cybersécurité
- Les risques qui pèsent sur les organisations,
- Cyber menaces, arnaques et dangers sur le réseau
- Bonnes pratiques en matière de sécurité : gouvernance, organisation, dispositif de contrôle permanent, outils
- Démonstrations et exemples d'attaques
- Focus audit et contrôle interne IT : présentation des méthodes, outils et techniques modernes de contrôle de maturité sécurité
- Conclusion

1h à 2h	Réf. : INTROCYBER	Sur demande	Sur demande

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Sensibilisation à la gestion de crise

La question aujourd'hui n'est plus de savoir si votre entreprise fera face à une crise cyber mais bien quand cette dernière aura lieu et comment y faire face. Les dirigeants et collaborateurs doivent donc être capables de comprendre les enjeux de cybersécurité auxquels fait face l'entreprise pour mettre en place un nombre de mesures permettant de se prémunir de la meilleure manière possible.
La première étape de ce processus passe par la sensibilisation des employés aux dangers d'une crise et quel comportement adopter.

Vous serez sensibilisé sur :

- Les évolutions des types d'attaques et attaquants
- L'identification d'une période de crise et le déclenchement du plan de gestion de crise
- L'organisation d'une entreprise en période de crise
- La communication particulière à adopter en temps de crise

Public visé

- Tous les employés
- Dirigeants d'entreprises
- Membres du COMEX
- Membres du CODIR
- Collaborateurs

Méthode pédagogique

- Intervention d'un ou plusieurs expert(s)
- Retours d'expériences
- Questions – réponses

Matériel

- Slides de présentation

Programme

- Les enjeux de la crise cyber
- Typologie des attaques et des différentes crises cyber
- Constitution d'une cellule de crise
- Communication de crise : méthodologie et processus de communication en cas de crise cyber et études de cas des do's and don't
- Attractivité et vulnérabilité associées au secteur du client (études de cas et échanges : mise en situation « et si vous étiez face à la crise ? »)

Remarque : le programme peut s'adapter en 2h, 4h ou plus, en fonction des exigences du client. L'exhaustivité de chaque sujet sera donc adaptée.

2h ou 4h	Réf. : CRISE	Sur demande	Sur demande

Sensibilisation du COMEX

La cybersécurité est devenue un enjeu majeur pour toutes les entreprises et doit faire partie intégrante de la stratégie globale de l'entreprise. Les dirigeants et collaborateurs du C-level doivent donc être en mesure de comprendre les enjeux de cybersécurité auxquels fait face l'entreprise et leur sensibilisation est donc essentielle. Ce programme vous permettra de développer une vision d'ensemble de l'environnement cyber et de prendre des décisions en conséquence.

Vous serez sensibilisé sur :

- Les enjeux cyber actuels et les principaux acteurs du domaine
- Les principaux risques et les différents types d'attaques cyber
- L'organisation de la cybersécurité au sein d'une entreprise
- Les évolutions de la cybersécurité

Public visé

- Dirigeants d'entreprises
- Membres du COMEX
- Membres du CODIR

Méthode pédagogique

- Intervention d'un ou plusieurs expert(s)
- Retours d'expériences
- Questions – réponses

Matériel

- Slides de présentation

Programme

- Introduction au Cyberespace
- Risque = menaces * vulnérabilité * impact
- Au-delà des attaques et des attaquants
- Articuler gouvernance et implémentation
- Les menaces cyber de demain
- Q&A – construire vos solutions

1h à 2h	Réf. : C-LEVEL	Sur demande	Sur demande

Campagne de phishing

Le phishing (ou hameçonnage) est un des premiers vecteurs d'attaque privilégiés des pirates informatiques. D'après le rapport « State of the Phish » 2020 de ProofPoint, 88% des organisations interrogées ont subi des attaques de phishing ciblé en 2019. Or, d'après le même rapport, l'intelligence humaine est la meilleure défense contre ce type d'attaque. C'est pourquoi il est nécessaire de sensibiliser vos collaborateurs aux conséquences liées à une attaque de phishing et aux bonnes pratiques pour identifier les mails d'hameçonnage et contrer ces risques.

Points clés d'une campagne de phishing

- Sensibilisation des collaborateurs
- Simulation en conditions réelles
- Attaque ciblée
- Modèle de courriel et formulaire réaliste
- Surveillance de la campagne
- Statistiques de la campagne

Nos outils

- Une plateforme dédiée répondant au critère de la norme ISO 27001
- Une communication chiffrée entre le client et notre plateforme
- Des courriels et formulaires types adaptables si souhaité
- Agrégation des résultats
- Une interface de monitoring

Nos offres

- Basique : scénario générique valable pour tout contexte et toute entreprise
- Premium : scénario sur-mesure adapté au contexte de l'entreprise
- Advanced – ciblé : scénario sur-mesure adapté aux profils des employés ciblés
- Advanced – Red Team : scénario sur-mesure incluant une pièce-jointe malveillante

En fonction des offres la méthodologie peut évoluer et demander plus ou moins de temps, les coûts varient également.

Notre approche

- Validation des pré-requis
- Préparation de la campagne
- Lancement de la campagne
- Agrégation des résultats
- Sensibilisation des employés

Préparation de la campagne
- Cadrage de la mission
- Validation du périmètre
- Validation des Pré-requis
- Planification du lancement de la campagne
- Choix et/ou conception des scénarios
- Phase de récolte d'informations

Lancement de la campagne
- Envoi des courriels aux cibles du périmètre
- Collecte et analyse des informations de la campagne

Agrégation des résultats
- Consolidation des résultats
- Rédaction du rapport de la campagne
- Restitution avec les différentes parties prenantes

Sensibilisation des employés
- Adaptation des supports de sensibilisation en fonction des résultats de la campagne
- Proposition de différents types de sensibilisations au phishing

/	Réf. : PHISHING	Sur demande	Sur demande

Zero Trust et Architecture Défensive : État de l'art & solutions

Le concept Zero Trust a été identifié à juste titre par les éditeurs comme un nouvel eldorado depuis que l'administration du président Joe Biden l'a rendu exécutoire en Mai 2021 pour toutes les agences fédérales. Les solutions marketées « Zero Trust » se comptent par plusieurs dizaines. Qu'est-ce que le Zero Trust et comment répond-il à un véritable besoin ? Quelle approche adopter pour une architecture pérenne? Les offres packagées sont-elles des solutions viables?

Vous allez apprendre à

- A distinguer une architecture de sécurité traditionnelle vs défensive
- Les bonnes pratiques pour sécuriser les switch, routeurs et point d'accès
- A identifier les 9 piliers Zero Trust du modèle Deloitte
- A comprendre de façon pratique l'application du Zero Trust sur une infrastructure existante
- A évaluer les solutions du marché
- A éviter les pièges organisationnels de mise en œuvre

Public visé

- Nouveaux ou futurs RSSI souhaitant découvrir le Zero Trust et échanger
- RSSI expérimentés souhaitant se remettre à niveau et échanger sur les bonnes pratiques Zero Trust avec d'autres RSSI
- Ingénieurs en sécurité des systèmes d'information souhaitant rapidement acquérir les bases du Zero Trust
- Directeurs des systèmes d'information ou auditeurs en systèmes d'information souhaitant connaitre les contours du Zero Trust

Pré-requis

- Expérience au sein d'une direction informatique en tant qu'informaticien ou bonne connaissance générale des systèmes d'information
- Des notions de base en sécurité appliquée aux systèmes d'information constituent un plus

Méthode pédagogique

- Cours magistral dispensé par des consultants et des experts de chaque domaine organisationnel, technique et commercial
- Formation dispensée en français

Matériel

- Support de cours en français au format papier

Programme

Introduction
- Accueil
- Les origines du firewall et de la défense périmétrique
- Architecture traditionnelle vs défensive
- Les caractéristiques d'un réseau défensif
- Les bonnes pratiques de sécurité appliquées au modèle OSI
- Zonage SOC
- Cas pratique

Zero Trust
- Concepts de base
- Principes d'architecture et stratégie d'application
- Modèles Zero Trust NIST & Forrester
- Les 9 piliers Zero Trust du modèle Deloitte
- Cas pratique

Les solutions du marché
- Panorama des solutions du marché
- Acteurs principaux

A**spects organisationnels de mise en œuvre**
- Cadrage
- Documents à préparer
- Conformité
- Considérations pratiques
- L'approche Deloitte

4 heures	Réf. : 0TRUST	Sur demande	Sur demande

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Sensibilisation

Nos outils – E-learning

Nous vous proposons des e-learnings sur les fondamentaux de la cybersécurité. Ces cours peuvent être adressés à un public averti en guise de rappel ou déployé auprès d'un public novice afin de le sensibiliser aux enjeux de la cybersécurité et aux risques les plus courants en entreprise. Ces cours présentent également les bonnes pratiques d'une façon ludique et engageante.

- Entre 20 minutes et 1h de e-learning en fonction de la thématique choisie.
- Vue d'ensemble des différents risques de cybersécurité : vol et fuite d'informations, atteinte à la réputation, problèmes juridiques et sanctions, etc. et bonnes pratiques associées.
- Quiz de validation des acquis.

Ces e-learnings peuvent facilement être déployés auprès d'un très grand nombre de collaborateurs. Ils sont disponibles sur notre plateforme de sensibilisation personnalisable et qui dispose d'option de dashboard de tracking pour suivre le taux de participation et de réussite des collaborateurs ciblés. Nous pouvons également intégrer ces modules à vos environnements de sensibilisation.

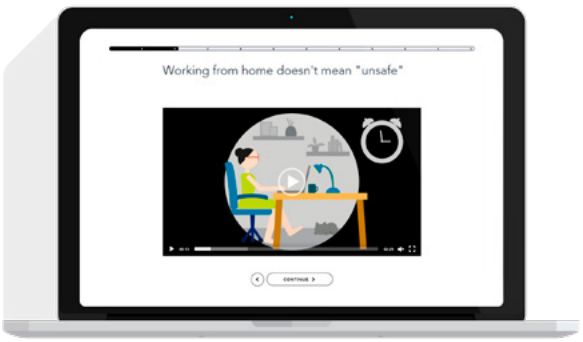
20 min à 1h	Réf. : E-LEARNING	Sur demande	Sur demande

Nos outils – Micro-learning

Nous mettons à votre disposition une série de micro-learnings axés sur des sujets clés de la cybersécurité, afin d'initier les employés aux meilleures pratiques en matière de cybersécurité.

- 30 micro-learnings d'une durée de 2 à 3 minutes
- Thèmes spécifiques et parcours à la carte
- Des contenus visuels attractifs

Le micro-learning présente de nombreux avantages: un taux d'engagement plus élevé que sur un format plus long, ainsi qu'une appréhension des concepts plus efficace grâce à des contenus plus spécifiques. N'hésitez plus!



Qu'est-ce-que la cybersécurité? | La cybersécurité à la maison | Mots de passe : la clé de votre sécurité en ligne | Etc.

2 à 3 min	Réf. : M-LEARNING	Sur demande	Sur demande

Nos outils de gamification - Hacker Game

Déployez notre hacker Game auprès de vos collaborateurs: une manière ludique de découvrir les vulnérabilités les plus communes de la cybersécurité; parmi lesquelles: navigation sur internet, mots de passe, phishing, etc. Ils pourront se mettre dans la peau d'un détective et devront répondre à des questions sur les failles de sécurité pour évoluer dans le scénario et débloquer les niveaux suivants.

Vos collaborateurs pourront suivre leur progression et leur position dans un classement. Ces statistiques sont traçables grâce à un dashboard de suivi.

Ce jeu est disponible sur notre plateforme de sensibilisation ou peut être intégré directement à votre outil.

Public visé

- Personnes non-initiées à la cybersécurité.

Selon la progression du participant	Réf. : H-GAME	Sur demande	Sur demande

Nos outils – Phishing Game

Le « Phishing Game» est un jeu de sensibilisation au phishing. Le joueur doit désamorcer la bombe en répondant à une série de questions sur le fonctionnement d'une attaque par hameçonnage. En cas de mauvaise réponse, une explication est donnée et une autre tentative est possible. Le participant peut ainsi appréhender au mieux les bonnes pratiques à appliquer.

Ce jeu est disponible sur notre plateforme de sensibilisation ou peut être intégré directement à votre outil.

Les statistiques des collaborateurs sont traçables grâce à un dashboard de suivi.

Public visé

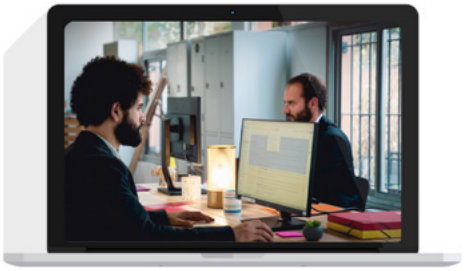
- Personnes non-initiées à la cybersécurité.

5 min	Réf. : P-GAME	Sur demande	Sur demande

Nos outils – Sensibilisation en Réalité Virtuelle

En partenariat avec REALITY ACADEMY

Fondamentalement convaincus que les moyens de la formation et de la sensibilisation évoluent en même temps que les besoins, nous vous proposons la mise à disposition d'un outillage de formation en réalité virtuelle. La méthode d'apprentissage « Learning by doing » fait de plus en plus ses preuves autant considérée comme un module auto-suffisant, que comme un outil complémentaire au sein d'un programme de sensibilisation.



Scénarios **interactifs et immersifs**

Mettez-vous dans la peau d'un collaborateur puis d'un hacker, et prenez des décisions à la 1ère personne.

Expérience **émotionnelle**

Vivez une cyber-attaque en entreprise et confrontez-vous aux conséquences directes et indirectes.

Suivi et bilan **personnalisés**

Accompagné.e par un coach virtuel, vous apprenez à identifier les différents types de cyber-attaques et adoptez les bonnes pratiques pour y faire face.

Les avantages de la formation en réalité virtuelle

Viralité de la formation

87% des apprenants encouragent à faire l'expérience

Motivation de l'apprenant

Un taux de complétion élevé, proche des **90%**

Mémorisation de l'information

Une rétention **4x** plus efficace des messages

2 parcours disponibles

- Les essentiels de la cybersécurité
- La protection des données sensibles

Publics visés

- Collaborateurs peu sensibilisés
- Dirigeants
- Partie tierce

Environ 20 minutes | Réf. : VR-learning | Sur demande | Disponible sur demande

Formation Itil v4 Foundation

Objectifs de la formation

- Réussir la certification ITIL 4 Foundation.
- Comprendre l'approche holistique de la co-création de valeur avec les clients et les autres parties prenantes sous forme de produits et de services.
- Identifier les principes directeurs de ITIL4.
- Acquérir les quatre dimensions de la gestion des services.
- Comprendre les Concepts clés de Lean IT, Agile, DevOps, et pourquoi ils sont importants pour permettre la creation de valeur opérationnelle.
- Comprendre comment les pratiques décrites dans ITIL 4 permettent de maintenir la valeur.
- Identifier l'importance fournie par les processus actuels tout en élargissant leur intégration à différents domaines de la gestion des services.
- Préparer, réviser et acquérir les trucs et astuces pour réussir l'examen officiel ITIL 4 Foundation.

Public visé

- Toute personne qui voudrait obtenir sa certification ITIL 4 Foundation.
- Toute personne qui voudrait connaitre l'une des meilleures pratiques pour la gestion d'un parc informatique.
- Les responsables d'exploitation, directeurs ou chefs de projets, experts qualité, toute personne souhaitant maitriser les concepts d'ITIL 4.

Pré-requis

- Il n'y a pas de pré-requis nécessaire pour suivre et réussir les objectifs de cette formation. Il est seulement préférable que le participant soit familiarisé avec les termes techniques lié au métier de l'informatique en général.

Certification

- Cette formation ITIL prépare à l'examen de certification Itil v4 Foundation.

Programme

- Les concepts clés de la gestion des services
- Les concepts clés de ITIL v4
- ITIL 4 « service value system »
- ITIL 4 « service value chain »
- Les 7 principes directeurs de ITIL 4
- Introduction aux ITIL 4 practices
- Description de 13 services management practices
- Description de 1 technical practice
- Révision générale des points principaux nécessaires au programme de l'examen
- Préparation à l'examen de certification ITIL 4 Foundation
- Passage de l'examen de certification ITIL 4 Foundation

3 jours / 21 heures	Réf. : ITIL	1 590€ hors taxes	Disponible sur demande

PMP - Project Management Professional

Objectifs de la formation

- Réussir la certification PMP, Project Management Professional.
- Connaitre les 5 groupes de processus du management de projet.
- Connaitre les 10 domaines de connaissance du management de projet.
- Se familiariser avec l'ouvrage de référence du PMI® : le PMBOK®.
- Maîtriser le référentiel PMI : les processus, domaines de management et techniques qui garantissent le ressort des projets.
- Préparer, Réviser et Acquérir les trucs et astuces de l'examen PMP®.

Public visé

Toute personne travaillant dans un environnement projet, qui veut obtenir sa certification PMP et/ou qui veut connaitre les meilleures pratiques pour la gestion de projets selon PMI.

Pré-requis

- Il n'y a pas de Pré-requis nécessaire pour suivre cette formation. Il est seulement préférable que le participant soit familiarisé à la gestion de projets ou d'avoir travaillé dans un environnement projet.
- Pour passer l'examen PMP, un dossier qui correspond à une demande d'autorisation de passer l'examen (dossier d'éligibilité) doit être déposée sur le site du PMI. Cette étape n'est pas complexe, mais il ne faut surtout pas la négliger. Nous avons un chapitre complet sur ce sujet lors de notre formation. Les pré-requis pour cette éligibilité sont liés à votre expérience professionelle. Il est conseillé d'avoir à minima 5 annnées d'expérience profesionnelle pour se lancer dans ce dossier d'éligibilité. N'hésitez pas à contacter nos experts formation pour en discuter.

Certification

Cette formation prépare à l'examen de certification PMP, Project Management Professional

Programme

- Les fondamentaux de la gestion de
- La méthodologie PMI®
- Gestion de l'intégration du projet
- Gestion du périmètre du projet
- Gestion des coûts du projet
- Gestion de la qualité du projet
- Gestion de ressources du projet
- Gestion des communications du projet
- Gestion des risques du projet
- Gestion des approvisionnements du projet
- Gestion des parties prenantes du projet
- La certification PMP

5 jours / 35 heures	Réf. : PMP	3 290€ hors taxes	Disponible sur demande

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Prince2 Foundation

Objectifs de la formation

- Réussir la certification Prince2 Foundation.
- Distinguer les différents composants de gestion de Prince2.
- Utiliser les sept lignes directrices de Prince2 constituant un référentiel de bonnes pratiques.
- Présenter les thèmes et processus clés formant le cœur de Prince2.
- Intégrer les éléments Prince2 pour visualiser la structure de la méthode.

Public visé

- Toute personne qui veut obtenir sa certification Prince2 et/ou qui veut connaitre l'une des meilleures pratiques pour la gestion de projet.

Pré-requis

- Il n'y a pas de Pré-requis nécessaire pour suivre et réussir les objectifs de cette formation. Il est seulement préférable que le participant soit familiarisé avec la conduite de projet, ou qu'il soit dans un environnement de travail en mode projet.
  La lecture des documents de préformation est recommandée : ils vous seront envoyés une semaine avant votre formation au plus tard, avec votre convocation.

Certification

- Cette formation prépare à l'examen de certification Prince2 Foundation.

Programme

- Pourquoi Prince2 ?
- Structure de Prince2
- Les sept thèmes de Prince2
- Les sept processus de Prince2
- Etude de cas & passage de la certification

3 jours / 21 heures	Réf. : PRINCE2	1 590€ hors taxes	Disponible sur demande

Prince2 Practitioner

Objectifs de la formation

Réussir la certification PRINCE2 Practitioner.
Distinguer les différents composants de gestion de PRINCE2.
Utiliser les sept lignes directrices de PRINCE2 constituant un référentiel de bonnes pratiques.
Présenter les thèmes et processus clés formant le cœur de PRINCE2.
Intégrer les éléments PRINCE2 pour visualiser la structure de la méthode.
Profiter de l'assurance Take² : 2ème passage possible sur l'examen PRINCE2 Practitioner.

Public visé

Toute personne qui veut obtenir sa certification PRINCE2 et/ou qui veut connaitre l'une des meilleures pratiques pour la gestion de projet.

Pré-requis

Il n'y a pas de pré-requis nécessaire pour suivre et réussir les objectifs de cette formation. Il est seulement demandé de posséder au préalable la certification PRINCE2 Foundation.
La lecture des documents de Pré-Formation est recommandée : ils vous seront envoyés une semaine avant votre formation au plus tard, avec votre convocation.

Certification

Cette formation prépare à l'examen de certification Prince2 Practitioner

Programme

Rappels sur Prince2 ?
Approfondissement de la méthode Prince2
Etude de cas
La certification Prince2 Practitioner

2 jours / 14 heures	Réf. : PRI2P	Sur demande	Disponible sur demande

Modalités d'inscription

Pour toute inscription aux formations HSC (une entité du réseau Deloitte), vous devez nous transmettre par courriel à formations-cyber@deloitte.fr ou par téléphone au +33 1 55 61 68 64 : les noms et prénoms du ou des participants, la ou les sessions de formation choisies, l'adresse postale de votre société et votre numéro de TVA intracommunautaire. Ces renseignements nous permettront d'établir une convention de formation.

Cette convention de formation devra nous être retournée tamponnée, signée et accompagnée d'un bon de commande de votre organisme. Le bon de commande devra indiquer votre adresse de facturation et le respect de nos conditions de règlement : il devra également être tamponné et signé par l'autorité compétente. La facture sera établie à la fin de la formation. L'inscription sera confirmée dès réception de ces documents. Une convocation sera envoyée par mail deux semaines avant le début de la formation.

HSC (une entité du réseau Deloitte) est enregistré comme centre de formation sous le n°11921448592 auprès du préfet de la région Île-de-France.

Si le client souhaite effectuer une demande de prise en charge par l'OPCO dont il dépend, il lui appartient :

- de faire une demande de prise en charge dans les délais requis et de s'assurer de la bonne fin de cette demande ;
- de l'indiquer explicitement au moment de l'inscription.

Si l'acceptation de la prise en charge OPCO n'est pas arrivée chez Deloitte Cyber Academy (HSC) au plus tard deux semaines avant le début de la formation, la demande de subrogation ne pourra être prise en compte par Deloitte Cyber Academy (HSC). Le client aura alors la possibilité :

- soit d'annuler ou de reporter l'inscription ;
- soit de produire, avant la formation, un bon de commande en bonne et due forme par lequel il s'engage à régler le coût de la formation à Deloitte Cyber Academy (HSC).

Nos formations sont disponibles en présentiel (Paris La Défense) et en distanciel.

Certaines de nos formations peuvent être dispensées en intra entreprise sous conditions (nous consulter).

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Vos contacts formation :

Emilie Bozzolo
Responsable formation
ebozzolo@deloitte.fr
+33 (0)1 40 88 71 46
+33 (0)7 72 88 28 28

Léa Wagner
Chargée de formation
lewagner@deloitte.fr
+33 (0)1 55 61 68 64
+33 (0)7 88 29 24 79

Constance Menard
Business Developer
comenard@deloitte.fr
+33 (0)1 40 88 72 39
+33 (0)6 72 14 43 44

Manal Aouak
Chargée de formation
maouak@deloitte.fr
+33 (0)1 55 61 58 21
+33 (0)6 82 40 48 76

Mary Jane Deniega
Chargée de formation
mdeniega@deloitte.fr
+33 (0)1 55 61 79 14

Calendrier des formations au premier semestre 2023

Ce planning est susceptible d'être complété ou modifié.
Retrouvez les dates de nos sessions de formation en nous appelant au +33 1 40 88 72 39.

Sécurité organisationnelle	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Certified in Cybersecurity (ISC)²	16 au 17						3 au 4
CISSP, (ISC)²			6 au 10		22 au 26	26 au 30	
CCSP, (ISC)²				3 au 7			
RSSI			27 au 31			12 au 16	
CISA				17 au 21			
Préparation à l'examen de certification CCISM		6 au 8					3 au 5
Préparation à l'examen de certification CRISC	23 au 27				22 au 26		
Gestion de crise IT/SSI			6 au 8				
Formation NIS					9		
Formation ISO 27001 & 27002 Introduction					11 au 12		
ISO 27001 Lead Auditor			13 au 17			5 au 9	
ISO 27001 Lead Implementer - Français		6 au 10		3 au 7		19 au 23	
ISO 27001 Lead Implementer - English	16 au 20						
ISO 27005 Risk Manager - Français	30/01 au 1/02			11 au 13	30/05 au 1/06		
ISO 27005 Risk Manager - English	9 au 11						3 au 5
Ebios Risk Manager 2018				17 au 19			
ISO 27005 RM + Ebios RM 2018 - Pack 1 semaine						12 au 16	
ISO 27032 Lead Cybersecurity Manager		13 au 17					
ISO 27035 Lead Incident Manager		13 au 17					
ISO 27701 Lead Implementer, Système de management de la protection de la vie privée			20 au 24				
ISO 31000 Risk Manager	23 au 25						
ISO 22301 Lead Auditor							
ISO 22301 Lead Implementer			27 au 31				

Sécurité juridique	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Droit de la Sécurité des Systèmes d'Information (SSI)					30/05 au 1/06		
RGPD : essentiel de la conformité					9 au 10		
Certification des Compétences du DPO conformément au référentiel de certification de la CNIL			20 au 24				

Sécurité technique	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Test d'intrusion et sécurité offensive							
Essentiels techniques de la SSI					15 au 16		
Socle technique de la cybersécurité							
Formation cybersécurité industrielle					22 au 24		
Architectures réseaux sécurisées			13 au 15				
Investigation numérique réseaux (ESD)				17 au 19			
Investigation numérique Windows (ESD)						12 au 14	
Intégration d'un SOC (ESD)	23 au 27			24 au 28			24 au 28
Sécurité des serveurs et applications web							
Durcissement sécurité Windows (ESD)	30/01 au 2/02					26 au 29	
Développement Sécurisé				11 au 13			
Sécurité Active Directory						19 au 22	

Calendrier des formations au second semestre 2023

Ce planning est susceptible d'être complété ou modifié.
Retrouvez les dates de nos sessions de formation en nous appelant au +33 1 40 88 72 39.

Sécurité organisationnelle	Août	Septembre	Octobre	Novembre	Décembre
Certified in Cybersecurity (ISC)²		11 au 12			
CISSP, (ISC)²		18 au 22		13 au 17	11 au 15
CCSP, (ISC)²				20 au 24	
RSSI			2 au 6	27/11 au 1/12	
CISA				20 au 24	
Préparation à l'examen de certification CCISM		4 au 6		6 au 8	
Préparation à l'examen de certification CRISC					18 au 22
Gestion de crise IT/SSI			16 au 18		
Formation NIS				6	
Formation ISO 27001 & 27002 Introduction				9 au 10	
ISO 27001 Lead Auditor			9 au 13		4 au 8
ISO 27001 Lead Implementer - Français		25 au 29		13 au 17	11 au 15
ISO 27001 Lead Implementer - English		4 au 8			
ISO 27005 Risk Manager - Français		20 au 22		6 au 8	4 au 6
ISO 27005 Risk Manager - English					
Ebios Risk Manager 2018			16 au 18		
ISO 27005 RM + Ebios RM 2018 - Pack 1 semaine				27/11 au 1/12	
ISO 27032 Lead Cybersecurity Manager			23 au 27		
ISO 27035 Lead Incident Manager			2 au 6		
ISO 27701 Lead Implementer, Système de management de la protection de la vie privée				20 au 24	
ISO 31000 Risk Manager			23 au 25		
ISO 22301 Lead Auditor		11 au 15			
ISO 22301 Lead Implementer			16 au 20		

Sécurité juridique	Août	Septembre	Octobre	Novembre	Décembre
Droit de la Sécurité des Systèmes d'Information (SSI)					4 au 6
RGPD : essentiel de la conformité			9 au 10		
Certification des Compétences du DPO conformément au référentiel de certification de la CNIL		11 au 15			11 au 15

Sécurité technique	Août	Septembre	Octobre	Novembre	Décembre
Test d'intrusion et sécurité offensive			9 au 13		
Essentiels techniques de la SSI				13 au 14	
Socle technique de la cybersécurité		25 au 29			
Formation cybersécurité industrielle				27 au 29	
Architectures réseaux sécurisées		18 au 20			
Investigation numérique réseaux (ESD)			16 au 18		
Investigation numérique Windows (ESD)				27 au 29	
Intégration d'un SOC (ESD)			23 au 27		
Sécurité des serveurs et applications web			23 au 27		
Durcissement sécurité Windows (ESD)		11 au 14		6 au 9	
Développement Sécurisé			2 au 4		
Sécurité Active Directory					11 au 14

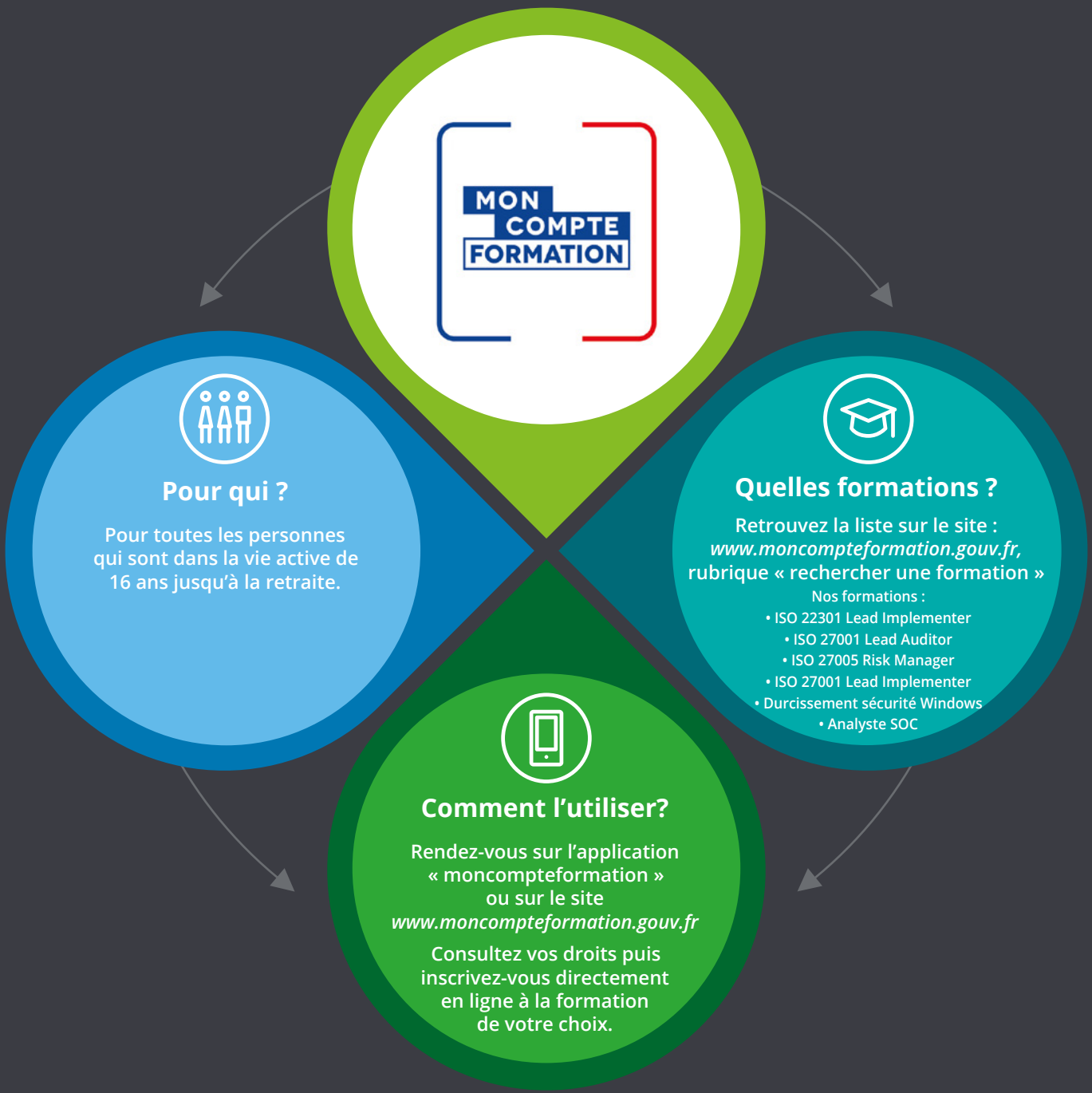
Toutes nos formations sont accessibles aux personnes en situation de handicap.

Et si vous financiez votre formation avec votre compte CPF ?

Le **CPF** c'est quoi ?

Le **Compte Personnel de Formation** existe depuis le 1er janvier 2015 et a remplacé le **DIF** (Droit Individuel à la Formation).

Ce compte permet de cumuler jusqu'à **500 euros** par an dans la limite de 5 000 euros (800€ pour les salariés non qualifiés dans la limite de 8 000€) qui seront utilisés pour financer **une formation** professionnelle **éligible au CPF**.



Conditions Générales de Ventes

1. Objet et dispositions générales

Les présentes conditions générales de vente s'appliquent aux commandes de formation interentreprises passées auprès de la société HSC (une entité du réseau Deloitte). Cela implique l'acceptation sans réserve par l'acheteur et son adhésion pleine et entière aux présentes conditions générales de vente et prévalent sur toutes conditions générales d'achat. Deloitte Cyber Academy (HSC) informe du niveau requis pour suivre les stages qu'elle propose. Il appartient au client d'évaluer ses besoins et de vérifier si ses collaborateurs ont le niveau de pré-requis attendu pour suivre les formations Deloitte Cyber Academy (HSC).

2. Inscription

L'inscription à un stage ne devient effective qu'après réception par nos services d'un bon de commande et de la convention de formation ou du devis, dûment renseigné et portant le cachet du client. Les documents devront parvenir à HSC au plus tard 15 jours avant le début de la formation.

Deloitte Cyber Academy (HSC) adressera par courriel, deux semaines avant le début de la formation, une convocation récapitulant les détails pratiques : date, lieu, horaires et accès, aux contacts indiqués dans les documents d'inscription. HSC filiale Deloitte ne peut être tenu responsable de la non-réception de la convocation quels qu'en soient le ou les destinataire(s) chez le client, notamment en cas d'absence du ou des stagiaires à la formation. A l'issue de la formation, une attestation individuelle de stage sera adressée par courriel, accompagnée de la facture correspondante.

Une commande n'est valable qu'après acceptation par HSC filiale Deloitte sous huitaine. Toute modification ultérieure apportée par le client devra faire l'objet d'un accord écrit de la part de HSC filiale Deloitte.

3. Modification, annulation et report

Toute annulation ou report d'inscription doit être signalé par téléphone et confirmé par écrit à HSC filiale Deloitte.
Pour les formations proposées en régions, à l'étranger ou hors de nos locaux (à Paris ou en région parisienne), si l'annulation ou le report intervient dans les trente jours ouvrés précédant le début de la formation, HSC filiale Deloitte facturera la totalité de la formation.

Pour les formations proposées dans nos locaux de La Défense (92) ou à distance, si le report ou l'annulation intervient :

- dans les 30 jours ouvrés précédant le début de la formation, HSC filiale Deloitte facturera à hauteur de 50% du coût total de la formation ;
- dans les 15 jours ouvrés précédant le début de la formation, HSC filiale Deloitte facturera la formation en totalité.

Toutefois, lorsqu'un participant ne peut pas assister à une formation à laquelle il est inscrit, il peut être remplacé par un collaborateur de la même entreprise.

Le nom et les coordonnées de ce nouveau participant doivent être confirmés par écrit à HSC filiale Deloitte. En cas d'absence du stagiaire pour un cas de force majeure communément admis par les tribunaux, à titre exceptionnel et après validation de caractère de force majeure de la situation, HSC filiale Deloitte accepte que le client puisse, dans les 12 mois maximum suivant son absence, choisir une date future pour la même formation.

HSC filiale Deloitte se réserve le droit d'annuler ou de reporter sans indemnités une formation, si le nombre de participants n'est pas suffisant ou en cas de force majeure. Le client peut alors choisir une autre date dans le calendrier des formations. HSC filiale Deloitte ne pourra être tenu responsable des frais ou dommages consécutifs à l'annulation d'un stage ou à un report à une date ultérieure.

4. Tarifs – Facturation

Les frais de participation comprennent : la participation à la formation, les supports de cours et les pauses café. Les déjeuners sont offerts par HSC filiale Deloitte. Toute formation commencée est due en totalité.

La facture est établie à l'issue de la formation.

L'échéance est mentionnée en clair sur la facture. Tout défaut de paiement (en tout ou en partie) par le client à l'échéance et ce, sauf report sollicité par le client et accordé par HSC filiale Deloitte de manière formelle, entraînera automatiquement, sans qu'aucun rappel ne soit nécessaire et dès le jour suivant la date de règlement figurant sur la facture, l'application de pénalités de retard fixées à trois fois le taux d'intérêt légal. HSC filiale Deloitte pourra également exiger le paiement de l'indemnité forfaitaire pour frais de recouvrement, d'un montant de quarante (40) euros, ainsi que, le cas échéant, le paiement d'une indemnisation complémentaire, sur justification.

Prise en charge par un OPCO :
Si le client souhaite effectuer une demande de prise en charge par l'OPCO dont il dépend, il lui appartient :

- de faire une demande de prise en charge dans les délais requis et de s'assurer de la bonne fin de cette demande ;
- de l'indiquer explicitement au moment de l'inscription.

Si l'acceptation de la prise en charge OPCO n'est pas arrivée chez HSC filiale Deloitte au plus tard deux semaines avant le début de la formation, la demande de subrogation ne pourra être prise en compte par HSC filiale Deloitte. Le client aura alors la possibilité :

- soit d'annuler ou reporter l'inscription,
- soit de produire, avant la formation, un bon de commande en bonne et due forme par lequel il s'engage à régler le coût de la formation à HSC filiale Deloitte.

5. Propriété intellectuelle

Chaque formation comprend la fourniture de documentation destinée à l'usage interne du client. Toute reproduction, modification ou divulgation à des tiers de tout ou partie des supports de formation ou documents, sous quelque forme que ce soit, est interdite sans l'accord préalable écrit de HSC filiale Deloitte.

6. Arbitrage en cas de litige

Les présentes conditions générales de vente sont régies par les lois françaises. Tout litige découlant de leur interprétation ou de leur application ressort de la compétence exclusive des tribunaux des Hauts-de-Seine (92).

Deloitte.

Deloitte
6, place de la Pyramide – 92908 Paris-La Défense Cedex