

**Deloitte.**



## **CyberAcademy**

Catalogue CyberAcademy 2024  
Formation & Sensibilisation

Sécurité organisationnelle, continuité d'activité, juridique  
et technique



# 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 CyberAcademy

Deloitte CyberAcademy 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.

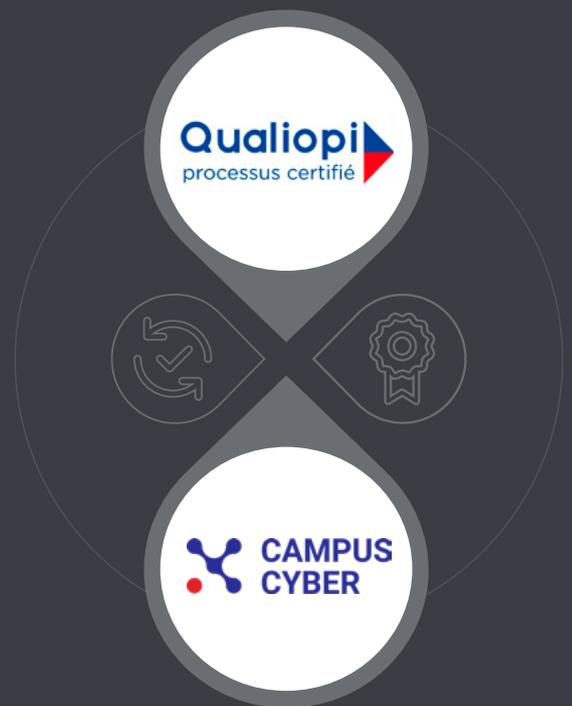
Vous trouverez au sein de ce catalogue l'ensemble de notre offre pour l'année 2024 avec :

- des formations de sécurité organisationnelle, juridique et technique ;
- des plans de sensibilisation adaptables au contexte de votre entreprise.

## Organismes de certification

Grâce au soutien de quatre organismes renommés, Deloitte CyberAcademy propose aux stagiaires de présenter les certifications les plus reconnues sur le marché international :

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



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



**Monia Ulmann**  
Directrice  
CyberAcademy  
mulmann@deloitte.fr  
+ 33 (0)1 40 88 25 92



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

# Campus Cyber

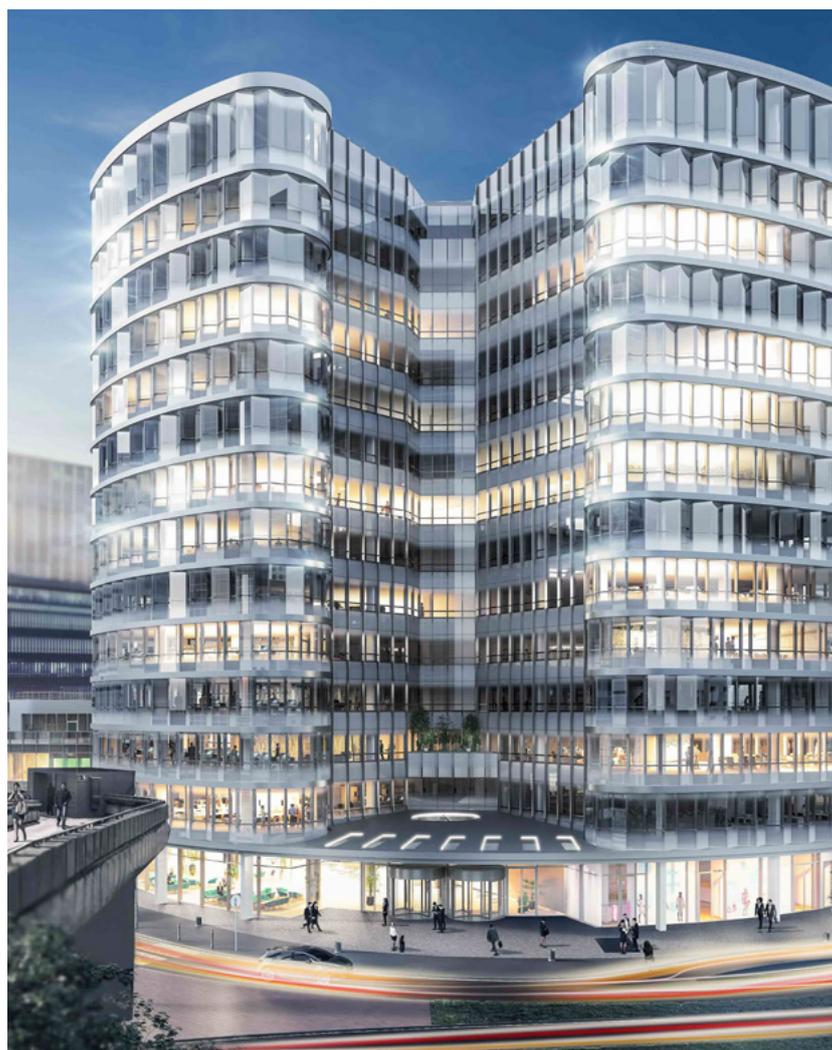
Le Campus Cyber a pour mission de fédérer l'ensemble des acteurs français en matière de cybersécurité et de confiance numérique. Deloitte détient des espaces en tant qu'acteur majeur de l'écosystème de la cybersécurité en Europe, afin d'apporter son expertise, soutenir et participer aux différentes actions du Campus Cyber, lieu totem du numérique et de la cybersécurité.



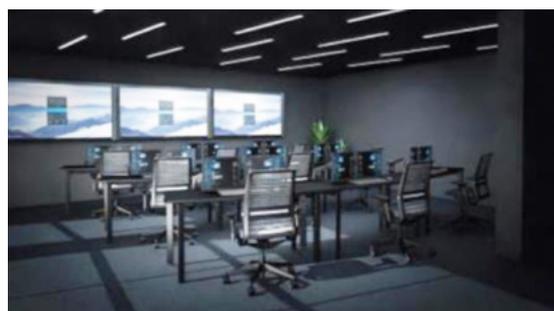
Deux salles de formation équipées d'écrans tactiles, d'amplificateurs et caméras à détection de mouvement pour maximiser l'expérience d'apprentissage.



Un accompagnement complet de la part de notre équipe pendant toute la durée de la formation.



**Tour Eria**



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



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

# Sommaire

Pour chaque prestation, ce catalogue vous fournira les informations suivantes :



		Code	Page	Durée (jours)
<b>Formation diplômante</b>				
Expert en Cybersécurité des systèmes d'information (RNCP Niveau 7)	New	ECSI	8	80
<b>Sécurité organisationnelle</b>				
<b>Management de la sécurité</b>				
Certified in Cybersecurity (ISC2)	New	CC	10	2
CISSP (ISC2)		CISSP	11	5
CCSP (ISC2)		CCSP	12	5
RSSI	New	RSSI	13	5
Préparation à l'examen CISA		CISA	14	5
Préparation à l'examen de certification Certified Information Security Manager (CISM)		CISM	15	5
Préparation à l'examen de certification Certified in Risk and Information Systems Control (CRISC)		CRISC	16	5
Gestion de crise IT/SSI		Crise IT/SSI	17	3
NIS	New	NIS	18	1
DORA	New	DORA	19	1
<b>Management de la sécurité avec les normes ISO</b>				
Fondamentaux ISO 27001 & 27002		27001 & 27002	21	2
Formation à la transition entre les normes ISO/IEC 27001:2013 -> 2022 et ISO 27002:2013-> 2022	New	TRANSI	22	2
ISO 27001 Lead Auditor		27001 LA	23	5
ISO 27001 Lead Implementer - Français		27001 LI	24	5
ISO 27005 Risk Manager - Français		27005 RM	25	3
EBIOS Risk Manager 2018	New	EBIOS RM	26	3
ISO 27032 Lead Cybersecurity Manager		27032 LCM	27	5
ISO 27035 Lead Incident Manager		27035 LIM	28	5
ISO 27701 Lead Implementer, Système de management de la protection de la vie privée		27701 LI	29	5
ISO 31000 Risk Manager		31000 RM	30	3
ISO 22301 Lead Auditor		22301 LA	31	5
ISO 22301 Lead Implementer		22301 LI	32	5
<b>Sécurité et juridique</b>				
Droit de la Sécurité des Systèmes d'Information (SSI)		Droit SSI	33	3
RGPD : essentiel de la conformité		RGPD	34	2
Certification des Compétences du DPO conformément au référentiel de certification de la CNIL		Cert DPO	35	5

# Sommaire

		Code	Page	Durée (jours)
<b>Sécurité technique</b>				
<b>Apprentissage en ligne</b>				
Offensive Security Certification	New	OFFSEC	36	/
<b>Intrusion</b>				
Test d'intrusion et sécurité offensive		INTRU1	37	5
<b>Introduction à la sécurité des systèmes d'information</b>				
Essentiels technique de la SSI		ESSI	38	2
Socle technique de la cybersécurité		SECU1	39	5
Cybersécurité industrielle		INDUS	40	2,5
Architectures réseaux sécurisées		SECARC	41	3
<b>Inforensique</b>				
Investigation réseaux Wireshark	New	SEC-INFRES	42	3
Investigation numérique Windows		INWIN	43	3
<b>Surveillance, défense et analyse</b>				
Analyste SOC (Security Operation Center)		SOC	44	5
Sécurité des serveurs et application web		SECWEB	45	5
Microsoft 365 – Durcissement	New	M365-SEC	46	4
Développement Sécurisé		DEVSEC	47	3
Sécurité Active Directory		SECUAD	48	4

<b>Sensibilisation</b>				
Introduction à la cybersécurité		INTROCYBER	51	1h à 2h
Sensibilisation gestion de crise		CRISE	52	2h à 4h
Sensibilisation C-LEVEL		C-LEVEL	53	1h à 2h
Campagne de phishing		PHISHING	54	/
Zéro Trust		OTRUST	55	4 h
Nos outils – E-learning		E-LEARNING	56	20 min à 1h
Nos outils – Micro-learning		M-LEARNING	56	2 min à 3 min
Nos outils de gamification – Hacker Game		H-GAME	57	Selon participant
Nos outils – Phishing Game		P-GAME	57	5 min
Nos outils – Sensibilisation en Réalité Virtuelle		VR-learning	58	20 min

<b>Référentiels et méthodes</b>				
Formation Itil v4 Foundation		ITIL	59	3
Project Management Professional		PMP	59	5
Prince2 Foundation		Prince2F	60	3
Prince2 Practitioner		Prince2P	60	2

<b>Informations pratiques</b>				
Modalités d'inscription et contacts			61	
Calendrier des formations			62	
Conditions générales de vente			64	





Un programme accrédité par la CGE.  
Conçu et délivré par EPITA, en  
partenariat avec IBM et Deloitte



**Deloitte.**



## Programme

### 1 Sécuriser et superviser le système d'information

#### Sécuriser les systèmes d'information

- Sécuriser les réseaux et infrastructures
- Sécuriser le cloud
- Sécuriser les systèmes industriels

#### Superviser les systèmes d'information

- Savoir mettre en œuvre des tests d'intrusion
- Formaliser un guide et une charte SSI
- Connaître la réglementation sur les données personnelles

### 2 Sécuriser les projets, les données et les développements

#### Mettre la sécurité au cœur des projets

- Suivre un projet informatique
- Sécuriser les projets informatiques
- Sécuriser les développements web
- Sécuriser les données
- Sécuriser les applications mobiles
- Conférences technologiques

### 3 Identifier les risques et organiser la cybersécurité

#### Organiser la cybersécurité dans la structure

- Introduction à la sécurité
- Connaître le marché de la sécurité, les acteurs et les outils
- Cybersécurité et renseignement
- Maîtriser les techniques d'influence et de négociation pour la mise en œuvre interne
- Comprendre les enjeux de sécurité et les facteurs de risques associés
- Droit de la cybersécurité
- Analyser et quantifier les risques

### 4 Détecter et répondre aux incidents

#### Manager une crise cyber

- Panorama et préparation à une crise
- Mettre en place un dispositif de gestion de crise
- Gérer la remédiation après une compromission
- Maîtriser la communication

#### Détecter et répondre aux incidents

- Collecter et analyse forensique
- Répondre aux intrusions et autres incidents



80 jours / 560 heures



Réf. : ECSI



18 000 € HT



• du 9 sept. 2024 au 5 fév. 2025  
• du 13 jan. au 14 juin 2025

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 ISC2 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 reconverter dans le domaine de la cybersécurité.

### Prérequis

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.

### Méthode pédagogique

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

### Matériel

- Supports de cours en anglais

### 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](http://www.pearsonvue.com/isc2).

### 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 ISC2

#### 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. : CC



2 000€ HT dont  
184€ HT de coupon  
d'examen



• 11 au 12 mars

• 17 au 18 octobre

## CISSP (ISC2)



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

### Prérequis\*

- Avoir lu le CBK (Common Body of Knowledge), livre officiel de l'ISC2
  - Disposer de 5 ans d'expérience dans au moins un des deux domaines suivants pour pouvoir passer la certification CISSP :
    - 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.
- 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'ISC2 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 CyberAcademy 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](http://www.pearsonvue.com).

### Programme

Les 8 domaines officiels du CBK :

- Security & Risk Management
- Asset Security
- Security Architecture and Engineering
- Communications & Network Security
- Identity & Access Management
- Security Assessment & Testing
- Security Operations
- Software Development Security

\* 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€ HT dont  
665€ HT de coupon  
d'examen



• 4 au 8 mars • 3 au 7 juin • 4 au 8 nov.  
• 22 au 26 avril • 16 au 20 sept. • 9 au 13 déc.

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'ISC2.

### 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

### Prérequis\*

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

### Matériel

- Support officiel de l'ISC2 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 l'ISC2.

### Les six domaines couverts par le CCSP

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

- Les concepts 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 démonstrabilité

#### 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€ HT dont  
555€ HT de coupon  
d'examen



• 13 au 17 mai

• 18 au 22 novembre

## RSSI

New

Cette formation de Deloitte CyberAcademy 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

### Prérequis\*

- 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

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

### Acteurs du marché de la sécurité

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

### Aspects juridiques de la SSI

- RGPD
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Administrateurs
- Charte informatique

### Soft-skills du RSSI

- Mieux se connaître pour développer ses compétences
- Renforcer son leadership
- Savoir s'adapter aux autres
- Convaincre, influencer et négocier
- Gérer son temps et ses priorités

### Stratégies de prise de fonction du RSSI

- Rôles du RSSI
- Relations avec les membres de la DSI, DG, les opérationnels
- Gouvernance
- Communication
- Questions/Réponses avec les stagiaires

### Intervention d'un RSSI selon disponibilité



5 jours / 35 heures



Réf. : RSSI



3 500€ HT



• 26 fév. au 1<sup>er</sup> mars  
• 10 au 14 juin  
• 23 au 27 septembre  
• 25 au 29 novembre

## Préparation à l'examen CISA



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](http://www.isaca.org)).

### Vous allez apprendre à

- 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

### Prérequis\*

- 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
- Bonne compréhension de l'anglais

### 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
- CISA Review Manual en anglais

### 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€ HT



• 22 au 26 avril

• 7 au 11 octobre

## 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 conformité spécifiques et la gestion de la sécurité grâce à un support développé par nos experts, incluant des diagrammes ainsi que des questionnaires pour s'entraîner.

### 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 et RSSI.

### 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

### Certification

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

Pour la certification officielle :

- Inscription à faire sur le site [www.isaca.org](http://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).
- Il n'y a pas de conditions préalables pour passer l'examen CISM ; cependant, pour obtenir la certification CISM, vous devez remplir les conditions d'expérience requises par l'ISACA.

### 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 demandés. Un QCM réussi de validation de l'atteinte des prérequis peut être nécessaire pour confirmer l'inscription.



5 jours / 35 heures



Réf. : CISM



3 500€ HT



• 17 au 21 juin

• 2 au 6 décembre

## 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. Nos experts vous apprendront comment concevoir, mettre en œuvre, surveiller et maintenir des contrôles de systèmes d'information efficaces et efficaces, basés sur les risques. La formation CRISC fera donc des participants 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 efficacité 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'efficacité 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'entraînement
- 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 échéant 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.
- 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 et 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

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.



5 jours / 35 heures



Réf. : CRISC



3 500€ HT



• 13 au 17 mai

• 16 au 20 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 maîtriser 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

### Prérequis

- Aucun prérequis n'est nécessaire. Des connaissances 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 de 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 chaîne 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€ HT



• 2 au 4 avril

• 12 au 14 novembre

## Formation NIS

New

Adoptée par les institutions européennes le 6 juillet 2016, la directive Network and Information Security (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 2006 et l'application de 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.

Face aux transformations du marché européen et à l'exposition croissante aux cybermenaces, l'Union Européenne a décidé de mettre à jour la première version de la directive NIS vers la directive NIS 2 publiée en décembre 2022. Cette dernière prévoit d'élargir les objectifs et le périmètre d'applicabilité du texte afin d'apporter davantage de protection.

### 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

### Prérequis\*

- 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 et son futur avec l'adoption de NIS 2
- 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 systèmes d'information ?
- Qu'est-ce-que la sécurité des réseaux ?
- Les règles de sécurité à appliquer par les Opérateurs de Services Essentiels (OSE) et les Fournisseurs de Service Numérique (FSN)
- Les limites de la directive
- Retour d'expérience, cas pratique (analyse des différences et correspondances entre ISO 27001/27002 – Directive NIS)
- Les perspectives d'évolution de la directive avec l'entrée en vigueur de NIS 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.



1 jour / 7 heures



Réf. : NIS



700€ HT



• 29 avril

• 12 novembre

## Formation DORA

New

Entré en vigueur le 16 janvier 2023, le règlement Digital Operational Resilience Act (DORA) doit permettre au secteur financier européen de rester résilient en cas de perturbation opérationnelle grave. Cette nouvelle réglementation intervient pour prévenir et atténuer le risque de cybermenaces, toujours plus nombreuses à l'encontre des banques et assurances. DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises du secteur financier ainsi que pour des tiers critiques qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC). Dans l'attente de l'élaboration des normes techniques par les autorités européennes de surveillance, cette formation vise à présenter ce cadre réglementaire innovant dans le droit européen et à vous préparer à son entrée en application prévue pour le 17 janvier 2025. En complément des obligations réglementaires et des recommandations des autorités, la formation vous présentera les principaux risques observés chez les entités financières et leurs prestataires TIC ainsi que les bonnes pratiques du marché. Vous serez donc en mesure de construire une stratégie visant à renforcer la résilience numérique d'une part, et d'identifier les mesures à mettre en œuvre en fonction des exigences et des risques inhérents à votre organisation d'autre part.

### Vous allez apprendre à

- Maîtriser les enjeux et les exigences du règlement
- Identifier les bonnes pratiques de résilience opérationnelle
- Appréhender un projet de mise en conformité
- Piloter sa mise en conformité avec les parties prenantes

### Public visé

- Les personnes souhaitant acquérir des connaissances relatives aux principales exigences du règlement
- Responsable de la sécurité de l'information ou équivalent
- Consultant, prestataire et tiers intervenant sur les domaines de la gouvernance SSI

### Prérequis

Aucune connaissance particulière n'est exigée

### Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques

### Matériel

Supports intégralement en français

### Certification

Cette formation n'est pas certifiante

### Programme

- Les enjeux du risque cyber pour le secteur financier européen
- Historique du règlement DORA et articulation avec les autres réglementations en vigueur (NISv2, CER, etc)
- Les grands objectifs de la réglementation DORA
- Les perspectives réglementaires autour des 5 piliers de DORA :
  - Le cadre de gestion des risques
  - La gestion des incidents
  - Les tests de résilience opérationnelle
  - La gestion des tiers
  - Le partage d'information et de renseignements
- Retours d'expérience pour préparer sa conformité DORA (analyse des différences et correspondances entre ISO 27001/27002 – Directive NIS)



1 jour / 7 heures



Réf. : DORA



700€ HT



• 3 avril

• 4 novembre

## Présentation des formations ISO

Vous souhaitez	Vous devez suivre	Page	
<ul style="list-style-type: none"> <li>• Avoir une introduction au SMSI</li> <li>• Acquérir les fondamentaux de la norme ISO 27001</li> <li>• Comprendre les mesures de sécurité et apprendre à les gérer (élaborer, améliorer et créer des enregistrements et des indicateurs)</li> </ul>	<b>Fondamentaux des normes ISO 27001 &amp; ISO 27002</b>	21	
<ul style="list-style-type: none"> <li>• Expliquer les différences entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022.</li> <li>• Interpréter les nouveaux concepts et exigences de l'ISO/IEC 27001:2022</li> <li>• Planifier et mettre en œuvre les changements nécessaires à un SMSI existant conformément à la norme ISO/IEC 27001:2022.</li> </ul>	<b>Transition entre la norme ISO 27001:2013 -&gt; 2022, 27002:2013 -&gt; 2022</b>	22	
<ul style="list-style-type: none"> <li>• Auditer un SMSI</li> <li>• Devenir auditeur interne ou auditeur de certification pour les SMSI</li> </ul>	<b>ISO 27001 Lead Auditor</b>	23	
<ul style="list-style-type: none"> <li>• Implémenter un SMSI</li> <li>• Devenir responsable de mise en œuvre d'un SMSI</li> </ul>	<span style="background-color: #76b82a; color: white; padding: 2px 5px;">Available in English</span>	<b>ISO 27001 Lead Implementer</b>	24
<ul style="list-style-type: none"> <li>• Apprendre à réaliser une gestion des risques avec la méthode ISO 27005</li> </ul>	<span style="background-color: #76b82a; color: white; padding: 2px 5px;">Available in English</span>	<b>ISO 27005 Risk Manager</b>	25
<ul style="list-style-type: none"> <li>• Apprendre à réaliser une gestion de risque avec la méthode EBIOS</li> </ul>	<b>EBIOS Risk Manager : 2018</b>	26	
<ul style="list-style-type: none"> <li>• Protéger les données et la confidentialité d'une organisation contre les menaces cybernétiques</li> <li>• Renforcer vos compétences dans la mise en place et la maintenance d'un programme de cybersécurité</li> <li>• Développer les bonnes pratiques pour gérer les politiques de cybersécurité</li> <li>• Améliorer le système de sécurité de l'organisation et assurer sa continuité d'activité</li> <li>• Réagir et récupérer plus rapidement en cas d'incident</li> </ul>	<b>ISO 27032 Lead Cybersecurity Manager</b>	27	
<ul style="list-style-type: none"> <li>• 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</li> </ul>	<b>ISO 27035 Lead Incident Manager</b>	28	
<ul style="list-style-type: none"> <li>• Comprendre le processus de mise en œuvre du système de management de la protection de la vie privée</li> <li>• 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</li> <li>• Soutenir le processus d'amélioration continue du système de management de la protection de la vie privée dans les organisations</li> <li>• Protéger la réputation de l'organisation</li> <li>• Augmenter la transparence des processus et procédures de l'organisation</li> <li>• Maintenir l'intégrité des informations des clients et des autres parties intéressées</li> </ul>	<b>ISO 27701 Lead Implementer</b>	29	
<ul style="list-style-type: none"> <li>• Acquérir des connaissances approfondies sur les principes fondamentaux, le cadre et les processus de management du risque conforme à la norme ISO 31000</li> </ul>	<b>ISO 31000 Risk Manager</b>	30	
<ul style="list-style-type: none"> <li>• Comprendre le fonctionnement d'un Système de management de la continuité d'activité (SMCA) conforme à la norme ISO 22301</li> <li>• 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</li> <li>• Savoir diriger un audit et une équipe d'audit</li> <li>• Savoir interpréter les exigences d'ISO 22301 dans le contexte d'un audit du SMCA</li> <li>• 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</li> </ul>	<b>ISO 22301 Lead Auditor</b>	31	
<ul style="list-style-type: none"> <li>• Étendre votre connaissance sur la façon dont un système de management de la continuité des activités vous aidera à atteindre vos objectifs opérationnels</li> <li>• Obtenir les connaissances suffisantes pour gérer une équipe pendant la mise en œuvre de l'ISO 22301</li> <li>• Renforcer la gestion de votre réputation</li> <li>• Identifier les risques et minimiser l'impact des incidents</li> </ul>	<b>ISO 22301 Lead Implementer</b>	32	

## 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

- Comprendre les éléments et le fonctionnement d'un Système de management de la sécurité de l'information
- Comprendre la mise en œuvre des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002
- Comprendre la corrélation entre la norme ISO/IEC 27001:2022 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres réglementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information (SI) et de gérer un Système de management de la sécurité de l'information (SMSI)

### 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

### Public visé

- Personnes intéressées par le management de la sécurité l'information et les mesures de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information

### Prérequis

- Aucun



2 jours / 14 heures



Réf. : 27001 & 27002



1 500€ HT



• 21 au 22 mai

• 13 au 14 novembre

## Transition entre les normes ISO/IEC 27001:2013 > 2022 et ISO 27002:2013 > 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. Cette formation vous permettra d'aborder les changements majeurs entre ISO/IEC 27001:2013 > 2022 et ISO 27002:2013 > 2022, portant principalement sur l'allègement en matière des contrôles de sécurité de l'information, ainsi que sur clauses de la norme.

### Vous allez apprendre à

- Expliquer les différences entre les versions 2013 et 2022
- Interpréter les nouveaux concepts et exigences
- Planifier et mettre en œuvre les changements nécessaires à un SMSI existant conformément aux normes

### Public visé

- Les personnes qui souhaitent rester à jour avec les exigences d'ISO/IEC 27001 et 27002 pour un SMSI
- Les personnes qui cherchent à comprendre les différences entre les exigences d'ISO/IEC 27001:2013 > 2022 et ISO 27002:2013 > 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
- Les professionnels souhaitant mettre à jour leur certificat ISO/IEC 27001 et 27002

### 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 et 27002\*.

### 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 > 2022 et ISO 27002:2013 > 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
- Quiz

### Certification

Après avoir réussi l'examen, les participants peuvent demander les qualifications :  
« PECB Certified ISO/IEC 27001:2022 » et  
« PECB Certified ISO/IEC 27002:2022 ».

### Programme

#### Jour 1

- Introduction aux versions des normes 2022 en comparaison avec celles de 2013
- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Aperçu des changements entre les versions de 2013 et 2022
- Modifications des clauses 4 à 10 d'ISO/IEC 27001

#### Jour 2

- Comparaison entre les contrôles de l'annexe A de l'ISO/IEC 27001:2013 et de l'ISO/IEC 27001:2022
- Annexe A - Contrôles organisationnels
- Annexe A - Contrôles des personnes
- Annexe A - Contrôles physiques
- Annexe A - Contrôles technologiques
- Clôture de la 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.



2 jours / 14 heures



Réf. : TRANSI



1 500€ HT



• 4 au 5 mars

• 14 au 15 octobre

## 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 acquerez 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

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

### 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

### Prérequis\*

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

\* 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

- 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 discussions
- 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 au SMSI et norme ISO/CEI 27001

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Processus de certification
- Concepts et principes fondamentaux de la sécurité de l'information
- SMSI

#### Jour 2 - Principes d'audit, préparation et initiation d'un audit

- Concepts et principes fondamentaux de l'audit
- Impact des tendances et de la technologie sur l'audit
- Audit fondé sur des preuves
- Audit fondé sur le risque
- Initiation du processus d'audit
- Étape 1 de l'audit

#### Jour 3 - Principes d'audit, préparation et initiation d'un audit

- Préparation à l'étape 2 de l'audit
- Étape 2 de l'audit
- Communication durant l'audit
- Procédures d'audit
- Création de plans de test d'audit

#### Jour 4 - Clôture de l'audit

- Rédaction des constatations d'audit et des rapports de non-conformité
- Documentation d'audit et revue de qualité
- Clôture de l'audit
- Évaluation des plans d'action par l'auditeur
- Après l'audit initial
- Management d'un programme d'audit interne
- Clôture de la formation

#### Jour 5 - Examen de certification



5 jours / 35 heures



Réf. : 27001 LA



3 500€ HT



• 11 au 15 mars  
• 10 au 14 juin

• 30 sep. au 4 oct.  
• 2 au 6 décembre

## ISO 27001 Lead Implementer

This training is available in English  
for Intra-company only



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

### Prérequis\*

Avoir une connaissance générale des concepts du SMSI et d'ISO/IEC 27001

\* 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

- 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 discussions
- 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 réglementaires
- 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 de son contexte
- Périmètre du SMSI

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

- Leadership et approbation du projet
- Structure organisationnelle
- Analyse du système existant
- Politique de sécurité de l'information
- Gestion des risques
- Déclaration d'applicabilité

#### Jour 3 – Mise en œuvre d'un SMSI

- Gestion des informations documentées
- Sélection et conception des mesures
- Mise en œuvre des mesures
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

#### 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
- Processus de certification et clôture de la formation

#### Jour 5 – Examen de certification



5 jours / 35 heures



Réf. : 27001 LI



3 500€ HT



• 5 au 9 fév. • 3 au 7 juin • 4 au 8 nov.  
• 25 au 29 mars • 16 au 20 sept. • 16 au 20 déc.

## ISO 27005 Risk Manager

This training is available in English  
for Intra-company only



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

### Prérequis\*

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

### Matériel

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

### Certification

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

### 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 réglementaires
- 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



**Pack Bundle :**  
**ISO 27005 RM +**  
**Ebios RM 2018**

Tarif : ~~4 300€ HT~~ -->  
**3 500€ HT**



\* 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. : 27005 RM



2 150€ HT



• 29 au 31 janvier • 27 au 29 mai • 14 au 16 oct.  
• 18 au 20 mars • 9 au 11 sept. • 9 au 11 déc.

## 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 Risk Manager. 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 Risk Manager
- Comprendre les étapes de la méthode Ebios Risk Manager 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 Risk Manager et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude Ebios Risk Manager
- 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 Risk Manager

### Public visé

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

### Prérequis\*

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 Risk Manager
- Les exercices de mise en situation représentent 70% du temps des cours en présentiel
- Les exercices pratiques sont basés sur des études de cas et incluent des jeux de rôle, des présentations orales et un serious game

### 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 CyberAcademy et labélisé par l'ANSSI
- L'examen de certification comprend un QCM et un cas d'étude qui est réalisé au fil du cours

**Nos formateurs sont signataires de la Charte Ebios : Fabien CAPARROS, Vincent LORIOT, Valentin LEMENNICIER.**

### Programme

#### Jour 1

Introduction à la méthode d'appréciation des risques Ebios Risk Manager

#### Jour 2

Réaliser l'appréciation des risques selon la méthode Ebios Risk Manager

#### Jour 3

Atelier avec études de cas et examen de certification



**Pack Bundle :  
ISO 27005 RM +  
Ebios RM 2018**

**Tarif : ~~4 300€ HT~~ -->  
3 500€ HT**



\* 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 est nécessaire pour confirmer l'inscription.



3 jours / 21 heures



Réf. : EBIOS RM



2 150€ HT



• 22 au 24 avril

• 9 au 11 octobre

## 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 acquerez 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 composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST
- Connaître l'objectif, le contenu et la corrélation entre l'ISO/IEC 27032 et le Cadre de Cybersécurité NIST ainsi qu'avec d'autres normes et cadres opérationnels
- Maîtriser les concepts, les approches, les normes, les méthodes et les techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation
- Savoir interpréter les lignes directrices de l'ISO/IEC 27032 dans le contexte spécifique d'une organisation
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans l'ISO/IEC 27032 et le cadre de Cybersécurité NIST
- Maîtriser les compétences pour conseiller une organisation sur les bonnes pratiques de gestion de la cybersécurité

### Prérequis\*

Une connaissance fondamentale sur la norme ISO/IEC 27032 et des connaissances approfondies sur la cybersécurité

\* 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.

### 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€ HT



• 22 au 26 janvier

• 9 au 13 septembre

## 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 acquerez 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

### Prérequis\*

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

### 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€ HT



• 5 au 9 février

• 14 au 18 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 acquerez 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

### Prérequis\*

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
- 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€ HT



• 8 au 12 avril

• 21 au 25 octobre

## 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

- Démontrer leur compréhension des principes de management du risque, tels que formulés dans ISO 31000
- Établir, maintenir et améliorer continuellement un cadre de management du risque, conformément aux lignes directrices d'ISO 31000
- Appliquer le processus de management du risque, conformément aux lignes directrices d'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

### Prérequis\*

Des connaissances fondamentales de la norme ISO 31000 et des connaissances approfondies sur le management du risque

### Méthode pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans le management du risque
- 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

### 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 réglementaires
- 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

\* L'apprenant s'engage à respecter les prérequis nécessaires. Une déclaration écrite et/ou un CV peuvent lui être demandés. 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€ HT



• 26 au 28 février

• 23 au 25 septembre

## 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 acquerez 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

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

### 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

### Prérequis\*

- 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 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 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 réglementaires
- 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

- Concepts et principes fondamentaux de l'audit
- L'impact des tendances et de la technologie dans le domaine de l'audit
- Audit basé sur des preuves
- Audit basé sur des risques
- Faisabilité de l'audit
- Audit de l'étape 1

#### Jour 3 – Activités d'audit sur site

- Préparation de l'audit de l'étape 2 (audit sur site)
- Audit de l'étape 2
- Communication durant l'audit
- Procédures d'audit
- Création de plans de test d'audit

#### Jour 4 – Clôture de l'audit

- Rédaction des conclusions d'audit et des rapports de non-conformité
- Documentation d'audit et examen de la qualité
- Clôture de l'audit
- Évaluation des plans d'action par l'auditeur
- Après l'audit initial
- Gestion d'un programme d'audit interne
- 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. : 22301 LA



3 500€ HT



• 25 au 29 mars

• 7 au 11 octobre

## 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

- Expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMCA basé sur ISO 22301, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMCA basé sur ISO 22301
- Préparer un organisme à un audit de certification par une tierce partie

### 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

### Prérequis\*

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
- Normes des systèmes de management
- Principes et concepts fondamentaux de la continuité d'activité
- Système de management de la continuité d'activité
- Déclenchement de la mise en œuvre du SMCA
- Compréhension de l'organisme et de son contexte
- Analyse du système existant
- Périmètre du SMCA

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

- Leadership et engagement
- Objectifs de continuité d'activité et planification des changements
- Politique de continuité d'activité
- Structure organisationnelle
- Gestion de l'information documentée
- Compétence et sensibilisation
- Analyse d'impact sur les activités

#### Jour 3 – Mise en œuvre d'un SMCA

- Évaluation des risques
- Stratégies et solutions de continuité d'activité
- Plans et procédures de continuité d'activité
- Plan d'intervention en cas d'incident
- Plan d'intervention d'urgence
- Plan de gestion de crise
- Communication

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

- Programmes d'exercices
- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- 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

\* 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€ HT



• 18 au 22 mars  
• 24 au 28 juin

• 25 au 29 novembre

## 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'œuvre de la SSI
- Chefs de projet
- Responsables de comptes
- Consultants

### Prérequis

- 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 juridique

#### Atteintes aux systèmes informatiques

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

#### Communications électroniques

- Cryptologie
- Brouillage des communications
- Filtrage

#### Informatique et libertés (RGPD)

- Notions essentielles
- Fondamentaux
- Sécurité des données personnelles
- Registres et analyse d'impact (PIA)
- Transferts en dehors de l'Union Européenne
- Sous-traitance
- Relations avec les personnes concernées

#### Conservation des traces (logs)

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

#### Surveillance des salariés

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

### Administrateurs systèmes et réseaux

- Obligation de confidentialité renforcée
- Accès étendus
- Responsabilité

### Charte informatique

- Fonctions et enjeux
- Contenu et rédaction
- Opposabilité et formalisme



3 jours / 21 heures



Réf. : Droit SSI



2 250€ HT



• 27 au 29 mai

• 4 au 6 novembre

## 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

- 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 MCE/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 maîtrise des risques

### Prérequis

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

### Méthode pédagogique

- Formation dispensée en français

### Matériel

- Support de cours en français

### 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 CyberAcademy.

### Programme

#### Introduction

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

#### Quels 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€ HT



• 18 au 19 mars

• 21 au 22 octobre

## 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

- Comprendre les concepts du RGPD et interpréter ses exigences
- Comprendre le contenu et la corrélation entre le Règlement général sur la protection des données et d'autres cadres réglementaires et normes applicables, telles que ISO/IEC 27701 et ISO/IEC 29134
- Acquérir la compétence nécessaire pour remplir le rôle et les tâches quotidiennes du délégué à la protection des données au sein d'un organisme
- Développer la capacité à informer, conseiller et surveiller la conformité au RGPD et à coopérer avec l'autorité de surveillance

### 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.

### Prérequis\*

Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences 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.

### Matériel

- Support de cours en français

### Certification

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

• Certification agréée par la 

### 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 demandés. 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€ HT



• 11 au 15 mars  
• 9 au 13 décembre  
• 16 au 20 septembre

## Offensive Security Certification

En collaboration avec Offensive Security, Deloitte CyberAcademy vous propose une large gamme d'abonnements en auto-apprentissage, ayant pour objectif de vous certifier dans les domaines suivants : penetration testing, sécurité des applications web, sécurité des opérations et développement d'exploits.



### Cours e-learning certifiants

Prix: 1 550€ HT / cours



#### PEN-200

Apprenez à utiliser les derniers outils et dernières techniques en les mettant en pratique dans un laboratoire virtuel composé de machines d'examen OSCP récemment retirées

90 jours d'accès au laboratoire  
OSCP Exam



#### PEN-300

Apprenez les techniques avancées de pentesting, y compris le contournement des mécanismes de sécurité et l'évasion des défenses

90 jours d'accès au laboratoire  
OSEP Exam



#### WEB-200

Apprenez les bases de l'évaluation des applications web. Exploitez les vulnérabilités web courantes, apprenez à exfiltrer des données sensibles à partir d'applications web ciblées

90 jours d'accès au laboratoire  
OSWA Exam



#### WEB-300

Spécialisez-vous dans la sécurité des applications web, des attaques XSS aux injections SQL. Apprenez à exploiter et à sécuriser les applications web en utilisant des méthodes de pentesting en boîte blanche

90 jours d'accès au laboratoire  
OSCP Exam



#### EXP-301

Apprenez les techniques de développement d'exploits. EXP-301 permet d'apprendre à contourner les mesures d'atténuation de la sécurité les plus courantes

90 jours d'accès au laboratoire  
OSED Exam



#### EXP-312

Apprenez à contourner les contrôles avancés de macOS. Un cours de développement d'exploits logiques offensifs sur macOS, axé sur l'escalade des privilèges locaux et le contournement des défenses du système d'exploitation

90 jours d'accès au laboratoire  
OSMR Exam



#### SOC-200

Apprenez les bases de la défense de la cybersécurité : le cours d'OffSec sur les opérations de sécurité et l'analyse défensive

90 jours d'accès au laboratoire  
OSDA Exam

### Abonnement

\* Prix par personne, par année



#### Learn Enterprise

Accès illimité à la bibliothèque pédagogique OffSec et au Cyber Range, ainsi qu'à des licences attribuables en fonction des besoins

4 600 € HT \*



#### Learn Unlimited

Accès illimité à la bibliothèque pédagogique OffSec et nombre illimité de tentatives d'examen pendant un an

5 100 € HT \*



#### Learn One

Un an d'accès au laboratoire pour un programme OffSec et deux tentatives d'examen

2 400 € HT \*



#### Learn Fundamentals

Accès à tous les contenus fondamentaux pendant un an pour se préparer aux cours avancés

750 € HT \*

## 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

### Prérequis\*

- 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

### Reconnaissance (OSINT)

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

### 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

### Intrusion sur les bases de données

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

### 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

### 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
- Active Directory

### Sécurité WiFi

- Présentation des protocoles d'authentification
- Attaques WiFi (exemples concrets)



5 jours / 35 heures



Réf. : INTRU1



3 600€ HT



• 30 septembre au 4 octobre

## Essentiels techniques de la SSI

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'enrichir de nouvelles connaissances en sécurité
- Administrateurs systèmes ou réseaux

### Prérequis\*

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

### 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
- 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 : sécurité 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, add-ons, 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

\* 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.



2 jours / 14 heures



Réf. : ESSI



1 400€ HT



• 17 au 18 juin

## 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 reconverter dans la sécurité des systèmes d'information
- Administrateurs systèmes ou réseaux
- Professionnels de la sécurité

### Prérequis\*

Une réelle connaissance informatique est nécessaire.

### Méthode pédagogique

- Cours magistral
- Travaux pratiques

### Travaux pratiques

- Jour 2 : challenges de cryptographie
- Jour 3 : capture de paquets
- Jour 4 matin : initiation linux
- Jour 4 après-midi : PingCastle
- Jour 5 :
  - Buffer overflow
  - Attaques sur les applications web :
    - DVWA
    - Juice Shop

### Matériel

- Ordinateurs portables mis à disposition des stagiaires
- Supports 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

#### 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



5 jours / 35 heures



Réf. : SECU1



3 600€ HT



• 18 au 22 novembre

## 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

### Prérequis\*

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

### Méthode pédagogique

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

### 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 3<sup>e</sup> 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

\* 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.



2,5 jours / 17,5 heures



Réf. : INDUS



2 250€ HT



• 17 au 19 juin

• 2 au 4 décembre

## Architectures réseaux sécurisées

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

## Prérequis\*

- 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 scanners
- 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€ HT



• 6 au 8 mars

• 23 au 25 septembre

## Investigation réseaux Wireshark

New

Formation en partenariat

Acquérir les compétences et la méthodologie pour une investigation numérique sur des réseaux Wireshark.

### Vous allez apprendre à

- Utiliser Wireshark pour capturer et analyser les paquets de données sur un réseau local ou distant
- Identifier les protocoles réseau courants (HTTP, HTTPS, FTP...) et leur structure de paquet – Utiliser les fonctionnalités de filtrage, de recherche et de coloration de Wireshark pour cibler les paquets d'intérêt
- Repérer et diagnostiquer les problèmes de latence, de perte de paquets et de congestion sur un réseau
- Personnaliser l'interface de Wireshark et utiliser des dissecteurs heuristiques pour afficher les données de manière plus lisible
- Utiliser les tableaux et graphiques de Wireshark pour visualiser et interpréter les données de trafic
- Exporter les paquets de Wireshark vers d'autres outils d'analyse
- Utiliser Wireshark en ligne de commande pour capturer, fractionner et fusionner des paquets de données.

### Public visé

- Ingénieurs réseau administrateurs système et professionnels de l'informatique souhaitant améliorer leurs compétences en matière d'analyse de réseau ou souhaitant découvrir les outils de diagnostic de réseau.

### Prérequis

- Avoir des connaissances de base en réseaux de données : modèle OSI, protocoles TCP/IP, adresses IP, masques de sous-réseau... Aucune connaissance préalable de Wireshark n'est nécessaire.

### Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques
- Auto-évaluation des compétences acquis

### Matériel

Supports de cours et exercices

### Certification

Cette formation n'est pas certifiante

### Programme

#### Jour 1

##### Introduction à Wireshark et aux réseaux de données

- Rappels et historique de Wireshark
- Modèle OSI et TCP/IP
- Supports de transmission et normes
- Format de trame :
  - 802.3
  - 802.1Q
- Adresses réseau et encapsulation IP
- Protocoles :
  - ARP
  - ICMP
  - DHCP
  - DNS
  - HTTP / HTTPS
- TCP/IP et adressage applicatif
- En-tête TCP et la couche application
- Installation de Wireshark

#### Jour 2

##### Outils de Wireshark et analyse de trafic

- Comment Wireshark traite les paquets
- Eléments clés de Wireshark
- Suivre un paquet et analyser le trafic
- Personnaliser Wireshark
  - Colonnes
  - Dissecteurs...
- Repérer les problèmes de latence
  - TCP Delta
- Filtres de capture et capture de réseau sans fil
- Filtres d'affichage

#### Jour 3

##### Utiliser Wireshark pour construire et interpréter les données

- Filtres d'affichage avancés
- Colorer et exporter les paquets
- Construire et interpréter les tableaux et graphiques
- Réassembler le trafic et exporter les objets
- Ajout de commentaires
- Utilisation de Wireshark en ligne de commande
- Capture
- Fraction et fusion des paquets
- Auto-évaluation des compétences acquis

\* 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. : SEC-INFRES



1 980€ HT



• 7 au 9 février  
• 3 au 5 juin

• 7 au 9 octobre

# Investigation numérique Windows

Formation en partenariat

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

## Prérequis\*

- 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
  - Echech/Réussite d'authentification
  - Évènement de service (démarrage)
  - Évènement d'authentification
  - Type d'authentification
  - Utilisation du RDP

- Différents artefacts USB

- Nomination des volumes
- Évènement 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.



3 jours / 21 heures



Réf. : INVWIN



1 980€ HT



- 26 au 28 février
- 19 au 21 juin

- 16 au 18 septembre
- 12 au 14 novembre

## Analyste SOC (Security Operation Center)

Formation en partenariat

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

### Prérequis\*

- 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)
- Prérequis 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 Sigma

##### 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



5 jours / 35 heures



Réf. : SOC



3 750€ HT



• 8 au 12 janvier  
• 25 au 29 mars

• 24 au 28 juin  
• 21 au 25 octobre

## Sécurité des serveurs et applications web

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

### Prérequis\*

- 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 CyberAcademy.

\* 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

- L'analyse de risques intégrée dans un projet
  - Les spécifications des exigences de sécurité liées aux spécifications d'un logiciel et de son infrastructure
  - Les choix de design
  - Architecture matérielle et 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, token 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 passe

#### 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



5 jours / 35 heures



Réf. : SECWEB



3 600€ HT



• 16 au 20 décembre

## Microsoft 365 - Durcissement

New

Formation en partenariat

La formation Microsoft 365 Durcissement, vise à doter les participants des compétences nécessaires pour renforcer la sécurité au sein de leur environnement Microsoft 365.

### Vous allez apprendre à

- Décrire les risques qui pèsent sur une entité sous Microsoft 365
- Mettre en place la sécurité dans son ensemble
- Implémenter et gérer les identités et les habilitations
- Etablir et gérer la protection des informations
- Implémenter et administrer la protection contre les menaces dans leur globalité
- Mettre en œuvre les bons outils
- Implémenter et mettre en œuvre les notions de conformités et de gouvernance

### Public visé

- Administrateurs Microsoft 365 et toute personne impliquée dans la sécurité ou la conformité Microsoft 365.

### Prérequis

- Maîtrise des outils de collaboration de Microsoft 365 et de la gestion des licences ainsi que leur architecture interne.
- Connaissance des bonnes pratiques de sécurité et de la protection des données au sein de l'environnement Microsoft 365.

### Méthode pédagogique

- Cours magistral interactif avec des exemples et des travaux pratiques
- Auto-évaluation des compétences acquis

### Matériel

Supports de cours et exercices

### Certification

Cette formation n'est pas certifiante

### Programme

#### Introduction aux risques

- Vue d'ensemble des principaux risques
- Introduction aux méthodes de durcissement
- Mettre en œuvre une méthode adaptée au sein de son entité
- Le principe du modèle Zero Trust
- Bonnes pratiques et gouvernance associée

\* 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.

#### Architecture Microsoft 365

- Tour d'horizon de l'architecture Microsoft 365 sous une vision sécurité
- Identifier les risques associés aux différentes parties
- Introduction aux outils de durcissement Microsoft
- Le chiffrement au sein de Microsoft 365
- Découverte de la console Sécurité et du SecureScore

#### Protection de l'identité

- Compréhension de l'identité sous Microsoft 365
- Planifier l'identité et l'authentification
- Créer, configurer et gérer des identités et des rôles
- Vue d'ensemble des spécificités liées à l'hybridation
- Implémenter l'architecture et les options AAD Connect adaptées
- Identifier les points de défaillances – Gérer les identités externes, tels que les partenaires ou clients

#### Gestion de l'identité sécurisée

- Mise en œuvre d'une stratégie d'authentification adaptée
- Introduction à Microsoft Entra
- Configurer les attributs de sécurités
- Authentification pass-through, MFA, SSPM, AD Smart, FIDO2, Kerberos, passwordless, OATH, HELLO...
- Mise en œuvre des packages de gouvernances de l'identité ; et des Conditional Access Policies
- Revue des accès utilisateurs
- Compréhension des sécurité par défaut
- Gérer : la protection par mot de passe et les seuils de verrouillage ; l'élévation de l'accès ; le contrôle d'application et le contrôle des sessions
- Mettre en œuvre : de l'accès privilégié ; et Azure AD Identity Protection

#### Microsoft Defender 365

- Tour d'horizon de la plateforme Microsoft Defender 365
- Mise en œuvre de Defender For Endpoint
- Durcissement des postes clients consommateurs de Microsoft 365 (MDM, MAM)

- Introduction à Microsoft Endpoint Manager et les modèles de durcissement
- Simuler des attaques

#### Mise en conformité

- Vue d'ensemble des outils de mises en conformité
- Implémenter des stratégies de conformité
- Gérer les accès conditionnels avancés
- Automatiser, investiguer et résoudre les incidents de conformités et de sécurité
- Former les équipes
- Gérer les Risk Management
- La RGPD et Microsoft 365
- Mise en œuvre de stratégies de communications
- Restreindre les communications

#### Protection des données

- Appréhender les différents types de données
- Introduction à l'Information Right Management (IRM)
- Implémenter l'empreinte des données
- Gérer les niveaux de confidentialités
- Appliquer des protections emails/fichiers basées sur les étiquettes
- Mise en œuvre : de Microsoft Purview et des DLP ; et des stratégies de protections contre la perte des données
- Gérer la rétention et le cycle de vie des données (DLM) au sein de l'architecture (Exchange, Teams, Sharepoint, Onedrive, etc)
- Gérer le risque interne (alertes, actions, modèles, mises en évidence)
- Introduction à Lockbox

#### Surveiller l'architecture

- Introduction à : Microsoft Sentinel et Microsoft Purview eDiscovery
- Mise en œuvre des journaux d'audits
- Recherche de contenu

#### Les bonnes pratiques de durcissement

- Bonnes pratiques de durcissements au sein de Microsoft Exchange Online
- Durcissements au sein de Microsoft Sharepoint Online et Onedrive, et de Microsoft Teams
- Bonnes pratiques Microsoft 365



4 jours / 28 heures



Réf. : M365-SEC



2 400€ HT



• 20 au 23 février  
• 22 au 25 avril  
• 1<sup>er</sup> au 4 juillet

• 10 au 13 septembre  
• 7 au 10 octobre  
• 9 au 12 décembre

## 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
- Connaître 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

### Prérequis\*

- Avoir une culture générale en informatique
- Connaître 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

### 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, etc.
- 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 chaîne de développement (DevSecOps)

\* 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. : DEVSEC



2 150€ HT



• 13 au 15 mai

• 25 au 27 novembre

## 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
- Connaître les outils et architectures permettant une administration sécurisée
- Acquérir les bonnes pratiques d'administration sécurisée

### Public visé

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

### Prérequis\*

- 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 sécurisée

- 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 / 28 heures



Réf. : SECUAD



2 850€ HT



• 2 au 5 avril

• 9 au 12 septembre

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



L'équipe Deloitte CyberAcademy 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](mailto:formations-cyber@deloitte.fr).

# 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 CyberAcademy 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-learning, 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** : Connaître les principaux risques informatiques ou a minima financier avec des exemples d'incidents parlants
- **Objectif 2** : Connaître la réglementation en matière de sécurité IT
- **Objectif 3** : Connaître 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

## 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 C-LEVEL

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 Prérequis
- 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 Prérequis
- 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 connaître les contours du Zero Trust

### Prérequis

- 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

#### Aspects organisationnels de mise en œuvre

- Cadrage
- Documents à préparer
- Conformité
- Considérations pratiques
- L'approche Deloitte



4 heures



Réf. : OTRUST



Sur demande



Sur demande

## 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



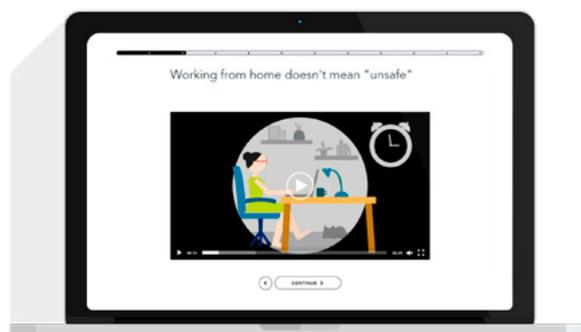
Sur demande

## 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



82% des cyber-attaques impliquent le facteur humain. Grâce à la Réalité Virtuelle, les collaborateurs sont en mesure de prévenir les risques et réagir face à la cybercriminalité. Ils sont plongés dans des mises en situations réalistes où ils apprennent par l'action. Lors de cette simulation innovante, ils alternent les points de vue de "l'attaquant" et de la "victime".



### Scénarios interactifs et immersifs

Mettez-vous dans la peau d'un collaborateur puis d'un hacker, et prenez des décisions à la 1<sup>ère</sup> 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



### Virilité 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-crédation 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 création 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 connaître 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 maîtriser les concepts d'ITIL 4.

### Prérequis

- Il n'y a pas de Prérequis 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.

Formation en partenariat

### 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€ HT



Disponible sur demande

## PMP - Project Management Professional

### Objectifs de la formation

- Réussir la certification PMP, Project Management Professional.
- Connaître les 5 groupes de processus du management de projet.
- Connaître 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 connaître les meilleures pratiques pour la gestion de projets selon PMI.

### Prérequis

- Il n'y a pas de Prérequis 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 Prérequis pour cette éligibilité sont liés à votre expérience professionnelle. Il est conseillé d'avoir à minima 5 années d'expérience professionnelle pour se lancer dans ce dossier d'éligibilité. N'hésitez pas à contacter nos experts formation pour en discuter.

Formation en partenariat

### 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€ HT



Disponible sur demande

## 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 connaître l'une des meilleures pratiques pour la gestion de projet.

### Prérequis

- Il n'y a pas de Prérequis 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.

Formation en partenariat

### 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. : PRINCE2F



1 350€ HT



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 Take<sup>2</sup> : 2ème passage possible sur l'examen PRINCE2 Practitioner.

### Public visé

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

### Prérequis

- Il n'y a pas de Prérequis 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.

Formation en partenariat

### 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. : PRINCE2P



1 350€ HT



Disponible sur demande

# Modalités d'inscription et contacts

Pour toute inscription aux formations Deloitte CyberAcademy, vous devez nous transmettre par courriel à [formations-cyber@deloitte.fr](mailto:formations-cyber@deloitte.fr) : les noms et prénoms du ou des participants, la ou les sessions de formation choisies, l'adresse postale de votre société et votre SIREN. 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.

Deloitte Conseil est enregistré sous le n° de déclaration d'activité 11 92 16 244 92 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 CyberAcademy au plus tard deux semaines avant le début de la formation, la demande de subrogation ne pourra être prise en compte par Deloitte CyberAcademy. 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 CyberAcademy.

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

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 :



**Monia Ulmann**  
Directrice CyberAcademy  
[mulmann@deloitte.fr](mailto:mulmann@deloitte.fr)  
+ 33 (0)1 40 88 25 92  
+ 33 (0)7 85 34 00 98



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



**Manal Aouak**  
Chargée de formation  
[maouak@deloitte.fr](mailto: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](mailto:mdeniega@deloitte.fr)  
+33 (0)1 55 61 79 14  
+33 (0)6 75 19 53 17

# Calendrier des formations au premier semestre 2024\*

L'ensemble de notre offre est également disponible en INTRA entreprise.  
Pour plus d'information : [formations-cyber@deloitte.fr](mailto:formations-cyber@deloitte.fr)

Sécurité organisationnelle	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Certified in Cybersecurity (ISC2)	New		11 au 12				
CISSP (ISC2)			4 au 8	22 au 26		3 au 7	
CCSP (ISC2)					13 au 17		
RSSI	New	26/02 au 01/03				10 au 14	
Préparation à l'examen CISA				22 au 26			
Préparation à l'examen de certification Certified Information Security Manager (CISM)						17 au 21	
Préparation à l'examen de certification Certified in Risk and Information Systems Control (CRISC)					13 au 17		
Gestion de crise IT/SSI				2 au 4			
NIS	New			29			
DORA	New			3			
Fondamentaux ISO 27001 & 27002					21 au 22		
Transition entre les normes ISO/IEC 27001:2013 > 2022 et ISO 27002:2013 > 2022	New		4 au 5				
ISO 27001 Lead Auditor			11 au 15			10 au 14	
ISO 27001 Lead Implementer - Français		5 au 9	25 au 29			3 au 7	
ISO 27005 Risk Manager - Français	29 au 31		18 au 20		27 au 29		
EBIOS Risk Manager 2018	New			22 au 24			
ISO 27032 Lead Cybersecurity Manager	22 au 26						
ISO 27035 Lead Incident Manager		5 au 9					
ISO 27701 Lead Implementer, Système de management de la protection de la vie privée				8 au 12			
ISO 31000 Risk Manager		26 au 28					
ISO 22301 Lead Auditor			25 au 29				
ISO 22301 Lead Implementer			18 au 22			24 au 28	

Sécurité juridique	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Droit de la Sécurité des Systèmes d'Information (SSI)					27 au 29		
RGPD : essentiel de la conformité			18 au 19				
Certification des Compétences du DPO conformément au référentiel de certification de la CNIL			11 au 15				

Sécurité technique	Janvier	Février	Mars	Avril	Mai	Juin	Juillet
Test d'intrusion et sécurité offensive							
Essentiels technique de la SSI						17 au 18	
Socle technique de la cybersécurité						17 au 19	
Cybersécurité industrielle						17 au 19	
Architectures réseaux sécurisées			6 au 8				
Investigation réseaux Wireshark	New	7 au 9				3 au 5	
Investigation numérique Windows		26 au 28				19 au 21	
Analyste SOC (Security Operation Center)	8 au 12		25 au 29			24 au 28	
Sécurité des serveurs et application web							
Microsoft 365 - Durcissement	New	20 au 23		22 au 25			1 <sup>er</sup> au 4
Développement Sécurisé					13 au 15		
Sécurité Active Directory				2 au 5			

\*Ce planning est susceptible d'être complété ou modifié.

# Calendrier des formations au second semestre 2024\*

L'ensemble de notre offre est également disponible en INTRA entreprise.  
Pour plus d'information : [formations-cyber@deloitte.fr](mailto:formations-cyber@deloitte.fr)

Sécurité organisationnelle		Septembre	Octobre	Novembre	Décembre
Certified in Cybersecurity (ISC2)	New		17 au 18		
CISSP (ISC2)		16 au 20		4 au 8	9 au 13
CCSP (ISC2)				18 au 22	
RSSI	New	23 au 27		25 au 29	
Préparation à l'examen CISA			7 au 11		
Préparation à l'examen de certification Certified Information Security Manager (CISM)					2 au 6
Préparation à l'examen de certification Certified in Risk and Information Systems Control (CRISC)					16 au 20
Gestion de crise IT/SSI				12 au 14	
NIS	New			12	
DORA	New			4	
Fondamentaux ISO 27001 & 27002				13 au 14	
Transition entre les normes ISO/IEC 27001:2013 > 2022 et ISO 27002:2013 > 2022	New		14 au 15		
ISO 27001 Lead Auditor			30/09 au 4/10		2 au 6
ISO 27001 Lead Implementer		16 au 20		4 au 8	16 au 20
ISO 27005 Risk Manager		9 au 11	14 au 16		9 au 11
EBIOS Risk Manager 2018	New		9 au 11		
ISO 27032 Lead Cybersecurity Manager		9 au 13			
ISO 27035 Lead Incident Manager			14 au 18		
ISO 27701 Lead Implementer, Système de management de la protection de la vie privée			21 au 25		
ISO 31000 Risk Manager		23 au 25			
ISO 22301 Lead Auditor			7 au 11		
ISO 22301 Lead Implementer				25 au 29	

Sécurité juridique		Septembre	Octobre	Novembre	Décembre
Droit de la Sécurité des Systèmes d'Information (SSI)				4 au 6	
RGPD : essentiel de la conformité			21 au 22		
Certification des Compétences du DPO conformément au référentiel de certification de la CNIL		16 au 20			9 au 13

Sécurité technique		Septembre	Octobre	Novembre	Décembre
Test d'intrusion et sécurité offensive		30/09 au 4/10			
Essentiels technique de la SSI					
Socle technique de la cybersécurité				18 au 22	
Cybersécurité industrielle					2 au 4
Architectures réseaux sécurisées		23 au 25			
Investigation réseaux Wireshark	New		7 au 9		
Investigation numérique Windows		16 au 18		12 au 14	
Analyste SOC (Security Operation Center)			21 au 25		
Sécurité des serveurs et application web					16 au 20
Microsoft 365 - Durcissement	New	10 au 13	7 au 10		9 au 12
Développement Sécurisé				25 au 27	
Sécurité Active Directory		9 au 12			

\*Ce planning est susceptible d'être complété ou modifié.

# 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 Deloitte Conseil. 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 CyberAcademy (Deloitte Conseil) 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 Prérequis attendu pour suivre les formations Deloitte CyberAcademy (Deloitte Conseil).

## 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 Deloitte Conseil au plus tard 15 jours avant le début de la formation.

Deloitte CyberAcademy (Deloitte Conseil) 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. Deloitte Conseil 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 Deloitte Conseil sous huitaine. Toute modification ultérieure apportée par le client devra faire l'objet d'un accord écrit de la part de Deloitte Conseil.

## 3. Modification, annulation et report

Toute annulation ou report d'inscription doit être signalé par téléphone et confirmé par écrit à Deloitte Conseil.

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, Deloitte Conseil 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, Deloitte Conseil facturera à hauteur de 50% du coût total de la formation ;
- dans les 15 jours ouvrés précédant le début de la formation, Deloitte Conseil 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 Deloitte Conseil. 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, Deloitte Conseil accepte que le client puisse, dans les 12 mois maximum suivant son absence, choisir une date future pour la même formation.

Deloitte Conseil 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. Deloitte Conseil 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 Deloitte Conseil. 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 Deloitte Conseil 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. Deloitte Conseil 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 Deloitte Conseil au plus tard deux semaines avant le début de la formation, la demande de subrogation ne pourra être prise en compte par Deloitte Conseil. 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 Deloitte Conseil.

## 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 Deloitte Conseil.

## 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 fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited (« DTTL »), à son réseau mondial de cabinets membres et à leurs entités liées (collectivement dénommés « l'organisation Deloitte »). DTTL (également désigné « Deloitte Global ») et chacun de ses cabinets membres et entités liées sont constitués en entités indépendantes et juridiquement distinctes, qui ne peuvent pas s'engager ou se lier les uns aux autres à l'égard des tiers. DTTL et chacun de ses cabinets membres et entités liées sont uniquement responsables de leurs propres actes et manquements, et aucunement de ceux des autres. DTTL ne fournit aucun service aux clients. Pour en savoir plus, consultez [www.deloitte.com/about](http://www.deloitte.com/about). En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

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

© Novembre 2023 Deloitte SAS - Membre de Deloitte Touche Tohmatsu Limited  
Designed by dot.