groupe cegos

Technologies et métiers du Numérique

Formations Cybersécurité

EDITION 2022

PARIS LA DÉFENSE · LYON · AIX-EN-PROVENCE · TOULOUSE · BORDEAUX · NANTES · RENNES · ROUEN · LILLE · STRASBOURG · SOPHIA ANTIPOLIS

Edito

Quelle que soit leur provenance - organisations gouvernementales, cabinets spécialisés, éditeurs de solutions, ... - les statistiques relatives à la cybersécurité sont aussi éloquentes qu'alarmantes. Et toutes montrent les mêmes tendances, à savoir que les attaques se multiplient à une vitesse phénoménale (plus de 400% d'augmentation depuis le début de la crise sanitaire) et qu'aucune organisation n'est à l'abri. Une étude de l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) consacrée à la menace rançongiciel révélait par exemple l'an passé que 11% des attaques qu'elle avait référencées concernaient les hôpitaux.
Et si les attaques dont les médias font écho touchent généralement des entreprises connues du grand public, les TPE/PME seraient victimes de 40% des incidents de sécurité.

Mais comment expliquer cette accélération ? D'une part en raison de la « professionnalisation » des cybercriminels qui sont de plus en plus compétents et organisés. Et d'autre part en raison d'une plus grande exposition aux risques de systèmes d'information qui offrent aux cybercriminels de nouvelles portes d'entrée avec la montée en puissance du télétravail. Si pendant longtemps les utilisateurs bénéficiaient de la protection du réseau de l'entreprise, c'est beaucoup moins vrai depuis qu'ils se connectent au dit réseau depuis leur domicile, et ce parfois même avec du matériel sur lequel les équipes informatiques n'ont pas la main.

Et aux dires de tous les spécialistes, la menace ne va faire que s'accroître dans les années à venir. Il n'y a effectivement aucune raison de penser que la tendance pourrait s'inverser alors que la liste des menaces et des victimes ne fait que s'allonger.

Fort heureusement, il existe des solutions. La première brique d'un dispositif efficace est la connaissance des risques puisque c'est en ayant conscience de ce à quoi le système d'information est exposé que l'on peut définir les leviers à activer. Il convient ensuite d'adopter les bons outils (firewall, antivirus,...) et de mettre en place des règles et des dispositifs qui complexifieront considérablement la tâche des personnes malveillantes. On agira par exemple sur la structure des mots de passe, sur les méthodes d'authentification et sur le chiffrement des données.
Il conviendra ensuite de tester la sécurité de son SI en menant des campagnes de pentest ou de stress-test. Il sera aussi pertinent de s'appuyer sur une ou plusieurs normes (ISO 2700x) pour s'assurer de l'efficacité globale de son dispositif. Et viendra enfin la mise en place d'un SOC (Security Operation Center) dont la mission sera de détecter, d'analyser et de gérer les incidents liés à la cybersécurité.

Mais au-delà de toutes ces mesures, il faudra agir sur les connaissances et les compétences. Les connaissances de ceux qui, bien involontairement, sont à l'origine de la majorité des incidents de sécurité, à savoir les utilisateurs qui doivent être fortement et régulièrement sensibilisés et responsabilisés. Et les compétences des acteurs de la DSI en charge de mener les actions (et bien d'autres) mentionnées ci-dessus.

ib et la cybersécurité

1 900
personnes formées en 2021

765
clients

96,2%
de participants satisfaits

Sommaire

Sommaire des formations

Sommaire des formations

Sommaire des formations

ib, en synthèse

Formations et séminaires interentreprises
(à distance et en présentiel)

Formations intra-entreprise et sur-mesure
(à distance et en présentiel)

Grands projets de formation
(conception et déploiement)

Aide au recrutement avec la Préparation Opérationnelle à l'Emploi

35 ans
au service
de nos clients

11 sites
de formation

88 salles
de formation
et 30 salles
volantes

145
collaborateurs

1150
formations
dont 1 050
accessibles
à distance

3000
sessions
intra et sur-mesure
formés chaque année

650
consultants-
formateurs
partenaires

Agréments et partenariats

10 bonnes raisons de choisir ib

1 Qualité et largeur des offres de formations

Choisir ib, c'est accéder à plus de 1 150 formations et séminaires dédiés aux technologies et métiers de l'informatique. C'est aussi profiter de dispositifs pédagogiques variés : présentiel, formations à distance, formations mixtes, solutions 100% digitales...

2 Des solutions multi-modales et digitales

Notre offre intègre de nombreuses formations mixtes (blended) qui associent au présentiel des activités digitales de différentes natures : modules e-learning, vidéocasts, rich média, quiz,... Accessibles en ligne avant, pendant ou après les phases de présentiel, ces modules digitaux renforcent l'efficacité de nos formations.

3 Des formations accessibles à distance

Avec notre solution de classes à distance, il est possible de suivre depuis n'importe quel lieu des formations animées par nos formateurs. Avec plus de 1000 formations proposées dans ce format, nous apportons une réponse efficace aux organisations qui souhaitent limiter les déplacements de leurs collaborateurs et optimiser leurs budgets.

4 Qualité des prestations

Notre recherche permanente de l'excellence s'est concrétisée par l'obtention de la certification ISO 9001 dès 1999, par notre référencement au Datadock et enfin par l'obtention de la certification Qualiopi. Les actions que nous engageons pour améliorer nos prestations se traduisent également par le niveau de satisfaction de nos stagiaires qui atteint 96,3% en 2021.

5 L'expertise des consultants-formateurs

Au-delà d'une expertise technique reconnue, nos consultants-formateurs ont en commun une réelle culture pédagogique qui garantit aux apprenants une appropriation optimale des programmes de formation. La note de 9,11 sur 10 que leur ont attribués les stagiaires en 2021 atteste de la qualité de nos formateurs.

6 Le savoir-faire pédagogique d'un groupe reconnu

Les synergies entretenues avec la Cegos, notre maison mère, favorisent la mise en œuvre les principes, méthodes et outils pédagogiques qui ont fait le renom du leader européen de la formation professionnelle. Cette pédagogie unique à l'efficacité reconnue guide toutes nos actions de conception et d'animation.

7 Qualité des sites de formation et de l'accueil

Parce que la qualité d'un environnement de travail est un élément indispensable à la réussite d'une formation, nous proposons des cadres conviviaux, propices à l'apprentissage et à la mise en pratique de nouveaux savoirs. Et tous nos centres offrent un accès rapide à des solutions d'hébergement et de restauration.

8 Une présence nationale

De par notre présence dans 11 grandes métropoles, nous proposons à nos clients des solutions de formation de proximité et mettons à leur disposition des interlocuteurs disposant d'une bonne connaissance de leurs contextes régionaux

9 Maintien des sessions

Nous mettons tout en œuvre pour améliorer continuellement nos capacités de maintien. En optimisant et en ajustant nos planifications et en mobilisant en permanence nos équipes, nous formons 90% des stagiaires à la date choisie au moment de leur inscription.

10 Un accès à de nombreux dispositifs de financement

Partenaire des OPCO, ib vous permet de bénéficier de dispositifs de financement de la formation tels que les Actions Collectives ou les POE. Et bien sûr, ib vous propose de nombreuses formations éligibles au CPF et vous accompagne dans le cadre du FNE Formation.

Parcours introductif à la Cybersécurité

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

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

Dans un contexte de transformation numérique accélérée, de digitalisation des flux et des activités, d'évolution des modes de vie (nomadisme, télétravail,...) et de tensions internationales, les risques liés à la cybercriminalité sont chaque jour plus importants. Il est donc logique que la cybersécurité soit aujourd'hui au cœur des préoccupations de tous. Mais de quoi parle-t-on réellement ? Que se cache-t-il derrière ce terme ? Ce parcours est précisément étudié pour apporter une vision élargie de ce qu'est la cybersécurité aux personnes s'orientant vers ce domaine comme à celle souhaitant plus simplement étendre leurs connaissances sur le sujet. A l'issue de 10 journées de formation, les participants disposeront d'un bon niveau de compréhension des menaces et des risques qui pèsent sur les organisations et des dispositifs (règlements, normes, outils, bonnes pratiques...) permettant de s'en prémunir.

OBJECTIFS

- Disposer d'une vision globale de la cybersécurité et son environnement (enjeux, écosystème...)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique

Public

- Toute personne souhaitant apprendre les fondamentaux de la sécurité informatique et/ou souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux

Pré-requis

Connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI

Les + de cette formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de bénéficier de nombreuses mises en situations et de disposer de beaucoup de pratique (environ 65% du temps), pour une meilleure assimilation des concepts techniques liés à la sécurité.

Programme

1ère partie (3 jours)

1 - Initiation à la cybersécurité

- Les enjeux de la sécurité des systèmes d'information : les enjeux, pourquoi les pirates s'intéressent-ils au SI, la nouvelle économie de la cybersécurité
- Les besoins de sécurité, les notions de base et vocabulaire
- Panorama de quelques menaces
- Exemples d'attaques connues et leurs modes opératoires
- Les différents types de Malwares

2 - Les bases de la sécurité numérique

- Détection de tentatives d'hameçonnage
- Identification des courriels indésirables ou dangereux
- Navigation sur Internet en toute sécurité
- Maîtrise des données personnelles et des informations de navigation
- Génération de mots de passe robustes
- Protection de la vie privée en ligne
- Gérer son e-réputation
- Chiffrement des données
- Protection de l'ordinateur
- Précautions relatives à la sécurité

2ème partie (3 jours)

1 - Sécurité des réseaux : translation et filtrage du trafic réseau

- La pile protocolaire TCP/IP
- Les différents mécanismes de translation d'adresses IP (NAT, PAT)
- Les contrôle d'accès vie des listes d'accès (ACL)

2 - Sécurité des réseaux : firewalls et architectures de sécurité

- Les pare-feu, Proxy et Reverse Proxy
- Architecture de sécurité et scénarios de déploiement
- Cloisonnement et segmentation logique

3 - Sécurité des réseaux : VPN, IDS/IPS et sécurité des réseaux sans-fil

- Les systèmes de détection d'intrusion IDS/IPS
- Les réseaux virtuels privés (VPN)
- Sécurité des réseaux sans-fil

3ème partie (2 jours)

1 - Sécurité des échanges et cryptographie

- Les besoins en cryptographie
- Les crypto-systèmes symétriques et asymétriques
- Les fonctions de hachage
- Les infrastructures à clé publiques PKI
- Les certificats électroniques et les protocoles de validation
- La signature numériqueLe protocole SSL

2 - Concepts fondamentaux de la sécurité applicative et OWASP

- Qu'est-ce que la sécurité applicative ?
- Statistiques et évolution des failles liées au Web et impacts
- Le nouveau périmètre de la sécurité
- Présentation de l'OWASP
- Les risques majeurs des applications Web selon l'OWASP
- Les attaques par injection (commandes injection, SQL Injection, LDAP injection, XXE...)
- Les attaques par violation de l'authentification et du contrôle d'accès
- Les mauvaises configurations de sécurité et l'insuffisance de la surveillance et de la journalisation
- L'exposition des données sensibles
- Les attaques "Cross Site Scripting" ou XSS
- L'utilisation de composants présentant des vulnérabilités connues
- Les attaques par dé sérialisation non sécurisée
- Autres outils OWASP : OWASP Application Security Guide, OWASP Cheat Sheets, OWASP ASVS, OWASP Dependency Check, OWASP ZAP, OWASP ModSecurity....

4ème partie (2 jours)

1 - La gestion de la cybersécurité au sein d'une organisation

- Intégrer la sécurité au sein d'une organisation et dans les projets : panorama des normes ISO 2700X, système de management de la sécurité de l'information (ISO 27001), code de bonnes pratiques pour le management de la sécurité de l'information (ISO 27002), gestion des risques (ISO 27005), classification des informations, gestion des ressources humaines
- Intégrer la sécurité dans les projets : sécurité dans l'ensemble du cycle de vie d'un projet, approche par l'analyse et le traitement du risque et plan d'action SSI
- Difficultés liées à la prise en compte de la sécurité : compréhension insuffisante des enjeux, implication nécessaire de la direction, difficultés pour faire des choix en toute confiance, délicat arbitrage entre commodité et sécurité, frontières floues entre sphères professionnelle, publique, et privée
- Métiers liés à la cybersécurité

2 - Les enjeux et les risques liés à la gestion des données personnelles

- Le concept de vie privée
- Les empreintes laissées par vos données
- Contrôle de l'accès aux données
- Protection du transfert des données sur les réseaux
- Le cadre légal
- Exploration du RGPD

Réf. MG847
10 jours (3+3+2+2)
(70h présentiel)

6 350 €HT

Paris 230 €HT

À DISTANCE
12/09 & 03/10 & 24/10 & 07/11

PARIS
12/09 & 03/10 & 24/10 & 07/11

Autres sites, nous consulter

Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Comprendre la sécurité informatique

SÉMINAIRE

ACCESSIBLE À DISTANCE

La sécurité informatique est devenue une préoccupation de tous les utilisateurs d'Internet et des Systèmes d'Information au même titre qu'elle l'est (depuis longtemps déjà) pour les professionnels de l'informatique. Si, pour certains d'entre nous, la notion de sécurité informatique reste encore confuse, voire même abstraite, il n'en reste pas moins vrai que tous autant que nous sommes, nous commençons dans notre quotidien à en mesurer l'importance. Ce séminaire de "vulgarisation" explique son concept, ses acronymes, son jargon et présente les différents moyens disponibles pour la mettre en œuvre. Il permet donc clairement aux participants de se familiariser avec la sécurité informatique et de disposer des connaissances nécessaires pour communiquer et collaborer avec des équipes techniques internes, des prestataires ou des fournisseurs spécialisés dans le domaine.

OBJECTIFS

- **Comprendre les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour travailler avec les spécialistes et piloter les prestataires**
- **Acquérir la vision globale de la sécurité**
- **Connaître les rôles des intervenants du secteur et leurs métiers**
- **Identifier les nouveaux enjeux associés à la sécurité informatique**

Public

- Commerciaux, spécialistes du marketing, futurs consultants, chefs de projets ou responsables de formation amenés à évoluer dans l'univers de la sécurité informatique
- Toute personne souhaitant comprendre la sécurité informatique pour optimiser leur collaboration avec les spécialistes du domaine

Pré-requis

Aucun

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €). L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de ce séminaire

- Une description des technologies et concepts illustrée d'exemples de solutions concrètes et des usages actuels.
- Un effort particulier de vulgarisation des technologies complexes rendant le séminaire accessible aux non spécialistes de l'informatique et de la sécurité.

Réf. **SR105**
2 jours
(14h présentiel)

1 390 €HT
Offerte

À DISTANCE	09/11
PARIS	09/11

Autres sites, nous consulter

Programme

1 - Principes généraux de la sécurité informatique
- Domaines concernés : intégrité, disponibilité, confidentialité, authentification, imputation, traçabilité...
- Démarche générale à entreprendre / analyse de risques
- Notions à connaître : authentification simple et forte - Système de confirmation 3D, défense en profondeur, PRA/PCA...

2 - Comprendre les différents types de vulnérabilités et d'attaques
- Malwares : cheval de Troie, Virus, Rootkit, Spyware...
- Attaques : terminal, réseaux, applications (Sniffing, DCI/DCI, DDoS...)
- Attaques de mots de passe, injection SQL, vol d'identité et de données
- Attaques non-malwares : attaques de phishing (hameçonnage)
- Évaluation des risques

3 - Connaître le fonctionnement des équipements de protection dédiés aux :
- Solution de gestion des mots de passe
- Cryptage : triple DES / AES
- Séparation des flux par la formation des réseaux virtuels (VLAN)
- Cryptage des données en ligne (VPN SSL et VPN IPSec)
- Authentification d'accès : authentification forte, Network Access Control (NAC) et Role Based Access Control (RBAC)
- Filtrage : firewalls protocolaires, de contenus, d'applications, d'identité...
- Filtrage des applications Web : WAF (Web Access Firewall)
- SIEM (Security Information and Event Management)
- IAM (Identity et Access Management)
- DLP (Data Lost Prevention) - Data Masking – Cryptage
- Empreintes logicielles et MAC (Mandatory Access Control)
- Autres domaines spécifiques

4 - Exploiter les plates-formes spécialisées de sécurité
- Plate-forme de Cloud de Sécurité (SecaaS : Security as a Service)
- Plate-forme de gestion et de sécurité des mobiles EMM (Entreprise Mobility Management)
- Plate-forme de sécurité NGFW (Next Generation of Firewall)

5 - Utiliser la combinaison des équipements pour sécuriser
- L'Internet (communication et transaction) : cryptologie PKI (Public Key Infrastructure)
- Les réseaux sans-fil Wifi : 802.11i (802.1X/EAP...) / WPA / WPA2 / WPA3
- Terminaux et applications mobiles et le télétravail (ODE, conteneurisation, App Stores, empreintes logicielles, App Wrapping...) / Banalisation du terminal et publication d'application (TS-WEB, VDI...)
- Le BYOD (utilisation des équipements personnels dans le cadre professionnel)
- La protection du Cloud et du Big Data (encryptions, vol de données, flux de données...)

6 - Mesurer les impacts de la mise en place de la sécurité sur :
- La performance du système global du système informatique
- L'architecture du système d'information

7 - S'appuyer sur les référentiels pour gérer la sécurité informatique
- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
- ENISA (organisme Européen - gestion des risques), NIST (standards suivis par des grands acteurs du secteur de sécurité)
- CSA (Cloud Alliance Security) / CSA Big Data / CSA Mobile
- CNIL/RGPD (Obligation Légale de sécurité)
- Critères communs
- CVE

8 - Grandes tendances
- Limites des solutions actuelles de sécurité
- Cybersécurité : recours à l'intelligence artificielle et à la machine learning
- Security Self Healing System et Software Defined Security
- BlockChain

État de l'art de la sécurité des Systèmes d'Information

Définition de la politique de sécurité et maîtrise des risques

SÉMINAIRE · ACCESSIBLE À DISTANCE · FORMATION MIXTE

Pour faire face à la montée en puissance des nouvelles menaces qui pèsent sur nos systèmes d'information, le monde de la sécurité doit s'adapter, et est de fait en perpétuelle évolution aussi bien sur le plan des technologies que sur celui des méthodes et modèles conceptuels sous-jacents. Ce séminaire de 3 jours dresse un état de l'art complet des outils organisationnels, méthodologiques et techniques de maîtrise du risque informatique. Il permettra aux participants de disposer des informations nécessaires à l'élaboration d'une feuille de route menant à la mise en place d'une politique de sécurité efficace.

OBJECTIFS

- Identifier les différents domaines de la sécurité et de la maîtrise des risques liés aux informations
- Connaître les principes et les normes de chaque domaine de la SSI
- Disposer d'informations sur les tendances actuelles au niveau des menaces et des solutions à notre disposition
- Pouvoir améliorer la communication entre la maîtrise d'ouvrage, la maîtrise d'œuvre et la SSI
- Être en mesure d'effectuer des choix techniques

Public

- Directeurs des systèmes d'information ou responsable informatique, RSSI, chefs de projet sécurité, architectes informatiques

Pré-requis

Bonne connaissance générale des systèmes d'information

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €). L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de ce séminaire

- Une approche favorisant les échanges entre les participants et un formateur qui accompagne les DSI ou les RSSI depuis plusieurs années.
- Un programme actualisé qui prend fortement en compte le contexte actuel et les obligations réglementaires en vigueur.
- Les contenus digitaux mis à disposition des participants avant et après la formation renforcent l'efficacité pédagogique du programme et garantissent un bénéfice durable de l'action de formation.

Réf. SEM54
3 jours
(21h présentiel)

2 250 € HT
Offerte

À DISTANCE	12/09, 28/11
PARIS	12/09, 28/11

Autres sites, nous consulter

Programme

1 Avant le présentiel

Pour aborder la formation dans les meilleures conditions, retrouvez sur le Learning Hub ib :
- Un quiz de consolidation des pré-requis

2 En présentiel

1 - Introduction

2 - Évolutions des menaces et les risques
- Statistiques sur la sécurité
- Tendances dans l'évolution des menaces

3 - Modèle d'approche et maturité effective de l'organisme
- Identification des acteurs : organisation et responsabilités
- Exigences SSI : obligations légales métiers, responsabilités civiles, responsabilités pénales, règlements, délégations

4 - L'identification des besoins DICP consécutifs aux enjeux
- Classification SSI : informations, données et documents, processus, ressources, les pièges
- Identification des menaces et des vulnérabilités : contextuelles métiers, contextuelles IT
- Cartographie des risques : gravité / vraisemblance, niveaux, traitement du risque, validation des risques résiduels

5 - L'état de l'art des méthodologies et des normes
- Bonnes pratiques SSI : les acteurs, les textes de référence, avantages et inconvénients ; les règles d'hygiène ANSSI, les fiches CNIL, le chapitre 7 RGS
- Approche enjeux : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27002
- Approche SMSI : les acteurs, les textes de référence, avantages et inconvénients ; ISO 27001

6 - Modélisation des niveaux de maturité des technologies SSI
- Les choix structurants et non structurants et positionnements dans la courbe de la pérennité
- La sécurité des accès : filtrage réseau, identification, authentification (faible, moyenne, forte), gestion des identités vs. SSO, habilitation, filtrage applicatif (WAF, CASB et protection du Cloud), détection/protection d'intrusion, journalisation, supervision
- La sécurité des échanges : algorithmes, protocoles, combinaisons symétriques et asymétriques TLS, certificats, IGCP, les recommandations ANSSI
- Infrastructures de clés publiques : autorités de certification et d'enregistrement, révocation
- Le cas du DLP : architecture

7 - Nomadisme
- Sécurité des postes nomades : problèmes de sécurité liés au nomadisme
- Protection d'un poste vs. solutions spécifiques
- Mise en quarantaine
- Accès distants
- VPN : concept et standards de VPN sécurisé, intérêts du VPN, contrôle du point d'accès

8 - Les architectures de cloisonnement
- La sécurité des VLAN et hébergements, DMZ et échanges, sécurisation des tunnels, VPN Peer to Peer et télé accès, de la sécurité périphérique à la sécurité en profondeur

9 - La sécurité des end point
- Le durcissement : postes de travail, ordi phones, serveurs
- L'adjonction d'outils : postes de travail, ordi phones, serveurs
- La sécurité des applications : les standards et les bonnes pratiques

3 Après le présentiel

Retrouvez sur le Learning Hub ib :
- Un quiz pédagogique pour évaluer vos acquis et approfondir les sujets de votre choix
- Des vidéocasts pour revenir sur les points clés de la formation

Le learning hub ib

Vous êtes inscrit à une formation mixte ib ?
Retrouvez sur le Learning Hub l'ensemble des activités digitales intégrées à votre parcours (quiz, vidéocasts, modules e-learning,...).

Avec le Learning Hub, confortez vos pré-requis grâce à des quiz pédagogiques, des vidéos ou des modules e-learning, testez vos acquis et approfondissez les sujets de votre choix avec nos quiz post-formation et nos vidéocasts. Consultez enfin nos vidéos-tutos pour bénéficier de l'accompagnement de nos experts dans la mise en œuvre de vos nouveaux savoirs.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Cybersécurité - Synthèse technique

Comprendre les risques et mesurer les enjeux

ACCESSIBLE À DISTANCE

L'interconnexion grandissante des réseaux, l'adoption du Cloud, le recours aux messageries en mode SaaS, l'utilisation de containers et la multiplication des applications et services web sont autant d'évolutions techniques qui fragilisent la sécurité globale des systèmes d'information. Et les risques qui pèsent sur les données des entreprises sont considérablement accrus en raison du fait que celles-ci sont aujourd'hui hébergées chez des fournisseurs de services qui constituent une cible privilégiée pour les hackers qui y voient l'opportunité de s'approprier des masses considérables d'informations. Cette synthèse technique permettra aux participants d'identifier les nouvelles menaces qui pèsent sur les données de l'entreprise et de comprendre quelles évolutions techniques et organisationnelles peuvent permettre de s'en prémunir.

OBJECTIFS

- Connaître l'entendue des risques qui pèsent sur les informations de l'entreprise
- Comprendre l'évolution des analyses de risque pour faire face aux nouvelles menaces
- Identifier les risques associés à l'émergence de nouvelles technologies
- Savoir mettre en œuvre une gouvernance efficace
- Comprendre l'intérêt de disposer d'une surveillance et d'une gestion des incidents de dernière génération

Public

- Tout manager de la DSI impliqué dans la sécurité

Pré-requis

Aucun

Les + de cette formation

- Un accent particulier est mis sur les bonnes pratiques de gouvernance de la sécurité.
- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - État de l'art et évolution de la cybersécurité

- Cybersécurité : nouveaux acteurs et nouvelles portées
- Sécurité et juridique
- CNIL ANSSI
- ENISA
- Les normes, certifications et labels sécurité

2 - Évolution des analyses de risques

- Comprendre les analyses de risques
- Les cartographies
- Modélisation de la menace
- Risque IT vs risque personne concernée
- Rapport d'analyse de risques
- Les mesures de sécurités et le ROSI

3 - La gouvernance de la sécurité

- Les indicateurs de sécurité performants
- Les indicateurs de sécurité efficaces
- Le TBSSi
- Matrice des compétences cyber
- RSSI évolution des fonctions
- DPO rôles et missions

4 - Évolutions technologiques

- État des menaces et attaques contemporaines
- Dissection d'une APT
- Les nouvelles architectures sécurisées
- Automatisation et sécurité
- L'IA et la sécurité
- Sécurité des systèmes embarqués et iot
- Sécurité dans le développement
- La sécurité en environnement Cloud
- Mobilité et sécurité

5 - Surveillance et gestion des incidents

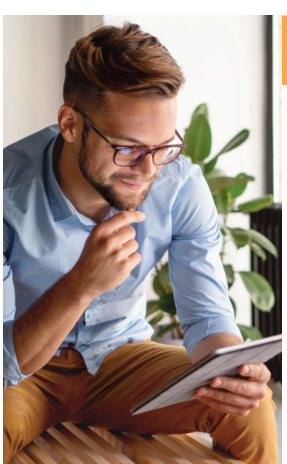
- Gestion et automatisation de la cartographie
- Sécurité offensive
- Supervision de la sécurité Gestion des incidents, SIEM, SOC CSIRT
- La cyber résilience
- Les CERT et gestion d'un programme de cyber sécurité

Réf. SE099
3 jours
(21h présentiel)

2 430 €HT
Offerte

À DISTANCE
13/06, 03/10
PARIS
13/06, 03/10

Autres sites, nous consulter



290 formations au format mixte en 2022

Des solutions multi-modales et digitales pour une nouvelle expérience d'apprentissage

Notre offre intègre de nombreuses formations mixtes (blended) qui associent à la formation en salle des activités digitales de différentes natures : modules e-learning, vidéocasts, rich média, classes virtuelles, Rapid Learning, quiz,...

Nous proposons ainsi des **dispositifs d'apprentissage entièrement tournés vers l'apprenant** qui reposent sur une combinaison optimisée de différentes modalités et qui renforcent ainsi l'efficacité et la rapidité de l'apprentissage.

Conçus par nos experts, les contenus digitaux qui enrichissent nos formations tout en permettant dans de nombreux cas d'en optimiser la durée sont accessibles à distance sur le Learning Hub ib avant, pendant ou après les phases de présentiel.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Sensibilisation à la cybersécurité

Sécurité des SI, des données personnelles et continuité d'activité

NOUVEAUTÉ N · SÉMINAIRE S · ACCESSIBLE À DISTANCE

L'utilisation des ressources du système d'information n'est pas sans risque. Cette sensibilisation présente à l'aide de très nombreux exemples les bonnes pratiques de l'utilisateur sédentaire, nomade ou en télétravail pour limiter les risques d'erreur ou de malveillance.

OBJECTIFS

- **Découvrir les bonnes pratiques pour limiter les risques juridiques et opérationnels**
- **Comprendre comment protéger les informations en adéquation avec les besoins métiers**

Public

- Tous les salariés d'une entreprise

Pré-requis

Aucun

Les + de ce séminaire

- L'approche méthodologique participative de ce séminaire permet des échanges entre les participants et le formateur sur des retours d'expériences concrets.
- Le formateur intervient auprès des comités de direction, des DSI, RSSI, Directions techniques opérationnelles, Chefs de projet, Administrateurs et utilisateurs de plusieurs administrations françaises et groupes internationaux privés de première importance.
- Support de cours remis sur clé USB ou lien de téléchargement.

Réf. **SR104**
1 jour
(7h présentiel)

890 €HT
Offerte

À DISTANCE	30/09, 25/11
PARIS	30/09, 25/11

Autres sites, nous consulter

Programme

1 - Introduction
- Les préjugés à surmonter
- Les valeurs essentielles à protéger
- Les périmètres
- Les menaces

2 - L'organisation et les responsabilités
- La direction générale
- Les directions métiers
- La DSI
- Les sous-traitants
- La voie fonctionnelle SSI et le RSSI
- La voie fonctionnelle protection de la vie privée et le DPO
- Les administrateurs techniques et fonctionnels
- Les utilisateurs

3 - Les référentiels SSI et vie privée
- Les politiques
- Les chartes
- Les guides et manuels
- Les procédures

4 - Vision synthétique des obligations légales
- Disciplinaire
- Contractuelle
- Civiles
- Pénales
- Le cas du contrôle par l'employeur : utilisation professionnelle et non-professionnelle

5 - Les menaces
- La divulgation d'information "spontanée"
- L'ingénierie sociale et l'incitation à dire ou faire
- Le lien avec l'intelligence économique
- Le lien avec l'espionnage industriel

6 - Les risques
- Vol, destruction
- Virus
- Les aspirateurs à données
- Le phishing /l'hameçonnage
- Les malwares
- Les spywares
- L'usurpation
- Les virus
- Le cas des réseaux sociaux

7 - Les bonnes pratiques d'évaluation de la sensibilité de l'information
- La classification par les impacts, (juridiques, opérationnels, financiers, image, sociaux)
- L'échelle d'impact
- Les pièges

8 - Les bonnes pratiques pour les comportements généraux
- A l'intérieur des établissements
- A l'extérieur des établissements

9 - Les bonnes pratiques d'utilisation des supports d'information sensible pour les phases de conception, stockage, échanges et fin de vie
- Papier
- Environnement partagé
- Environnement individuel sédentaire
- Environnement individuel mobile

10 - Les bonnes pratiques d'utilisation des ressources du système d'information
- Installation et maintenance : postes fixes, équipements nomades, portables, ordiphones
- Identification et authentification
- Échanges et communications : intranet, internet, contrôle des certificats serveurs, les échanges de fichiers via la plate-forme "institutionnelle", le nomadisme, les télétravailleurs et le VPN de télé accès, email, la consultation en Web mail, signature, chiffrement, Cloud, réseaux sociaux et forums thématiques professionnels et privés, téléphonie
- Stockages et sauvegardes (clés usb, locales, serveurs, ...)
- Archivages
- Anonymisation
- Destruction ou recyclage

11 - Conclusion
- Les engagements de responsabilité

Cybercriminalité - Enjeux et défis

Comment se protéger de la Cybercriminalité

NOUVEAUTÉ N · SÉMINAIRE S · ACCESSIBLE À DISTANCE

La cybercriminalité est une menace qui touche toutes les organisations, sociétés, administrations. Elle a explosé de 60% entre 2019 et 2020. La question qui importe est de savoir si votre organisation sera prête lorsqu'elle se fera attaquer.

OBJECTIFS

- Comprendre les enjeux de la cybercriminalité
- Être capable d'identifier les biens essentiels à protéger
- Pouvoir identifier les sources de risques dans son organisation
- Comprendre comment détecter des actes de malveillance
- Savoir réagir face à un acte de malveillance

Public

- RSSI, Fonction SSI, direction générale, DSI, juristes

Pré-requis

Aucun

Les + de ce séminaire

- Exemples de faits et incidents de sécurité réels et récents et jurisprudence en France et en Europe.
- Evaluation des compétences par un quizz en cours et en fin de formation.

Réf. SEM95
2 jours
(14h présentiel)

1 895 €HT
Offerte

À DISTANCE	23/06, 06/10
PARIS	23/06, 06/10

Autres sites, nous consulter

Programme

1 - L'évolution de la cybercriminalité
- Internet aujourd'hui, données et chiffres
- Les nouveaux marchés de la cybercriminalité
- Approche économique de la cybercriminalité
- Comprendre le darknet
- Les outils des cybercriminels (botnets, attaques etc...)
- Quelques typologies d'attaque

2 - Droit des TIC et organisation de la cybersécurité en France
- Organisation de la cybersécurité en France
- Contexte juridique
- Droit des TIC
- La lutte contre la cybercriminalité, ANSSI et cybermalveillance
- Le rôle de la CNIL et la protection des données personnelles

3 - Protéger son organisation
- Lexique et définitions (vulnérabilités, menaces, risques...)
- Les enjeux des Systèmes d'Information
- Identifier les biens essentiels et les biens supports
- Intégrer la sécurité au sein de son organisation
- Intégrer la sécurité au sein d'un projet
- Identification des difficultés liées à la prise en compte de la sécurité

4 - Identifier et prévenir les sources de risques
- Gouvernance et cybersécurité, définition des rôles et responsabilités
- Définir une stratégie de sécurité des systèmes d'information
- La Charte Informatique
- La gestion des contrats
- Mettre en place un système de gestion des risques
- Aperçu des ISO 27001 et 27005

5 - Prévenir les risques : les bonnes pratiques
- Les contrôles d'accès (physiques, logiques...)
- La gestion des comptes administrateurs
- La gestion des mots de passe
- Gérer les développements, les mises à jours et les déploiements
- Mettre en place une procédure d'escalade d'incidents
- Procédures ANSSI et CNIL de déclaration d'actes de malveillance

Panorama des techniques de hacking et de contre-mesures

Connaître les attaques SI les plus courantes

SÉMINAIRE

ACCESSIBLE À DISTANCE

Comment les hackers exploitent les failles de nos systèmes ? Quels sont les risques encourus ? Comment s'en prémunir ? Autant de questions auxquelles les responsables du système d'information sont confrontés. Les participants à cette formation de 3 jours découvriront les attaques les plus courantes, qu'elles portent sur les données, le réseau ou encore les serveurs Web, et seront à même d'identifier les failles de leur système d'information puis de prendre les mesures nécessaires pour le protéger.

OBJECTIFS

- Comprendre les risques, évaluer leur portée
- Savoir identifier les techniques de hacking et repérer les failles
- Connaître les mesures à adopter et savoir engager des actions préventives et correctives
- Définir les priorités d'investissement en termes de sécurité

Public

- Responsable réseau
- Toute personne en charge de la sécurité
- Cette formation ne convient pas aux développeurs
- Ce séminaire étant relativement généraliste. Pour des formations techniquement plus approfondies, nous vous invitons à consulter les programmes des formations "Hacking et Sécurité - Les fondamentaux " (SE100) et "Hacking et Sécurité - Niveau avancé" (SE101)

Pré-requis

Avoir suivi les formations "Sécurité systèmes et réseaux - Mise en œuvre" (SR211) ou "Sécurité systèmes et réseaux - Les fondamentaux" (SR220) ou connaissances équivalentes

Les + de ce séminaire

- L'acquisition de techniques d'identification des failles de sécurité et de traitement des attaques.
- Ce séminaire apporte l'adoption du point de vue des hackers pour une meilleure compréhension des risques encourus.

Réf. SR225
3 jours
(21h présentiel)

ORGANISÉ SUR DEMANDE, NOUS CONSULTER

Programme

1 - Introduction et définition
- La sécurité informatique, pour quoi, pour qui ?
- Le hacking se veut éthique
- Connaître son ennemi pour s'en défendre

2 - Méthodologie d'une attaque
- Préambule
- Cibler ma victime
- L'attaque
- Introduire le système et assurer son succès
- Bilan de l'intrusion et sécurisation

3 - Social Engineering
- Brève histoire d'une technique vieille comme le monde
- Ingénierie sociale : pourquoi ?
- Solution de protection
- Pour aller plus loin

4 - Les failles physiques
- Généralités
- Accès direct à l'ordinateur : accès à un ordinateur éteint (BIOS protégé et non protégé) et accès à un ordinateur allumé

5 - Les prises d'empreinte
- Le hacking éthique
- Collecte d'informations : le footprinting, le fingerprinting, découverte de failles potentielles, le reporting, sites internet

6 - Les failles réseaux
- Généralités
- Rappel sur les réseaux TCP/IP
- Outils pratiques
- Dos et DDos
- Sniffing
- Man in the middle (avec petit TP)
- Vol de session TCP HIJACKING
- Failles Wifi
- IP over DNS
- La téléphonie sur IP

7 - Les failles systèmes
- Généralités
- Les mots de passe
- Utilisateurs, groupes et permissions sur le système
- Élévations des privilèges
- Le processus
- Le démarrage
- L'hibernation
- Les appels de procédures distantes
- La virtualisation
- Les logs, les mises à jour et la sauvegarde
- Bilan

8 - Risques juridiques et solutions
- Préambule
- Atteintes à un système d'information
- Atteintes aux traitements de données à caractère personnel
- Infractions classiques applicables à l'informatique
- Solutions et préconisations

Toutes nos formations en détail sur...

www.ib-formation.fr

Avis de l'expert, parcours pédagogiques, publics, dates, ...
tout ce qu'il faut savoir sur nos formations est sur notre site.
Découvrez également nos tests de pré-requis en ligne et nos conseils pour aller plus loin dans l'expertise.

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Devenir Responsable de la Sécurité du Système d'Information

Toutes les dimensions du métier

ACCESSIBLE À DISTANCE

FORMATION MIXTE

Tout le monde s'accorde à dire qu'une des pires choses qui puisse aujourd'hui arriver à une organisation (entreprise, administration, agence gouvernementale,...) est une cyber attaque entrainant une paralysie partielle ou totale de son activité ! Et ce sans même parler de vol de données qui, au-delà des conséquences immédiates de l'attaque en termes d'activité, entacherait durablement la réputation de l'organisation victime. On comprend dès lors pourquoi la protection de l'information et la sécurité des systèmes d'information revêt aujourd'hui une telle importance que les professionnels qui en ont la responsabilité sont de plus en plus impliqués dans les processus de gouvernance des organisations qui les emploient. Pour mener à bien leur mission, ils ne doivent donc plus seulement être "bon" techniquement, ils doivent également savoir construire et mettre en œuvre des politiques de sécurité efficaces.

OBJECTIFS

- Identifier toutes les facettes du métier de Responsable de la Sécurité du SI, son rôle et ses responsabilités
- Savoir construire une politique de sécurité efficace et gérer les risques du SI
- Avoir une vue d'ensemble des mesures techniques de protection des SI
- Disposer d'une méthodologie pour assurer la mise en œuvre et le suivi de la sécurité
- Connaître les bonnes pratiques pour construire son plan d'action et définir ses indicateurs

Public

- Responsables métiers ou informatiques souhaitant évoluer vers le métier de RSSI
- RSSI opérationnels souhaitant appréhender les nouvelles missions du RSSI

Pré-requis

Bonne culture générale sur les infrastructures IT

Les + de cette formation

- Un tour d'horizon exhaustif des différents aspects de la mission de RSSI.
- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des RSSI depuis plusieurs années dans l'accomplissement de leurs missions.
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des SI. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.
- Les contenus digitaux mis à disposition des participants avant et après la formation renforcent l'efficacité pédagogique du programme et garantissent un bénéfice durable de l'action de formation.

Programme

1 Avant le présentiel

Pour aborder la formation dans les meilleures conditions, retrouvez sur le Learning Hub ib :

- Un quiz de consolidation des pré-requis

2 En présentiel

1ère partie : le métier de RSSI, son rôle, ses responsabilités, son périmètre d'action et ses méthodes de travail (4j)

1 - Introduction : Quels sont les enjeux de la SSI ?

- Quelques définitions, périmètres et terminologies de base - Enjeux, menaces et risques

2 - Les missions du RSSI

- Conseiller la Direction Générale par rapport aux obligations légales et les risques SSI
- Formaliser une stratégie et définir un plan d'actions
- Définir un référentiel SSI
- Participer à la mise en en place de la gouvernance
- Conseiller et assister la maîtrise d'ouvrage et la maîtrise d'œuvre
- Former, sensibiliser - Réaliser une veille proactive
- Auditer et réaliser des contrôles de conformité et mesurer l'efficacité

3 - Les obligations légales et les exigences SSI

- Responsabilités civile délictuelle et contractuelle
- Les obligations légales
- PPST : Protection des informations relatives au potentiel technique de la nation
- Les respect de la vie privée / Secret des correspondances
- GDPR : General Data Protection Regulation
- Loi pour une république numérique
- SOX : Sarbanes Oaxley - Les lois LSF, LCEN et LSQ
- CPI : Code de la Propriété Intellectuelle
- La directive "Network and Information Security"
- LMP : Loi de Programmation Militaire

4 - Identification des autorités compétentes et référentiels

- ANSSI, PSSI x, RGS, Agence Française de la santé numérique, PCI DSS, CNIL

5 - Les contrats

6 - La gouvernance de la SSI

- Niveaux de maturité SSI et types d'organisation
- Le comité de pilotage, arbitrage, suivi et homologation
- Voie hiérarchique et voie fonctionnelle
- Les articulations avec les autres filières
- La notification d'incidents, la gestion d'alerte

7 - Formalisation d'une stratégie SSI

- Adjonction d'outils et bonnes pratiques
- Orientée enjeux ou orientée SMSI
- Les étapes de la formalisation d'une feuille de route

8 - La gestion des risques

- La norme ISO 31000 - La norme ISO 27005
- Études de cas
- La norme ISO 27002 - La norme ISO 27001

9 - La définition d'un référentiel SSI

- Lettre d'engagement de la direction
- Lettre de nomination du RSSI
- La politique générale de protection de l'information
- Comment construire la politique sécurité système d'information ?
- Chartes - Guides et procédures

10 - Mise en œuvre d'une méthode d'intégration SSI dans les projets

- EBIOS - Adaptée

2ème partie : de la théorie à la pratique (3j)

1 - L'état de l'art des solutions technique de sécurité du SI

- La sécurité des accès, des échanges et des serveurs
- La sécurité des postes de travail sédentaires et mobiles
- La sécurité des applications

2 - Les architectures SSI

- Périphériques - En profondeur

3 - Introduction aux plans de continuité des activités et plans de secours

- Fondamentaux de la continuité des activités
- Le modèle du BCI et de la norme ISO 22301
- Les différents plans : PCA, PCO, PSI, PGC, PCOM...
- Les phases d'un projet de PCA

4 - La prise en compte du facteur humain

- Sensibilisation
- Formation - Communication

5 - La veille juridique et technique SSI

6 - Contrôle et audit

- Définition des indicateurs de contrôle
- Les tests intrusifs
- Formalisation et mise à jour des tableaux de bord

7 - Conseils généraux pour réussir dans son métier de RSSI

- Les freins et les difficultés rencontrés par les RSSI (retour d'expérience)
- La bonne appropriation et la bonne communication du rôle du RSSI
- Les erreurs à ne pas commettre, les conseils d'accompagnement au changement

3 Après le présentiel

Retrouvez sur le Learning Hub ib :

- Un quiz pédagogique pour évaluer vos acquis et approfondir les sujets de votre choix
- Des vidéocasts pour revenir sur les points clés de la formation

Réf. MG802
7 jours (4+3)
(49h présentiel)

4 690 €HT
Offerte

À DISTANCE	PARIS	Autres sites, nous consulter
07/06 & 20/06, 26/09 & 10/10, 21/11 & 05/12	07/06 & 20/06, 26/09 & 10/10, 21/11 & 05/12	

Cursus Expert en cybersécurité

Cursus Métier

CURSUS MÉTIER

ACCESSIBLE À DISTANCE

Il ne se passe pas une semaine sans que les médias n'évoquent des actes de piratage touchant de grandes entreprises, des acteurs de la nouvelle économie ou ... des états. Vol d'informations stratégiques, de fichiers clients, détournements de fonds bancaires, neutralisation de serveurs web... Et bien sûr, il est facile de comprendre qu'au-delà du préjudice financier, il y a toujours un important préjudice d'image. Il n'est donc pas surprenant que de nombreuses entreprises cherchent à se prémunir de ce type de risques. Pour autant, elles peinent souvent à trouver les profils capables de sécuriser efficacement leur SI et de mettre en échec les tentatives d'intrusion des (hackers). A l'issue de ce cursus de 23 jours, les participants disposeront précisément des connaissances et compétences nécessaires à l'atteinte de ces objectifs.

OBJECTIFS

- Disposer des compétences techniques et métiers nécessaires pour comprendre et contrer les attaques des systèmes et réseaux
- Disposer d'éléments méthodologiques propres à chaque phase d'investigation
- Savoir rédiger des rapports d'audit complets et percutants faisant état de recommandations précises et concrètes pour se prémunir des risques d'intrusion
- Savoir organiser une procédure d'audit de sécurité de type test de pénétration sur son SI
- Comprendre comment mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle
- Être en mesure de rédiger un rapport d'audit professionnel
- Maîtriser l'utilisation d'outils dédiés à la sécurité
- Savoir mener une analyse forensic
- Savoir répondre à un incident de sécurité informatique
- Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Public

- Tout personnel technique souhaitant évoluer vers une mission d'expert technique en sécurité

Pré-requis

Avoir une bonne connaissance de l'informatique et des systèmes Windows est nécessaire

Les + de cette formation

- Chaque participant établit son propre planning de formation. En fonction de la date de début choisie parmi celles proposées ci-dessous, nos Conseillers Formation proposent différentes dates pour chacun des modules du cursus. Pour des raisons d'efficacité pédagogique, il est fortement recommandé de suivre les modules dans l'ordre présenté sur ce programme.
- L'alternance de formations et de périodes de mise en pratique en entreprise favorise l'acquisition rapide et durable de nouveaux savoirs.
- Animé par un expert spécialiste du sujet traité, chacun des 5 modules aborde un aspect spécifique de la thématique de formation.
- A travers de nombreuses mises en situation, les participants mettront en pratique les aspects théoriques abordés au cours des différentes étapes du cursus.

Programme

1 - LES FONDAMENTAUX DU HACKING ET DE LA SÉCURITÉ (4j)

- **Objectif :** découvrir les techniques de base du hacking et comprendre comment les mécanismes et outils de sécurité peuvent constituer un premier rempart
- Les fondamentaux de la sécurité des réseaux : prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants, consultation d'informations publiques, localisation un système cible, énumération des services actifs
- Les attaques à distance : intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants, et prise de contrôle des postes utilisateurs par troyen, authentification par brute force, recherche et exploitation de vulnérabilités sur un système cible, prise de contrôle à distance
- Les attaques systèmes : outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion, attaque du Bios, cracking de mot de passe et espionnage du système
- Sécuriser le système : les outils de base permettant d'assurer le minimum de sécurité à un S.I., la cryptographie, le chiffrement des données, ...

2 - HACKING ET SÉCURITÉ AVANCÉE (5j)

- **Objectif :** comprendre les techniques de collectes d'information et de mesure de la vulnérabilité d'un système cible et apprendre à mettre en œuvre les contre-mesures appropriées
- TCP/IP : rappels
- Veille technologique : vocabulaire spécifique, utilisation des bases de données de vulnérabilité et exploitation
- Collecte d'informations : recherche d'informations publiques, prise d'information active
- Mesure de la vulnérabilité par scan et prise d'empreinte : énumération des machines, scan de ports, prise d'empreinte du système d'exploitation, prise d'empreinte des services
- Recherche de failles : vulnérabilités réseau, applicative, web et maintien de l'accès à une machine
- Mise en œuvre d'une stratégie d'attaque sur un laboratoire créé spécifiquement pour la formation

3 - MÉTHODOLOGIE D'AUDIT DE TESTS D'INTRUSION - PENTEST (5j)

- **Objectif :** disposer d'une méthodologie complète d'audit de sécurité et de la connaissance des outils associés pour réaliser un rapport exhaustif
- Présentation de la méthodologie
- Les différents types de PenTest
- Les aspects réglementaires : les responsabilités de l'auditeur, les contraintes fréquentes, la législation et les articles de loi, les précautions
- Méthodologies et outils : préparation et déroulement de l'audit, habilitations nécessaires, dénis de service, ingénierie sociale
- Mise en pratique sur Metasploitable : attaque de la machine virtuelle Metasploitable, recherche d'informations, recherche de vulnérabilités, exploitation des vulnérabilités, maintien de l'accès
- Le rapport d'audit : son importance, sa composition, l'importance de se mettre à la place du mandataire
- La préparation du rapport d'audit : mise en forme des informations collectées lors de l'audit, préparation du document et application de la méthodologie vue en début de formation
- L'écriture du rapport : l'analyse globale de la sécurité du système, la description des vulnérabilités trouvées, les recommandations de sécurité, la synthèse générale sur la sécurité du système
- La transmission du rapport : les précautions nécessaires, la méthodologie de transmission de rapport
- Que faire une fois le rapport transmis ?

4 - ANALYSE APRÈS INCIDENT (4j)

- **Objectif :** comprendre comment constituer un dossier juridique suite à l'intrusion d'un tiers dans le SI.
- Les aspects juridiques : les bases légales de la sécurité de l'information, la classification des crimes informatiques, le rôle de l'enquêteur et de l'inforensique, les acteurs technico-juridiques
- La détection de l'incident : repérer les anomalies, passage en revue des outils de détection d'incident, mise en œuvre d'un IDS / IPS
- Mise en pratique au travers de l'analyse d'un système informatique piraté sur un laboratoire dédié à la formation : analyse des anomalies, établissement de l'incident de sécurité, diagnostic technique et neutralisation de la menace, recherche de l'origine de l'attaque, mise en place de contre-mesures

5 - ATELIER DE MISE EN PRATIQUE DE SOLUTIONS DE CONTRE-ATTAQUES (5j)

- **Objectif :** se mettre concrètement à la place d'un hacker pour ainsi être capable de déterminer la meilleure parade à opposer en vue de garantir la sécurité du SI
- Rappels sur les ateliers d'attaques : revue des failles de Metasploitable, revue des attaques sur WebGoat
- Passage en revue des différents types de protection informatiques : protection réseau, protection applicative, protection web
- Mes meilleures pratiques en termes de sécurité : établir un modèle de menace efficace, revue des Best Practices pour les langages de programmation classiques, revue des Best Practices réseau
- Mise en pratique d'une stratégie de protection progressive : Protection progressive de WebGoat, d'un réseau vulnérable, d'un réseau Wifi, d'un téléphone mobile

Réf. **CM063**

23 jours
(161h présentiel)

11 320 €HT

Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
04/07, 05/09, 24/10	03/10	
PARIS	**LYON**	
04/07, 05/09, 24/10	14/11	

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Prise en compte native de la sécurité dans les projets informatiques

ACCESSIBLE À DISTANCE

Identifier, estimer et réduire les risques dans le cadre de projets informatiques

Aujourd'hui, la sécurité des SI nécessite une implication et une adhésion forte de tous et plus particulièrement des directions métiers. Seule l'intégration native de la SSI pourra permettre une sécurité conforme aux obligations légales et adaptées aux besoins et aux risques des directions métiers. L'intégration native de la sécurité dans les projets est devenue obligatoire. Cette formation a pour objectif de donner les éléments méthodologiques et techniques nécessaires pour améliorer la qualité du dialogue entre les maîtrises d'ouvrage, les directions ou comités d'homologations, les RSSI et les maîtrises d'œuvre en charge du projet.

OBJECTIFS

- Appréhender les obligations légales et réglementaires
- Description des normes ISO 27001 à 27005
- Être en mesure de concevoir des architectures de système d'information en adéquation avec les exigences règlementaires et les besoins métiers
- Savoir identifier les risques
- Concevoir et mettre en œuvre les dispositifs de sécurité afin de les réduire
- Les appliquer aux projets, pouvoir constituer un dossier d'homologation / validation du projet

Public

- Chefs de projet informatique, chefs de projet métier, représentants de la maîtrise d'ouvrage, responsables sécurité des systèmes d'information, directeur des systèmes d'information, responsable des risques opérationnels, maîtres d'œuvre.

Pré-requis

Aucun

Les + de cette formation

- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur pressenti accompagne des chefs de projets informatiques depuis plusieurs années dans l'accomplissement de leurs missions.
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.

Programme

1 - L'identification des acteurs SSI dans le projet
- Les directions métiers
- Les maîtrises d'ouvrage ou MOA
- Les maîtres d'œuvre ou MOE
- Le gestionnaire de risques ou le RSSI
- Le DPO
- Les sous-traitants

2 - Les obligations légales par la maîtrise d'ouvrage
- Les exigences liées au GDPR
- Les exigences liées au RGS
- Les exigences liées aux différents codes (santé, sécurité sociale, protection des mineurs, ...)
- Les exigences SOX, Solvency II, Bâle, ...
- Les exigences LPM

3 - L'approche normative aide à la méthodologie de mise en place des SSI
- Le cycle ISO - OSI
- ISO 31000
- ISO 27001
- ISO 27005
- ISO 29134
- ISO 22301

4 - Outils et méthode de la gestion des risques
- MEHARI
- EBIOS
- EIVP CNIL
- Exercice CNIL

5 - La sécurité dans le processus de développement de la gestion de projets
- Cycle en V
- En mode Agile
- Comparaison V - Agile

6 - La formalisation des besoins de sécurité DICP
- Définitions et termes
- Rapport à la norme 27001
- Disponibilité
- Intégrité
- Confidentialité
- Continuité Prise de Risques

7 - Cartographie : analyse - identification - gestion des risques
- Analyse avant l'action
- Identification des menaces
- Gestion des risques

8 - ISO 27002 (PSSI E, PSSI MCAS, PGSSIS)
- Préambule
- Définition
- Positionnement
- Les types de Sécurité ciblées
- Adaptation ISO27002 / Security by Design

9 - La gestion de l'externalisation : Le PAS
- Préambule
- Définition
- Objectif
- Contenu
- Un nouveau cycle

10 - Mise en pratique de SSI dans le projet
- Intégration dans le projet
- La sécurité des accès et des échanges

Réf. **MG773**
2 jours
(14h présentiel)

**ORGANISÉ SUR DEMANDE,
NOUS CONSULTER**

Télétravail - Technologies et sécurité

Les clés pour une mise en œuvre réussie

SÉMINAIRE

ACCESSIBLE À DISTANCE

Que ce soit pour des raisons sanitaires, pour rationaliser l'utilisation des locaux ou plus simplement pour répondre aux attentes des salariés, le télétravail est progressivement devenu une véritable alternative au fonctionnement classique des entreprises. Mais avant de franchir le pas, il convient de s'assurer que toutes les conditions techniques sont réunies pour fournir un service de qualité aux utilisateurs mais aussi pour garantir le bon fonctionnement des applications et outils, et ce, de façon sécurisée. Cette introduction technique permettra aux participants de disposer d'une première approche pour la mise en œuvre d'une solution technique permettant le télétravail.

OBJECTIFS

- Acquérir une approche de vérification de la pertinence des différentes solutions d'accès distant du marché
- Bâtir une checklist des critères de validation d'une solution
- Construire une liste de questions à poser aux fournisseurs

Public

- Responsable des services informatiques et auditeur technique
- Responsable des achats IT, chargé de missions et chef de projets généralistes
- Toute personne souhaitant mettre en place le télétravail ou vérifier une solution existante

Pré-requis

Connaissance générale de l'informatique

Les + de ce séminaire

- Une technique de vulgarisation qui permet aux professionnels non-spécialistes de comprendre les technologies complexes et la démarche de vérification.
- Le contenu change en continu pour s'adapter à l'évolution des technologies présentées.

Programme

1 - Introduction
- Différentes solutions d'accès distant : client lourd et client léger TS-WEB ; VDI et BYOD
- Composants d'une solution d'accès distant générique
- Métriques de qualité d'usage : 4 A

2 - Vérification des points-clés de la performance
- Capacité d'accès des terminaux
- Caractéristiques des réseaux de communication : 4/5G et WiFi 6
- Applications compatibles et interopérables des logiciels de vidéoconférence (Team, Meet...)
- Montée en charge : nombre de connexion en vidéo...

3 - Contrôle des éléments essentiels de la sécurité
- Sécurité des terminaux par des solutions classiques et spécifiques (EMM)
- Sécurité des réseaux selon les lieux de connexion (VPN, WPA3...)
- Sécurité des accès : authentification forte, 3D, Filtrage (FW, IDS/IPS...)
- Sécurité des applications à distance (Proxy, honeypot...)
- Protection par la conception de l'architecture et les opérations spécifiques
- Protection des vols de données (protection des données...)
- Autres

4 - Perspectives et autres solutions
- Solutions hébergées de sécurité dans le Cloud Sécurité par l'IA et la Machine Learning
- Cybersécurité externalisée et plates-formes publiques SeaaS
- Questions à poser aux fournisseurs

Réf. SEM93
1 jour
(7h présentiel)

975 €HT
101 Offerte

À DISTANCE	02/09, 19/12
PARIS	02/09, 19/12

Autres sites, nous consulter

Auditer et contrôler la sécurité du SI

Assurer le suivi de la sécurité

SÉMINAIRE

ACCESSIBLE À DISTANCE

La mise en œuvre d'une politique de sécurité des systèmes d'information nécessite un pilotage et un suivi à tous les niveaux hiérarchiques de l'organisation tant d'un point de vue technique que d'un point de vue fonctionnel. La capacité de l'organisation à maitriser les risques et à améliorer en continu le niveau de protection de son patrimoine informationnel doit être démontré et contrôlé. Ce séminaire synthétique vise à présenter les démarches et les méthodes permettant de piloter la sécurité des systèmes d'information au travers d'audits et d'indicateurs conformes aux enjeux de l'organisme et aux obligations réglementaires en vigueur.

OBJECTIFS

- Être capable de construire les indicateurs et les tableaux de bord nécessaires à l'audit et au suivi de la sécurité du SI
- Connaître les enjeux et les obligations en matière de pilotage de la sécurité
- Disposer d'une méthodologie d'audit de la sécurité
- Comprendre comment réaliser des tableaux de bord parlants et efficaces
- Pouvoir maîtriser les techniques de contrôle de la sécurité des SI

Public

- RSSI ou correspondants sécurité, risk manager, DPD, DSI, chefs de projet, auditeurs, responsables techniques

Pré-requis

Connaissances de base en sécurité informatique

Les + de ce séminaire

- Un panorama complet des outils et techniques d'audit et du contrôle de la sécurité.
- Le séminaire alterne entre présentation de fondamentaux théoriques et études de cas.
- Les retours d'expériences et conseils d'un consultant expert en sécurité qui étayera son approche de nombreux exemples concrets.

Réf. SR239
2 jours
(14h présentiel)

1 825 €HT
Offerte

À DISTANCE	22/08, 24/10, 15/12
PARIS	22/08, 24/10, 15/12

Autres sites, nous consulter

Programme

1 - Introduction : Rappel sur les enjeux et les obligations en matière de pilotage de la SSI
- Définitions
- Rappel sur les principes d'un système de management de la SSI (ISO 27001)
- Les exigences réglementaires et légales en matière de pilotage de la SSI

2 - Les rôles et les responsabilités en matière de pilotage et de suivi de la SSI
- Rôles et responsabilités des acteurs impliqués dans la SSI (Direction générale, Directions métiers, DSI, RSSI, DPO, RPCA, Auditeur, contrôle interne, ...)
- Les instances de décisions
- La gouvernance à prévoir dans le cadre du pilotage et du suivi de la SSI

3 - Audit de la sécurité des SI
- Les catégories d'audit (audit de configuration, tests intrusifs, audit de code, ...)
- Les recommandations de l'ANSSI (Guide PASSI)
- La démarche à adopter par l'auditeur (préparation de la mission, réalisation de la mission, restitution de la mission, métriques, ...)
- L'audit dans le cadre de la sous-traitance
- La certification des auditeurs
- La prise en compte des résultats de l'audit par l'organisme (arbitrage, amélioration des dispositifs opérationnels, ...)
- Les indicateurs de suivi des audits

4 - Tableaux de bord de la sécurité des SI
- Les démarches proposées (normes ISO 27004, démarche proposée par l'ANSSI, démarche proposée par le CIGREF, ...)
- Les catégories d'indicateurs SSI de niveau stratégique et opérationnel
- La construction et l'alimentation des tableaux de bord SSI
- Le traitement des écarts (identification des non-conformités, définition des mesures correctives, ...)

5 - Contrôles de la sécurité des SI
- Les contrôles permanents de la SSI (détections d'intrusion, gestion des logs, journalisation, ...)
- Les contrôles périodiques de la SSI (enquêtes, gestion des traces, ...)
- Les revues de direction (démarche, objectifs, ...)

6 - La prise en compte des audits, tableaux et contrôles de la SSI dans les démarches projets
- La démarche GISSIP proposée par l'ANSSI
- Les nouvelles règles Européennes imposées par le règlement Européen (Privacy By Design)

7 - Étude de cas
- Mise en œuvre de tableaux de bord SSI

Les implantations

En mettant à votre disposition des équipes commerciales dans chacune de nos agences, nous vous apportons la garantie d'une vraie relation de proximité. Quel que soit votre besoin, vous bénéficiez de l'accompagnement d'experts géographiquement et culturellement proches de vous :

PARIS
AIX-EN-PROVENCE
BORDEAUX
LILLE
LYON
NANTES
RENNES
ROUEN
SOPHIA-ANTIPOLIS
STRASBOURG
TOULOUSE

Maîtriser l'analyse des risques du SI

Mettre en œuvre une politique d'analyse de risques

ACCESSIBLE À DISTANCE

L'évolution de la réglementation et de la gouvernance des entreprises met aujourd'hui en avant la notion de maîtrise des risques. L'exigence ambitieuse qui nous est donnée est désormais à la fois d'assurer la robustesse de l'entreprise face à l'imprévu, mais aussi d'optimiser l'efficacité économique de son dispositif de maîtrise des risques. Cette formation approfondit les outils de la gestion des risques liés aux informations, et donne au RSSI ou au risk-manager les clés pour connaître ces risques, élaborer un plan d'action orienté vers les métiers de l'entreprise et piloter sa mise en œuvre.

OBJECTIFS

- Appréhender les concepts fondamentaux de l'analyse de risques SSI
- Savoir identifier les enjeux
- Disposer d'une démarche complète pour mener à bien un projet d'analyse de risques
- Découvrir les méthodes d'analyse et les solutions logicielles disponibles pour maîtriser les risques du SI

Public

- Directeur des systèmes d'information, responsable des risques opérationnels, risk-manager, auditeur ou professionnel du contrôle interne, chef de projets

Pré-requis

Aucun

Les + de cette formation

- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur, expert en analyse des risques, accompagne des responsables de la sécurité des SI depuis plusieurs années dans l'accomplissement de leurs missions.
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des systèmes d'information. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.
- Des documents annexes illustrent les cas concrets abordés durant la formation.

Programme

1 - Les concepts généraux de la gestion des risques
- Définition du risque et des typologies de menaces
- Modèle général de gestion des risques

2 - Les acteurs impliqués dans l a cartographie des risques
- La gouvernance à prévoir, les acteurs, leurs rôles et responsabilités
- La voie hiérarchique et les voies fonctionnelles
- Identification des risques juridiques : métier, civil, pénal, réglementaire, contractuel
- Identification des risques accidentels
- Identification des risques d'erreurs
- Identification des risques liés à la malveillance (cybercriminelle, concurrentielle, ludique, idéologique et stratégique) : les caractéristiques de compétence, temps, moyen, connaissance au préalable sur la cible, ...

3 - Présentation de la norme ISO 31000
- Objectifs de la norme

4 - Présentation de la norme ISO 27005
- Objectifs de la norme
- Présentation du contenu de la norme
- Démarche générale de l'analyse des risques
- Démarche d'appréciation et d'analyse des risques
- Classification
- Les pièges à éviter
- Présentation des référentiels d'analyse des menaces, des enjeux et des contraintes : la granularité et les domaines d'analyse
- Présentation des référentiels de vulnérabilité proposés par la norme
- Présentation des métriques d'appréciation des risques : les approches possibles
- La stratégie de traitement des risques, les objectifs et l'acceptation des risques selon la norme
- Les processus de communication et de surveillance des risques
- Les validations EIVP
- Les homologations RGS, PSSIx

5 - La norme ISO 29134
- Objectifs de la norme
- Présentation du contenu de la norme
- Démarche générale de l'analyse des risques
- Démarche d'appréciation et d'analyse des risques
- Les validations AIPD

6 - Les homologations RGS, PSSIX
- Objectifs
- Présentation du RGS
- Démarche d'homologation...

7 - Études de cas

8 - La prise en compte native des risques SSI dans les projets
- L'approche en V
- L'approche Agile
- EBIOS
- EBIOS RM
- MEHARI
- Adaptée
- La déclinaison Privacy by design du RGPD

9 - Études de cas

10 - La définition et la mise en œuvre du plan de prévention des risques (PPR)
- Notions principales et objectifs du PPR
- Le processus d'élaboration du PPR
- La définition des objectifs et des priorités de mise en œuvre
- Introduction à la norme ISO 27002
- Le cas du Cloud ISO 27018
- Les relations avec les PCA et la norme 22301
- Les relations avec la gestion de crise

11 - Les conseils de mise en œuvre d'une gestion structurée des risques
- La gouvernance
- La mise en œuvre du système de management de gestion des risques
- Le maintien en condition opérationnelle

12 - La prise en compte du facteur humain dans la gestion du risque SI
- Direction générale
- Encadrement
- Acteurs DSI
- Représentant de la MOA
- Les utilisateurs
- Les solutions
- Études de cas

13 - Les principes généraux relatifs aux systèmes de management de la sécurité
- Le système de management ISO 31000
- Présentation générale du modèle PDCA ISO 27001

Réf. MG803
2 jours
(14h présentiel)

1 560 €HT
Offerte

À DISTANCE
13/10
PARIS
13/10

Autres sites, nous consulter

Élaborer un plan de continuité et de reprise après sinistre

De l'évaluation des risques au système de management de la continuité – ISO 22301

SÉMINAIRE

ACCESSIBLE À DISTANCE

La continuité des activités est plus que jamais au cœur de la préoccupation des entreprises et des instances de réglementation. Bien au-delà de la dimension informatique à laquelle il est trop souvent confiné, un Plan de continuité des activités (PCA) est avant tout centré sur les métiers, et vise à assurer la robustesse de l'entreprise face à tout type de risque opérationnel. Ce séminaire donne les clés pour prendre en compte toutes les dimensions de la continuité des activités, puis concevoir et mettre en œuvre son PCA.

OBJECTIFS

- Évaluer les risques et enjeux de la reprise après sinistre et de la continuité de service
- Élaborer les plans répondant aux besoins de l'entreprise dans ce domaine
- Connaître les méthodes et outils pour choisir le type de site de reprise et réussir les projets
- Sélectionner les technologies, architectures et solutions les plus pertinentes
- Connaître les meilleures pratiques et bâtir un budget réaliste

Public

- DSI, RSSI, responsable en charge du plan de continuité, architecte en charge du choix des solutions de reprise

Pré-requis

Aucun

Les + de ce séminaire

- Les clés pour concevoir et mettre en œuvre un PCA efficace.
- Les échanges entre participants et l'expérience du formateur/consultant facilitent les retours d'expérience.
- Le séminaire alterne entre présentation de fondamentaux théoriques et études de cas. Tous les outils et démarches proposés ont été utilisés dans des cas réels d'entreprises.

Réf. SEM19
3 jours
(21h présentiel)

2 490 €HT
Offerte

À DISTANCE	26/09
PARIS	26/09

Autres sites, nous consulter

Programme

1 - Introduction à la gestion de crise et à la continuité d'activité
- Contexte
- Fondamentaux
- Objectifs et enjeux
- Définitions
- Principales réglementations

2 - Réaliser l'analyse des risques et des besoins
- Risques bruts et risques nets (VIT)
- Analyse des risques par sites
- Analyse du référentiel des risques (si existe)
- Détermination du référentiel des activités ou processus
- Analyse par DMIA (Durée Maximale admissible d'Interruption de l'Activité) par activité ou processus
- Les BIA (Bilans d'Impacts sur Activités/Affaires) : présentation de l'activité, analyse des impacts sur le risque financier, analyse des impacts sur le risque légal et réglementaire, analyse des impacts sur le risque d'image et de réputation, analyse des impacts sur le risque opérationnel, analyse des impacts sur le risque de sous-traitance, analyse des besoins RH, analyse des besoins informatiques et analyse des besoins logistiques

3 - Mettre en place un dispositif de gestion de crise (GC)
- Les grands principes de la gestion de crise
- Définir une organisation autour de cellules de crises
- Réaliser la documentation : le Plan de Gestion de Crise (PGC), le Plan de Communication de Crise (PCC), le Plan de Gestion des RH (PGRH), le mémo de poche, le Manuel de Crise
- Exemples de PGC spécifiques : cybercrise, pandémie - épidémie, incendie, intrusion - sécurité, aléa climatique
- Communiquer, informer, sensibiliser et former
- Mettre en place les moyens adaptés
- Gérer les incidents et escalader l'alerte
- Mobiliser la cellule de crise décisionnelle
- Mobiliser les autres cellules de crise
- Gérer les premiers moments de la crise
- Gérer la crise dans le temps
- Effectuer le bilan de la crise
- Documenter le suivi de la crise
- Mettre en place un plan de progrès

4 - Mettre en place un plan de continuité d'activité (CA)
- Le rôle Les grands principes de la continuité d'activité
- Se mettre en mode projet
- Définir l'organisation de la filière de CA
- Réaliser la documentation : les Plans de Continuité Métiers ou Plan de Continuité Opérationnels (PCM ou PCO), le Plan de Continuité des Systèmes d'Information (PCSI), le Plan de Continuité Logistique et Sécurité (PCLS), le Plan de Reconstruction (PREC)
- Déployer le PCA : scénario 1 : perte durable d'accessibilité à un immeuble, scénario 2 : indisponibilité durable du système d'information, scénario 3 : absence importante durable de personnel, scénario 4 : défaillance importante et durable d'un prestataire essentiel
- Communiquer, sensibiliser et former
- Mettre en place les moyens adaptés

5 - S'assurer de l'efficacité du PGC et du PCA
- Le Plan d'Amélioration Continue (PAC) ou Plan de Maintien en Condition Opérationnelle (PMCO)
- Les tests et exercices
- L'audit

6 - LE SMCA (Système de Management de la Continuité d'Activité - Norme ISO22301)
- Les grands principes du SMCA
- Mettre en place le SMCA
- Se faire certifier ISO22301

7 - Mise en situation
- Le plan de formation des acteurs du PCA
- La formation des cellules de crise
- La formation des RPCO et des utilisateurs

8 - Quizz
- Les documents à prévoir (Protocole de tests, fiche de suivi, ...)
- L'organisation et la préparation des tests

9 - Conclusion

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Élaborer un plan de secours informatique

Réalisation de l'étude technique et fonctionnelle

SÉMINAIRE

ACCESSIBLE À DISTANCE

Le plan de secours informatique (PSI) qui est en réalité le volet informatique d'un plan de continuité ou de reprise d'activité (PCA/PRA) prévoit le scenario du pire, telle que la destruction d'un Datacenter par exemple. Les équipes en charge de l'élaboration d'un PSI doivent réfléchir à la mise en œuvre des moyens techniques, organisationnels et humains qui permettront à l'entreprise de poursuivre son activité dans les meilleures conditions possibles en cas de sinistre. Ce séminaire de 2 jours qui passe en revue tous les aspects d'un plan de secours informatique, fournit aux participants des clés et des méthodes qui leur permettront, de retour dans leur entreprise, d'élaborer ou d'améliorer leur PSI.

OBJECTIFS

- **Comprendre comment concevoir et suivre une démarche appropriée de conception d'un plan de secours informatique dans le cadre de la mise en œuvre d'un Plan de Continuité d'Activités**
- **Acquérir une démarche méthodologique simple et efficace**
- **Savoir réaliser l'étude technique et fonctionnelle qui mènera à la mise en œuvre du PSI**

Public

- Directeur du système d'information
- Responsable sécurité des systèmes d'information
- Responsable PCA
- Responsable des risques
- Responsable de l'organisation

Pré-requis

Aucun

Les + de ce séminaire

- Une approche méthodologique participative permettant des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des responsables de la continuité d'activité depuis plusieurs années dans l'accomplissement de leurs missions.
- Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques. Le support est adapté au contexte actuel et aux obligations réglementaires en vigueur.
- Des documents annexes illustrent les cas concrets abordés durant le séminaire.

Réf. SEM20
2 jours
(14h présentiel)

1 930 €HT
Offerte

À DISTANCE	07/07, 07/11
PARIS	07/07, 07/11

Autres sites, nous consulter

Programme

1 - Introduction
- Objectifs de la formation
- La place du plan de secours informatique dans le cadre du Plan de continuité d'activités

2 - L'organisation
- Le comité de crise
- La cellule de coordination
- Les équipes d'intervention
- Les services utilisateurs

3 - Les documentations
- De communication
- De mise en œuvre
- De gestion
- De contrôle

4 - Les solutions de secours informatiques
- Typologies et moyens de secours
- Types de mise en œuvre
- Préparation

5 - Les solutions de secours de la téléphonie
- Le raccordement au réseau
- Les moyens téléphoniques de secours
- Le routage

6 - Le sauvetage des locaux et des équipements

7 - Les sauvegardes et restaurations
- Les types de sauvegarde (physiques, logiques, complètes, incrémentales, applicatives, journalisations)
- Les techniques de duplication, de sauvegarde et de restauration
- Les architectures

8 - Le secours des impressions

9 - Le secours des accès au réseau Internet
- Le raccordement
- Le reroutage

10 - Le contrat de secours
- Objet
- Nature détaillée des prestations
- Procédure de déclenchement
- Conditions de fonctionnement
- Logistique
- Tests et répétitions
- Gestions de priorités
- Engagements et responsabilités
- Aspects financiers
- Évolutions

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Gérer une cyber-crise

Quand une attaque cyber devient virale, voire vitale, pour un organisme

ACCESSIBLE À DISTANCE

"Il y a deux types d'entreprises, celles qui ont été piratées et celles qui ne le savent pas encore". Une étude récente montre que les 2 principaux risques aux yeux des organisations sont la perte de production/business et la cybercriminalité : 92% d'entre elles ont déjà subi une ou plusieurs cyberattaques. Et au-delà de leur fréquence croissante, les cyberattaques deviennent en plus difficiles à détecter et potentiellement beaucoup plus dangereuses, jusqu'à générer des crises profondes pour les organismes les subissant puisqu'elles peuvent entrainer des indisponibilités de sites internet, des retards de livraison, des arrêts de production, des pertes de CA et bien souvent des dommages collatéraux très impactant dès lors que l'entreprise victime fournit des services sensibles. Être prêt à gérer une cyber-crise devient donc un impératif pour les organisations, et ce quelle que soit leur nature. Mais comment procéder ? Quelles actions entreprendre dès à présent ? Quelles actions prévoir ? Quelle organisation mettre en place ? Autant de questions auxquelles nous répondrons pendant cette formation.

OBJECTIFS

- Comprendre ce qu'est une gestion de crise notamment dans le cas d'une des cyber-attaques
- Être capable de prendre de la hauteur et se positionner comme gestionnaire d'une crise en plus d'être un expert SI
- Acquérir les clés de la gestion d'une cyber crise
- Être prêt à entrer en action

Public

- Responsable du plan de continuité d'activité (RPCA) et de la gestion de crise
- Dirigeants de l'organisme membres ou non de la cellule de crise
- Responsable de la Sécurité du Système d'Information (RSSI)
- Directeur des Systèmes d'Information (DSI)
- Directeur des risques
- Équipes techniques devant mettre en œuvre les solutions de secours

Pré-requis

Aucun

Les + de cette formation

- Les clés pour se préparer et gérer efficacement une cyber-crise.
- Les retours d'expériences de l'intervenant permettent de mieux appréhender les diverses dimensions d'une gestion de cyber-crise.
- La formation propose une approche largement inspirée de cas réels.
- L'étendue du sujet permet de faire le lien entre des systèmes de management de l'organisme (SMCA, SMSI, ...).

Programme

1 - Introduction
- Définitions
- Enjeux
- Périmètre
- Règlementation
- PCA et gestion de crise

2 - Les risques de cyber-crise
- Les cyber-menaces
- Les attaquants
- Les risques
- Vous protéger

3 - Se préparer à gérer une cyber-crise
- Gestion de crise : mieux vaut prévenir que guérir
- Cyber-crises : un des nombreux scénarios de crise ... mais le plus prégnant à ce jour
- Se préparer : s'entraîner et déterminer tous les points à traiter
- S'organiser : se donner les moyens de réagir efficacement
- Documenter : apporter un support pour tous

4 - Gérer une cyber-crise
- Organiser : ne pas laisser faire le hasard
- Mobiliser : se donner les chances d'être opérant
- Gérer : être efficace et résilient
- Communiquer : être transparent et respecter les règles
- Documenter : formaliser pour se rappeler et pour les audits

5 - Mise en situation
- Choix du sujet, mise en situation et debriefing commun

6 - Quiz

7 - Conclusion

Réf. MG858
2 jours
(14h présentiel)

1 935 €HT
Offerte

À DISTANCE
07/07, 17/11
PARIS
07/07, 17/11

Autres sites, nous consulter

L'aide au recrutement avec la POE (Préparation Opérationnelle à l'Emploi)

Vous rencontrez des difficultés pour recruter des collaborateurs dont les profils et les compétences sont en adéquation avec vos besoins ?

ib vous propose un dispositif complet qui répond précisément à cette problématique. En associant pré-recrutement et formation préalable à l'embauche, ib vous propose une solution clé en main qui vous permettra d'intégrer des collaborateurs immédiatement opérationnels sur des métiers en tension.

A travers notre dispositif qui associe aux avantages liés à la POEI des services à forte valeur ajoutée, nous apportons une réponse efficace aux problèmes de pénuries de compétences et d'employabilité auxquels sont aujourd'hui confrontées les entreprises.

Pour en savoir plus, contactez-nous au 0 825 07 6000

ISO 22301 - Lead Auditor

Devenir auditeur ISO 22301

CERTIFIANT

ACCESSIBLE À DISTANCE

La norme ISO 22301 spécifie les exigences liées à la mise en œuvre d'un Système de Management de la Continuité d'Activité (SMCA) visant à protéger l'entreprise des incidents perturbateurs, à réduire leur probabilité et le cas échéant à y répondre et à s'en rétablir quand ils surviennent. Ce programme s'adresse à toute personne souhaitant être en mesure d'auditer un SMCA, que ce soit dans le cadre de démarches internes ou dans celui d'un audit de certification ISO 22301. Les participants à cette formation certifiante acquerront les compétences nécessaires à la conduite d'un audit ainsi qu'à la gestion d'une équipe d'auditeurs.

OBJECTIFS

- Comprendre le fonctionnement d'un SMCA selon la norme ISO 22301
- Découvrir le déroulement, les spécificités et les exigences d'un audit ISO 22301
- Acquérir les compétences nécessaires pour réaliser un audit interne ou un audit de certification ISO22301, en fonction de la norme ISO 19011
- Savoir gérer une équipe d'auditeurs de SMCA
- Devenir auditeur ISO 22301 certifié

Public

- Stagiaires amenés à conduire des audits de SMCA
- Responsables chargés de la Continuité d'Activité (RPCA)
- Consultants
- Auditeurs
- Chefs de projet
- Qualiticiens
- Équipes du contrôle interne

Pré-requis

Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans

Certification

Cette formation prépare à l'examen du PECB qui permet d'obtenir la certification ISO 22301 Lead Auditor.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cours magistraux basés sur les normes ISO 19011, ISO 22301, ISO 22313, ISO 27031, ISO 31000.
- Exercices pratiques, individuels et collectifs basés sur une étude de cas.
- Exercices individuels de révision.
- Formation nécessitant 1 heure de travail à la maison et ce quotidiennement.
- Support de cours en français au format papier et annexes associées en anglais et/ou français.

Programme

1 - Introduction
- Présentation générale du cours
- Introduction aux systèmes de management
- Principes fondamentaux de la continuité d'activité

2 - Présentation détaillée de la norme ISO 22301
- Notions de Système de Management de la Continuité d'Activité (SMCA)
- Modèle PDCA (Plan – Do – Check - Act)
- Les exigences
- Les enregistrements

3 - Panorama des normes ISO complémentaires : ISO 190011, ISO 22313, ISO 27031, ISO 31000

4 - Présentation de la continuité d'activité
- Stratégie de continuité
- Plan de continuité et procédures
- Exercices et tests
- Retours d'expérience sur l'audit de Plans de Continuité d'Activité (PCA)

5 - Processus de certification ISO 23201

6 - Présentation de la démarche d'audit ISO 19011
- Normes ISO 19011
- Principe de l'audit
- Types d'audit
- Programme d'audit
- Démarche d'audit
- Auditeur
- Responsable d'équipe d'audit

7 - Présentation de la démarche d'un SMCA basé sur l'ISO 19011
- Normes ISO 19011
- Audit d'un SMCA
- Règlement de certification
- Exemple de pratiques

8 - Exercices de préparation à l'examen

9 - Passage de l'examen "PECB ISO 22301 Lead Auditor" (en ligne après la formation)
- Révision des concepts en vue de la certification
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-pr%C3%A9paration-a-l%E2%80%99examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70% est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec ils bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du Système de management de la continuité d'activité
  - Domaine 2 : Système de management de la continuité d'activité (SMCA)
  - Domaine 3 : Principes et concepts fondamentaux de l'audit
  - Domaine 4 : Préparation d'un audit ISO 22301
  - Domaine 5 : Réalisation d'un audit ISO 22301
  - Domaine 6 : Clôturer un audit ISO 22301
  - Domaine 7 : Gérer un programme d'audit ISO 22301

Réf. MG812
5 jours
(35h présentiel)

3 730 €HT
Offerte

À DISTANCE
05/12
PARIS
05/12

Autres sites, nous consulter

Les programmes certifiants

CERTIFIANT

Les programmes certifiants ib sont destinés aux personnes souhaitant acquérir de nouveaux savoirs et les valoriser par l'obtention d'une certification reconnue sur le marché de l'informatique.

Des cursus de plusieurs semaines permettant d'évoluer vers un nouveau métier aux formations courtes visant à acquérir une expertise sur un domaine précis, notre offre de formations certifiantes est à la fois complète et variée

Le passage des examens de certification, généralement proposés en fin de session, est systématiquement inclus dans le prix de nos formations certifiantes.

ISO 22301 - Lead Implementer

Mettre en œuvre et gérer un Système de Management de la Continuité d'Activité

CERTIFIANT

ACCESSIBLE À DISTANCE

La norme ISO 22301 spécifie les exigences liées à la mise en œuvre d'un Système de Management de la Continuité d'Activité (SMCA) visant à protéger l'entreprise des incidents perturbateurs, à réduire leur probabilité et le cas échéant à y répondre et à s'en rétablir quand ils surviennent. Ce programme intensif s'adresse à toute personne souhaitant acquérir les connaissances et compétences nécessaires à la mise en œuvre ou à l'accompagnement à la mise en œuvre d'un Système de Management de la Continuité d'Activité dans le respect des exigences de la norme ISO 22301. Les participants réussissant l'examen proposé après la formation obtiendront la certification ISO 22031 Lead Implementer.

OBJECTIFS

- Comprendre la mise en œuvre d'un SMCA suivant l'ISO 22301
- Se familiariser avec les concepts, les approches, les méthodes et les techniques requises pour gérer un SMCA
- Acquérir les compétences nécessaires pour accompagner et conseiller une organisation dans l'implémentation et la gestion d'un SMCA conformément à l'ISO 22301
- Devenir un implémenteur certifié ISO 22301

Public

- Stagiaires devant mettre en œuvre un SMCA
- Managers
- Responsables de direction opérationnelle
- Responsables chargés de la Continuité d'Activité (RPCA)
- Gestionnaire de risque
- Chefs de projets
- Consultants

Pré-requis

Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans

Connaître les principes fondamentaux de la continuité d'activité

Certification

Cette formation prépare à l'examen du PECB qui permet d'obtenir la certification ISO 22301 Lead Implementer.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cours magistraux basés sur les normes ISO 22301, ISO 22313, ISO 27031, ISO 31000, ISO 22317, ISO 27005...
- Exercices pratiques, individuels et collectifs basés sur une étude de cas.
- Quizz préparatoire à l'examen.
- Formation nécessitant 1 heure de travail à la maison et ce quotidiennement.
- Support de cours en français au format papier et annexes associées en anglais et/ou français.

Programme

1 - Introduction
- Introduction des systèmes de management
- Principes fondamentaux de la continuité d'activité

2 - Présentation détaillée de la norme ISO 22301
- Notions de Système de Management de la Continuité d'activité (SMCA)
- Modèle PDCA (Plan – Do – Check - Act)
- Les processus du SMCA

3 - Panorama des normes ISO complémentaires : ISO 22313, ISO 27031, ISO 31000

4 - Présentation des processus de continuité d'activité
- Analyse des impacts sur l'activité ou Business Impact Analysis (BIA)
- Appréciation du risque pour un SMCA sur la base de l'ISO 31000
- Procédures de continuité d'activité
- Exercices et tests
- Retours d'expérience sur l'implémentation de Plans de Continuité d'Activité (PCA)

5 - Mener un projet d'implémentation d'un SMCA
- Convaincre la Direction
- Les étapes du projet
- Les acteurs
- Les facteurs clés de succès
- Les risques et opportunités

6 - Intégration de l'ISO 27031 dans le SMCA

7 - Processus de certification ISO 22301

8 - Gestion des indicateurs

9 - Préparation de l'examen

10 - Passage de l'examen PECB ISO 22301 Lead Implementer (en ligne après la formation)
- Révision des concepts en vue de la certification
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-preparation-a-l-examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70% est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires
- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du Système de management de la continuité d'activité
  - Domaine 2 : Système de management de la continuité d'activité
  - Domaine 3 : Planification de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
  - Domaine 4 : Mise en œuvre d'un SMCA conforme à la norme ISO 22301
  - Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMCA conforme à la norme ISO 22301
  - Domaine 6 : Amélioration continue d'un SMCA conforme à la norme ISO 22301
  - Domaine 7 : Préparation de l'audit de certification d'un SMCA

Réf. MG813
5 jours
(35h présentiel)

3 730 €HT

Offerte

À DISTANCE
21/11

PARIS
21/11

Autres sites, nous consulter

Evaluations des pré-requis

Testez vos pré-requis en ligne

Parce qu'il est important de ne pas se tromper dans le choix d'une formation, nous avons développé des tests d'évaluation des pré-requis permettant aux stagiaires de s'assurer qu'ils disposent des connaissances nécessaires pour suivre les formations dans de bonnes conditions.

Généralement constitués d'une dizaine de questions à choix multiples, ces évaluations sont disponibles sur les fiches formation présentées sur notre site web (rubrique pré-requis).

ISO 27001 - Lead Auditor

Préparer un audit de sécurité du système d'information

CERTIFIANT

ACCESSIBLE À DISTANCE

L'établissement de normes vise généralement à garantir la sécurité, la fiabilité et la qualité des produits et services proposés par les entreprises. Perçues parfois comme des contraintes, elles constituent aussi souvent pour ces dernières des outils stratégiques permettant d'abaisser les coûts, en augmentant la productivité et en réduisant les risques, les déchets et les erreurs. La norme ISO27001 décrit par exemple les exigences liées à la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Cette formation permet d'acquérir l'expertise nécessaire à la réalisation d'audits internes et externes de Système de Management de la Sécurité de l'Information (SMSI) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues et ce, conformément à la norme ISO 19011 et au processus de certification d'ISO/CEI 17021-1. Lors de la dernière journée de formation, ils passeront un examen leur permettant d'obtenir le titre de "PECB Certified ISO/CEI 27001 Lead Auditor".

OBJECTIFS

- Connaître le fonctionnement d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO /CEI 27001
- Connaître la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Être en mesure de planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir rédiger des rapports d'audit et assurer le suivi d'un audit en conformité avec la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI

Public

- Chefs de projet
- Consultants
- Architectes techniques
- Toute personne souhaitant conduire des audits de conformité ISO 27001
- Toute personne responsable du maintien de la conformité aux exigences du SMSI

Pré-requis

Connaitre le guide d'hygiène sécurité de l'ANSSI (Document téléchargeable l'adresse https://www.ib-formation.fr/guide_hygiene_informatique_anssi.pdf)

Certification

Cette formation prépare à l'examen du PECB qui permet d'obtenir la certification ISO 27001 Lead Auditor.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.
- Répartition théorie/pratique : 70%/30%.
- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Programme

1 - Introduction au Système de Management de la Sécurité de l'Information et à la norme ISO/CEI 27001

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires : organisation et principes de base de l'ISO, système de management intégré, normes en sécurité de l'information, avantages de l'ISO27001
- Processus de certification : schéma de certification, autorité d'accréditation, organisme de certification
- Principes fondamentaux du Système de Management de la Sécurité de l'Information
- Définition et mise en œuvre d'un SMSI

2 - Principes, préparation et déclenchement de l'audit

- Principes et concepts fondamentaux d'audit : normes d'audit, types d'audits, acteurs, objectifs et critères de l'audit, audit combinée
- Approche d'audit fondée sur les preuves
- Approche d'audit fondée sur le risque
- Déclenchement de l'audit : revue de la demande, nomination d'un responsable, validation des objectifs, du périmètre et des critères d'audit
- Étape 1 de l'audit : objectif, visite des lieux, entretiens, revue de la documentation, rapport d'audit
- Préparation de l'étape 2 de l'audit (audit sur site) : préparation du plan d'audit, assignation des auditeurs, recours aux experts techniques, préparation des documents de travail, utilisation d'une liste de contrôle, mise en place d'une norme de documentation
- Étape 2 de l'audit (première partie) : conduire la réunion d'ouverture, collecter des informations, conduire les tests d'audits avec les procédures appropriées, rédiger des constats d'audits et des rapports de non-conformité

3 - Activités d'audit sur site

- Étape 2 de l'audit (deuxième partie) : rédiger des constats d'audit et de non-conformité, exécuter la revue qualité des constats d'audit
- Communication pendant l'audit : comportement pendant les visites sur site, communication durant l'audit, réunions de l'équipe d'audit, rôles des guides et observateurs, gestion des conflits, aspects culturels de l'audit, communication avec la direction
- Rédaction des plans de tests d'audit
- Rédaction des constats d'audit et des rapports de non-conformité

4 - Clôture de l'audit

- Documentation de l'audit et revue de qualité de l'audit : documents de travail, enregistrements d'audits, revue de qualité, documentation de la revue de qualité
- Clôture de l'audit : préparation des conclusions, discussion des conclusions avec l'audité, réunion de clôture, rapport d'audit, audit de suivi, décision de certification, contenu d'un certificat
- Évaluation des plans d'actions par l'auditeur : dépôt des plans d'actions par l'audité, contenu des plans d'action, évaluation des plans d'action
- Suite de l'audit initial : activité de surveillance, audit de surveillance, audit de renouvellement, utilisation des marques déposées ISO
- Management d'un programme d'audit interne : particularités de l'audit interne, indépendance et impartialité, le rôle de la fonction de l'audit interne, ressources et outils de l'audit interne, surveillance du programme
- Compétence et évaluation des auditeurs : qualification, compétences des responsables d'équipes d'audit, schéma de certification, certification, maintien de la certification

5 - Passage de l'examen "PECB ISO 27001 Lead Auditoré (en ligne après la formation)

- Révision des concepts en vue de la certification et examen blanc
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-préparation-a-l'examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70 % est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- Les candidats sont autorisés à utiliser les supports de cours et les normes ISO/IEC 27001 et ISO/IEC 27002 qui leurs seront remises
- En cas d'échec ils bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du SMSI
  - Domaine 2 : Le SMSI
  - Domaine 3 : Principes et concepts fondamentaux de l'audit
  - Domaine 4 : Préparation d'un audit ISO/CEI 27001
  - Domaine 5 : Réalisation d'un audit ISO/CEI 27001
  - Domaine 6 : Clôturer un audit ISO/CEI 27001
  - Domaine 7 : Gérer un programme d'audit ISO/CEI 27001

Réf. MG207
5 jours
(35h présentiel)

3 730 €HT
Offerte

À DISTANCE
04/07, 26/09, 21/11

PARIS
04/07, 26/09, 21/11

Autres sites, nous consulter

ISO 27001 - Lead Implementer

Mettre en œuvre un SMSI

CERTIFIANT

ACCESSIBLE À DISTANCE

Quel que soit le secteur d'activité de l'entreprise, assurer la sécurité du système d'information est une préoccupation importante de toute DSI. Internationalement reconnue, la norme 27001, a pour objectif de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion. Le référentiel dicte également les exigences en matière de mesures de sécurité qui peuvent varier en fonction des secteurs d'activité (banque versus industrie par exemple). Le rôle du Lead Implementer est précisément de définir un Système de Management de la Sécurité de l'Information (SMSI) propre à une organisation. Cette formation permet 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 SMSI conforme à la norme ISO/CEI 27001. Après la formation, les participants passeront l'examen leur permettant d'obtenir le titre de "PECB Certified ISO/CEI 27001 Lead Implementer" qui attestera de leurs capacités à mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

OBJECTIFS

- **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

- Chefs de projet
- Consultants
- Architectes techniques
- Toute personne désirant maîtriser la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI)
- Toute personne responsable du maintien de la conformité aux exigences du SMSI

Pré-requis

Connaitre le guide d'hygiène sécurité de l'ANSSI (Document téléchargeable l'adresse https://www.ib-formation.fr/guide_hygiene_informatique_anssi.pdf)

Certification

Cette formation prépare à l'examen du PECB qui permet d'obtenir la certification ISO 27001 Lead Implementer.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.
- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Programme

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

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

2 - Planification de la mise en œuvre d'un SMSI

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

3 - Mise en œuvre d'un SMSI

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

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

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

5 - Passage de l'examen "PECB ISO 27001 Lead Implementer" (en ligne après la formation)

- Révision des concepts en vue de la certification et examen blanc
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-préparation-a-l'examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70 % est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- Les candidats sont autorisés à utiliser non seulement les supports de cours mais aussi les normes ISO/IEC 27001 et ISO/IEC 27002 qui leurs seront remises
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du SMSI
  - Domaine 2 : Système de Management de la Sécurité de l'Information
  - Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001
  - Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001
  - Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001
  - Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001
  - Domaine 7 : Préparation de l'audit de certification d'un SMSI

Réf. **MG208**

5 jours

(35h présentiel)

3 730 €HT

Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
13/06, 29/08, 24/10, 05/12	13/06, 17/10	
PARIS	**LYON**	
13/06, 29/08, 24/10, 05/12	05/12	

ISO 27001 / ISO 27002 - Les fondamentaux

Les bonnes pratiques pour la gestion de la sécurité de l'information

CERTIFIANT

ACCESSIBLE À DISTANCE

La norme ISO 27001 est devenue la référence internationale en termes de système de management de la sécurité de l'information (SMSI). Les projets de mise en conformité se multipliant et une connaissance des éléments fondamentaux pour la mise en œuvre et la gestion d'un SMSI devient nécessaire. La norme ISO 27001 décrit une approche pragmatique de la gestion de la sécurité de l'information avec le choix de mesures de sécurité découlant d'une appréciation des risques. Elle s'appuie sur le guide ISO 27002 pour fournir des recommandations sur le choix et l'implémentation des mesures de sécurité.

OBJECTIFS

- **Être capable de présenter la norme ISO 27001:2013, les processus de sécurité qui lui sont associés et la démarche de certification**
- **Savoir présenter la norme ISO 27002:2013 et les mesures de sécurité**
- **Comprendre les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité**
- **Savoir sélectionner et approfondir des mesures de sécurité en prenant en compte l'appréciation des risques, les pièges à éviter et l'audit de ces mesures**
- **Disposer d'une vue globale des référentiels existants, des guides d'implémentation ou des bonnes pratiques des mesures de sécurité**

Public

- Toute personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information et enrichir sa connaissance des référentiels existants pour faciliter leur mise en œuvre
- Opérationnels (techniques ou métiers) et auditeurs souhaitant améliorer leur compréhension des mesures propres à la SSI
- RSSI souhaitant avoir un panorama des mesures, organiser leur plan d'action, ou dynamiser les échanges avec les opérationnels

Pré-requis

Culture dans le domaine de la sécurité de l'information

Certification

Cette formation prépare aux examens du PECB qui permettent d'obtenir les certifications ISO/CEI 27001 Foundation et ISO/CEI 27002 Foundation.
Le passage des examens de certification est compris dans le prix de la formation.

Les + de cette formation

- Des exercices pratiques individuels et collectifs basés sur une étude de cas viennent enrichir ce cours magistral basé sur les normes.
- Les animateurs de ce module sont des formateurs certifiés ISO 27001 et ISO 27002.

Programme

1 - Introduction aux systèmes de management

2 - Historique des normes

3 - L'organisation de la sécurité

4 - Présentation détaillée de la norme ISO 27001

5 - L'origine des mesures
- La conformité
- La gestion des risques
- Les ACP ou initiatives internes

6 - Introduction à la gestion des mesures de sécurité
- Les différents acteurs
- Identification des contraintes
- Typologies de mesures de sécurité
- Plan d'action sécurité
- Documentation
- Audit des mesures

7 - La norme ISO 27002
- Présentation et historique
- Structure et objectifs
- Exemple d'application du modèle PDCA aux mesures
- Cas pratique positionnant le stagiaire dans le rôle de : gestionnaire des risques, implémenteur de mesures de sécurité, auditeur

8 - Les référentiels de mesures de sécurité
- Les référentiels sectoriels (HDS, ARJEL, PCI-DSS, SAS-70/ISAE3402/SOC 1-2-3, RGS)
- Les autres sources de référentiels et guides de bonnes pratiques : organismes étatiques (Guide d'hygiène de l'ANSSI, NIST, NSA, etc.), les associations et instituts (SANS, OWASP, CIS, Clusif, etc.), les éditeurs

9 - Passage des examens de certification "PECB Certified ISO/CEI 27001 Foundation" et "PECB Certified ISO/CEI 27002 Foundation" (en ligne après la formation)
- Révision des concepts en vue du passage des certifications et examens blancs
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-péparation-a-l'examen-en-ligne-de-PECB.pdf
- L'examen de certification ISO 27001 est en français tandis que l'examen 27002 est en anglais. Chaque examen se déroule sur 1 heure
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir les certifications
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen "PECB Certified ISO/CEI 27001 Foundation" couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
  - Domaine 2 : Système de management de la sécurité de l'information
- L'examen "PECB Certified ISO/CEI 27002 Foundation" couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux de management de la sécurité de l'information
  - Domaine 2 : Mesures de la sécurité de l'information, conformes à la norme ISO/CEI 27002

Réf. **MG206**
2 jours
(14h présentiel)

1 775 €HT
Offerte

À DISTANCE
07/07, 22/08, 06/10, 01/12
PARIS
07/07, 22/08, 06/10, 01/12

Autres sites, nous consulter

ISO 27005 - Risk Manager

Implémenter la norme ISO 27005

CERTIFIANT

ACCESSIBLE À DISTANCE

Avec la généralisation des échanges sur Internet, les risques en matière de sécurité de l'information sont chaque jour plus importants. L'un des éléments clés dans la prévention des fraudes en ligne, vols d'identité ou autres détériorations de sites Web est la gestion et l'évaluation des risques couvertes par la nouvelle norme internationale ISO/CEI 27005. La formation "ISO/CEI 27005 Risk Manager" permet 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.
Ce programme qui s'inscrit parfaitement dans le processus de mise en œuvre du cadre SMSI selon la norme ISO/CEI 27001, intègre également une présentation de différentes méthodes d'appréciation des risques (OCTAVE, EBIOS, MEHARI,...). Après la formation, les participants passeront l'examen "ISO/CEI 27005 Risk Manager" qui attestera de leurs capacités à apprécier les risques de la sécurité de l'information et à les gérer.

OBJECTIFS

- **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 de mettre en place 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**
- **Être en mesure de conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information**

Public

- Chefs de projet
- Consultants
- Architectes techniques
- Toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation
- Toute personne amenée à mettre en œuvre ISO/CEI 27001 ou impliquée dans un programme de gestion des risques

Pré-requis

Connaitre le guide d'hygiène sécurité de l'ANSSI (Document téléchargeable l'adresse https://www.ib-formation.fr/guide_hygiene_informatique_anssi.pdf)

Certification

Cette formation prépare à l'examen PECB qui permet d'obtenir la certification ISO/IEC 27005 Risk Manager.
Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.
- Répartition théorie/pratique : 60%/40%.
- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Programme

1 - Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005
- Objectifs et structure de la formation
- Concepts du risque
- Définition scientifique du risque
- Le risque et les statistiques
- Le risque et les opportunités
- La perception du risque
- Le risque lié à la sécurité de l'information

2 - Connaître le cadre normatif et réglementaire
- Norme et méthodologie
- ISO/IEC 31000 et ISO/IEC 31010
- Normes de la famille ISO/IEC 27000

3 - Mettre en œuvre un programme de management du risque
- Mandat et engagement de la direction
- Responsable de la gestion du risque et des principales parties prenantes
- Mesures de responsabilisation
- Politique et processus de la gestion du risque
- Approche et méthodologie d'appréciation du risque
- Planification des activités de gestion du risque et fourniture des ressources

4 - Établir le contexte mission, objectifs, valeurs, stratégies
- Établissement du contexte externe et interne
- Identification et analyse des parties prenantes
- Identification et analyse des exigences
- Détermination des objectifs, des critères de base
- Définition du domaine d'application et limites

5 - Identifier les risques
- Techniques de collecte d'information
- Identification des actifs, des menaces, des mesures existantes, des vulnérabilités et des impacts

6 - Analyser et évaluer les risques
- Appréciation des conséquences
- Appréciation de la vraisemblance de l'incident
- Appréciation des niveaux des risques
- Évaluation des risques

7 - Apprécier les risques avec une méthode quantitative
- Notion de ROSI
- Calcul de la perte annuelle anticipée
- Calcul de la valeur d'une mesure de sécurité
- Politiques spécifiques
- Processus de management de la politique

8 - Traiter les risques
- Processus de traitement des risques
- Option et plan de traitement des risques

9 - Apprécier les risques et gérer les risques résiduels
- Acceptation des risques
- Approbation des risques résiduels
- Gestion des risques résiduels
- Communication sur la gestion des risques

10 - Communiquer sur les risques
- Objectifs de communication sur la gestion des risques
- Communication et perception des risques
- Plan de communication

11 - Surveiller les risques
- Surveillance et revue des facteurs de risque et de la gestion des risques
- Amélioration continue de la gestion des risques
- Mesurer le niveau de maturité de la gestion des risques
- Enregistrement des décisions et des plans de communications

12 - Découvrir la méthode OCTAVE
- Méthodologies OCTAVE - OCTAVE Allegro Roadmap

13 - Découvrir la méthode MEHARI
- L'approche MEHARI
- Analyse des enjeux et classification
- Évaluation des services de sécurité
- Analyse des risques
- Développement des plans de sécurité

14 - Découvrir la méthode EBIOS
- Les 5 modules d'EBIOS
- Établissement du contexte
- Étude d'événements redoutés, des scénarios des menaces, des risques et des mesures de sécurité

15 - Passage de l'examen de certification "PECB Certified ISO/CEI 27005 Risk Manager" (en ligne après la formation)
- Révision des concepts en vue de la certification et examen blanc
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-péparation-a-l'examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 2 heures - Un score minimum de 70% est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- Les candidats sont autorisés à utiliser les supports de cours et la norme ISO/IEC 27005
- En cas d'échec, ils bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative

Réf. **MG209**
3 jours
(21h présentiel)

2 380 €HT
Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
26/09, 05/12	03/10	
PARIS	**LYON**	
26/09, 05/12	19/12	

ISO 27032 - Lead Cybersecurity Manager

Devenir le garant de la Cyber sécurité dans l'entreprise

CERTIFIANT

ACCESSIBLE À DISTANCE

La norme ISO/IEC27032 définit un cadre stratégique de classification des échanges d'informations dans le Cyberespace. Cette classification permet d'optimiser l'orchestration du management des différentes actions et outils de sécurisation. Pour préparer et mettre en place un programme de cyber sécurité efficace qui intègrera les relations avec d'autres types de sécurité informatique (SI de l'entreprise...), il peut être bénéfique d'intégrer les recommandations de cette norme. Tout en préparant la certification ISO/IEC 27032, les participants à cette formation de 5 jours s'approprieront les lignes directrices de cette norme pour être en mesure d'élaborer des plans stratégiques de management de la cybersécurité, les mettre en application dans l'entreprise, garantir leur opérabilité avec la sécurisation du système d'informations interne, et assurer leur évolution.

OBJECTIFS

- 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
- Acquérir des connaissances approfondies sur la cybersécurité, la relation entre la cybersécurité et d'autres types de sécurité informatique, et du rôle des parties prenantes dans la cybersécurité
- Se préparer à l'examen qui permet d'obtenir la certification "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager"

Public

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels cherchant à gérer un programme de cybersécurité
- Personnes responsables de concevoir 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

Pré-requis

Une première expérience dans le domaine de la sécurité de l'information est fortement recommandée

Il est recommandé d'avoir suivi les formations "ISO 27001/ISO 27002 - Les fondamentaux" (MG206) et "ITIL® 4 Foundation Certifiant" (MG191)

Certification

Cette formation prépare à l'examen PECB qui permet d'obtenir la certification ISO/IEC 27032 Lead Cybersecurity Manager.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Du matériel de formation contenant plus de 400 pages d'information et d'exemples pratiques sera distribué aux participants.

Programme

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

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

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

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

Réf. MG827
5 jours
(35h présentiel)

3 760 €HT
Offerte

À DISTANCE
05/09, 14/11

PARIS
05/09, 14/11

Autres sites, nous consulter

+ de 3000 missions réalisées chaque année

Un projet de formation sur-mesure ?

Vous devez former plusieurs collaborateurs sur une même thématique ou une même technologie et vous souhaitez pour cela organiser une formation en intra-entreprise ?

Qu'il s'agisse de décliner les programmes présentés sur notre site web ou de concevoir un dispositif sur-mesure, nos équipes sont à votre entière disposition pour vous accompagner dans votre projet.

Après une analyse de vos besoins, elles apporteront à votre demande la réponse pédagogique, technique et logistique la plus pertinente.

Contactez nos Conseillers Formation au 0 825 07 6000

ISO 27035 - Lead Incident Manager : gestion des incidents de sécurité

CERTIFIANT

ACCESSIBLE À DISTANCE

Mettre en œuvre, gérer et tenir à jour un plan d'intervention en cas d'incident

OBJECTIFS

- Être capable de 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
- Comprendre comment développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

Public

- 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

Pré-requis

Aucun

Certification

Cette formation prépare à l'examen PECB qui permet d'obtenir la certification ISO/CEI 27035 Lead Incident Manager.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.

Programme

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

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

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

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

5 - Passage de l'examen de certification "PECB certified ISO/CEI 27035 Lead Incident Manager" (en ligne après la formation)

- Révision des concepts en vue de la certification
- Un voucher permettant le passage du test
- de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-preparation-a-l'examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en anglais en 3 heures
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires
- 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

Réf. MG841
5 jours
(35h présentiel)

3 690 €HT
Paris 115 €HT

À DISTANCE	Autres sites, nous consulter
03/10	
PARIS	
03/10	

CERTIFIANT

Les programmes certifiants

Les programmes certifiants ib sont destinés aux personnes souhaitant acquérir de nouveaux savoirs et les valoriser par l'obtention d'une certification reconnue sur le marché de l'informatique.

Des cursus de plusieurs semaines permettant d'évoluer vers un nouveau métier aux formations courtes visant à acquérir une expertise sur un domaine précis, notre offre de formations certifiantes est à la fois complète et variée

Le passage des examens de certification, généralement proposés en fin de session, est systématiquement inclus dans le prix de nos formations certifiantes.

Ebios Risk Manager Certifiant

Evaluer la sécurité du SI

EBIOS (Étude des Besoins et Identification des Objectifs de Sécurité) s'est imposée comme la méthodologie phare en France pour apprécier les risques dans le secteur public comme dans les entreprises. Elle est recommandée par l'ANSSI pour l'élaboration de PSSI et schéma directeur, pour l'homologation de téléservice dans le cadre du RGS, dans le guide GISSIP comme par la CNIL pour réaliser des analyses d'impacts sur les données nominatives (PIA ou Privacy Impact Assessment). EBIOS présente des caractéristiques uniques qui permettent son usage dans tous les secteurs de la sécurité, bien au-delà de la SSI. EBIOS permet également d'identifier les risques d'un système en construction, donc encore non existant, et demeure idéale pour la rédaction de cahier des charges. La formation certifiante "EBIOS Risk Manager" traite de la méthode EBIOS de l'ANSSI et de la gestion du risque de sécurité de l'information en général. Cette formation permet d'acquérir les compétences nécessaires à la conduite de bout en bout d'une appréciation des risques, de l'étude des besoins à la formalisation des objectifs de sécurité.

OBJECTIFS

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

Public

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

Pré-requis

Connaître le guide d'hygiène sécurité de l'ANSSI (Document téléchargeable l'adresse https://www.ib-formation.fr/guide_hygiene_informatique_anssi.pdf)

Certification

Cette formation prépare à l'examen PECB qui permet d'obtenir la certification EBIOS Risk Manager.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cette formation se compose d'une alternance d'apports théoriques (70% du temps), de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.
- Tous les ateliers proposés reposent sur divers exemples d'une entreprise fictive (@RCHIMED) qui fera l'objet d'une étude de cas complète lors de la phase de mise en application.

Programme

1 - Introduction à la méthode EBIOS
- Présentation générale d'EBIOS
- Principales définition
- Les 5 phases d'EBIOS : étude du contexte, des évènements redoutés, des scénarios de menaces, des risques et des mesures de sécurité
- L'ISO 27005 appliquée dans EBIOS
- Les grands principes d'EBIOS : implication sensibilisation, adhésion et responsabilisation

2 - Définir le cadre de la gestion des risques
- Cadrage de l'étude des risques
- Description du contexte général
- Limites du périmètre de l'étude
- Identification des paramètres à prendre en compte
- Identification des sources de menace

3 - Préparer les métriques
- Définition des critères de sécurité
- Élaboration des échelles de besoin
- Élaboration d'une échelle de niveaux de gravité
- Élaboration d'une échelle de niveaux de vraisemblance
- Définition des critères de gestion des risques

4 - Identifier les biens
- Identification des biens essentiels, leurs relations et leurs dépositaires
- Identifier les biens supports, leurs relations et leurs dépositaires
- Détermination des liens entre les biens essentiels et les biens supports
- Identification des mesures de sécurité existantes

5 - Apprécier les événements redoutés
- Analyse d'événements redoutés
- Évaluation de chaque événement redouté

6 - Apprécier les scénarios de menaces
- Analyse de tous les scenarios de menaces
- Évaluation de chaque scenario de menace

7 - Apprécier les risques
- Analyse des risques
- Évaluation de chaque risque

8 - Identifier les objectifs de sécurité
- Choix des options de traitement des risques
- Analyse des risques résiduels

9 - Formaliser les mesures de sécurité à mettre en œuvre
- Détermination des mesures de sécurité
- Analyse des risques résiduels
- Établissement d'une déclaration d'applicabilité

10 - Mettre en œuvre les scenarios de sécurité
- Élaboration d'un plan d'actions
- Suivi de la réalisation des mesures de sécurité
- Analyse des risques résiduels
- L'homologation de sécurité

11 - Préparation de l'examen à travers une étude de cas
- Passage en revue de tous les thèmes abordés

12 - Passage de l'examen "PECB Certified EBIOS Risk Manager"
- Passage de l'examen écrit de certification en français qui consiste à répondre à 12 questions en 3 heures
- Un score minimum de 70 % est exigé pour réussir l'examen
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information selon la méthode EBIOS
  - Domaine 2 : Programme de gestion des risques liés à la sécurité de l'information basé sur EBIOS
  - Domaine 3 : Appréciation des risques liés à la sécurité de l'information basée sur la méthode EBIOS

Réf. **MG807**
3 jours
(21h présentiel)

2 440 €HT
Offerte

PARIS
20/06, 12/09, 19/12

Autres sites, nous consulter

ISO 27005 - Certified Risk Manager avec EBIOS

Évaluer les risques et mettre en place les réponses ad'hoc

CERTIFIANT

En matière d'appréciation des risques, EBIOS (pour Expression des Besoins et Identification des Objectifs de Sécurité), la méthode proposée par l'Agence National de la Sécurité des Systèmes d'Information (ANSSI) qui a notamment pour mission de proposer des règles à appliquer pour la protection des systèmes d'information de l'Etat français, fait figure de référence. Conforme à la norme ISO 27005 conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche méthodique du risque, EBIOS constitue la boite à outils idéale pour construire son référentiel SSI. Indispensable à tout manager impliqué dans la gestion de la sécurité, cette formation intensive de 5 jours prépare aux certifications EBIOS Risk Manager et ISO 27005 Risk Manager qui seront passées en séance.

OBJECTIFS

- Connaître les concepts, approches, méthodes et techniques associés à 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
- Être en mesure de conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information
- Connaître les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Maîtriser les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Acquérir les compétences nécessaires afin de mener une étude EBIOS et en analyser et restituer les résultats

Public

- Chefs de projet, consultants, architectes techniques
- Toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation
- Toute personne amenée à mettre en œuvre ISO/CEI 27001 ou impliquée dans un programme de gestion des risques selon la méthode EBIOS

Pré-requis

Connaitre le guide d'hygiène sécurité de l'ANSSI (Document téléchargeable l'adresse https://www.ib-formation.fr/guide_hygiene_informatique_anssi.pdf)

Certification

Cette formation prépare aux examens PECB qui permettent d'obtenir les certifications ISO/IEC 27005 Risk Manager et EBIOS Risk Manager. Le passage des examens est compris dans le prix de la formation.

Les + de cette formation

- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage des certifications dans les meilleures conditions.
- Les résultats des examens sont disponibles sous 4 à 8 semaines et sont directement envoyés aux candidats par email.

Programme

1ère partie : ISO 27005 - Risk Manager

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

2 - Connaître le cadre normatif et réglementaire
- Norme et méthodologie
- ISO/IEC 31000 et ISO/IEC 31010
- Normes de la famille ISO/IEC 27000

3 - Mettre en œuvre un programme de management du risque
- Mandat et engagement de la direction
- Responsable de la gestion du risque et des principales parties prenantes
- Mesures de responsabilisation
- Politique et processus de la gestion du risque

4 - Établir le contexte mission, objectifs, valeurs, stratégies
- Établissement du contexte externe et interne
- Identification et analyse des parties prenantes
- Identification et analyse des exigences

5 - Identifier les risques
- Techniques de collecte d'information
- Identification des actifs, des menaces, des mesures existantes, des vulnérabilités

6 - Analyser et évaluer les risques
- Appréciation des conséquences
- Appréciation de la vraisemblance de l'incident
- Appréciation des niveaux des risques
- Évaluation des risques

7 - Apprécier les risques avec une méthode quantitative
- Notion de ROSI
- Calcul de la perte annuelle anticipée
- Calcul de la valeur d'une mesure de sécurité
- Politiques spécifiques

8 - Traiter les risques
- Processus et option de traitement des risques
- Plan de traitement des risques

9 - Apprécier les risques et gérer les risques résiduels
- Acceptation des risques
- Approbation des risques résiduels
- Gestion des risques résiduels
- Communication sur la gestion des risques

10 - Communiquer sur les risques
- Communication et perception des risques
- Plan de communication

11 - Surveiller les risques
- Surveillance et revue des facteurs de risque
- Surveillance et revue de la gestion des risque
- Amélioration continue de la gestion des risques

12 - Découvrir la méthode OCTAVE
- Méthodologies OCTAVE - OCTAVE Allegro Roadmap

13 - Découvrir la méthode MEHARI
- L'approche MEHARI
- Analyse des enjeux et classification
- Évaluation des services de sécurité
- Analyse des risques
- Développement des plans de sécurité

14 - Découvrir la méthode EBIOS
- Les 5 modules d'EBIOS
- Établissement du contexte

2ème partie : EBIOS Risk Manager certifiant

1 - Introduction à la méthode EBIOS
- Principales définition
- Les 5 phases d'EBIOS
- L'ISO 27005 appliquée dans EBIOS
- Les grands principes d'EBIOS

2 - Définir le cadre de la gestion des risques
- Cadrage de l'étude des risques
- Description du contexte général
- Limites du périmètre de l'étude
- Identification des paramètres à prendre en compte et des sources de menace

3 - Préparer les métriques
- Définition des critères de sécurité
- Élaboration des échelles de besoin
- Définition des critères de gestion des risques

4 - Identifier les biens
- Identification des biens essentiels, leurs relations et leurs dépositaires
- Identifier les biens supports, leurs relations et leurs dépositaires
- Identification des mesures de sécurité existantes

5 - Apprécier les événements redoutés
- Analyse d'événements redoutés
- Évaluation de chaque événement redouté

6 - Apprécier les scénarios de menaces
- Analyse de tous les scenarios de menaces
- Évaluation de chaque scenario de menace

7 - Apprécier les risques
- Analyse des risques
- Évaluation de chaque risque

8 - Identifier les objectifs de sécurité
- Choix des options de traitement des risques
- Analyse des risques résiduels

9 - Formaliser les mesures de sécurité à mettre en œuvre
- Détermination des mesures de sécurité
- Analyse des risques résiduels
- Établissement d'une déclaration d'applicabilité

10 - Mettre en œuvre les scenarios de sécurité
- Élaboration d'un plan d'actions
- Suivi de la réalisation des mesures de sécurité
- Analyse des risques résiduels
- L'homologation de sécurité

11 - Préparation de l'examen à travers une étude de cas

3ème partie : Passage des examens de certification ISO/IEC 27005 Risk Manager et EBIOS Risk Manager

1 - Examen de certification ISO/IEC 27005 Risk Manager

2 - Examen de certification EBIOS Risk Manager

Réf. **MG828**
5 jours
(35h présentiel)

3 450 €HT
Offerte

PARIS	Autres sites, nous consulter
20/06, 12/09, 28/11	

CLEH, Certified Lead Ethical Hacker

S'initier à la conduite de piratage éthique

CERTIFIANT

ACCESSIBLE À DISTANCE

OBJECTIFS

- Comprendre et connaître les référentiels liés au pentest
- Prendre connaissance des outils et source de veille
- Savoir mener une analyse de vulnérabilité sur un système Linux et Windows
- Comprendre l'exploitation et la post-exploitation des différents environnements
- Préparer et passer l'examen de certification "CLEH, Certified Lead Ethical Hacker" du PECB

Public

- Professionnels de la cybersécurité
- Spécialistes des TI

Pré-requis

Connaissance de base d'un système Linux et Windows
Connaissance des réseaux et modèle OSI

Certification

Cette formation prépare à l'examen PECB qui permet d'obtenir la certification PECB Lead Ethical Hacker.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans les investigations légales informatiques.
- 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.
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré.

Programme

1 - Introduction
- Panorama et faits marquants (WannaCry, NotPetya, Facebook)
- Les composants de la sécurité (CID)
- Les types et référentiels du Pentest : BlackBox / GreyBox / White / RedBlue Team - PTES , OSSTM (OWASP)
- Le cycle de l'attaquant
- La trousse à outil et l'environnement : Kali (Site de Kali et système), étude de l'environnement, conservation des résultats (Utilisation de keepnote ou équivalent)

2 - Intelligence Gathering
- Les principes de la recherche Internet/Passive (OSINT) : exemple de cas
- Recherche sur l'entreprise : physique, logique, organisation, électronique, recherche infrastructure, finance
- Recherche sur l'employé : social network, présence sur internet
- Reconnaissance externe : reconnaissance passive (Recherche DNS et BGP), reconnaissance Active (Scan des services, Scan des versions, Scan des OS, Recherche des services avancée, AXFR, SMTP, DNSBF etc...)
- Reconnaissance interne : énumération du réseau courant (ARP/ICMP), le focus interne

3 - Modélisation et analyse des vulnérabilités
- Etude et compréhension des CVEs : les types (Remote , Local , Web)
- Examen et revue des vulnérabilités manuels : NMAP → CVE DETAILS
- Examen et revue des vulnérabilités automatiques : Nessus, Openvas, NSE
- Bilan et cartographie

4 - Exploitation
- Les exploitations réseaux courantes : le man in the middle, fake DHCP
- Client exploitation : les attaques courantes sur l'humain (le navigateur, attaque sur les fichiers, USB)
- Exploitation des services et OS : mauvaise configuration - tous systèmes (Default password, Anonymous ftp), Windows (Buffer Overflow à la main, exploitation connue à l'aide d'exploit-db), Linux (exploitation connue à l'aide d'exploit-db)

5 - Post-exploitation
- Élévation des privilèges : Windows (Linux)
- Persistence / Backdoor : mise en place de backdoor sous Windows et Linux, Cron, Scheduled Task
- Pivoting et rebond
- Exfiltration de données

6 - Préparation et passage de l'examen de certification PECB Certified Lead Ethical Hacker
- Révision des concepts en vue de la certification
- Examen blanc
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétence suivants :
  - Domaine 1 : Principes et concepts fondamentaux du piratage éthique
  - Domaine 2 : Mécanismes d'attaque
  - Domaine 3 : Principes et référentiels sur les tests d'intrusion
  - Domaine 4 : Planifier et effectuer des tests de pénétration en utilisant divers outils et techniques
  - Domaine 5 : Rédaction de rapports de tests d'intrusion
- L'examen comprend deux parties. La première partie est un examen sur papier, qui consiste en des questions de type dissertation. La deuxième partie est plutôt technique, dans laquelle le candidat devra effectuer des exercices de test d'intrusion sur ordinateur et rédiger un rapport d'analyse
- Les participants sont autorisés à utiliser leurs notes personnelles lors de l'examen sur papier et lors de la partie pratique de l'examen

Réf. SE202
5 jours
(35h présentiel)

3 890 €HT

Paris 115 €HT

À DISTANCE
04/07, 17/10, 12/12
Autres sites, nous consulter

PARIS
04/07, 17/10, 12/12

Renseignements, conseils, projets, inscriptions...

Un numéro unique :

0 825 07 6000

SCADA - Sécurité des systèmes industriels

Mettre en œuvre un système de contrôle et d'acquisition de données en temps réel

Les systèmes industriels ne sont plus isolés, bien au contraire. Ils se retrouvent de plus en plus exposés, car informatisés et interconnectés à d'autres actifs informationnels, souvent du monde « IT ». 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, notamment les systèmes SCADA.

OBJECTIFS

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

Public

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

Pré-requis

Disposer d'une bonne connaissance générale de la sécurité des systèmes d'information

La connaissance des systèmes industriels n'est pas un pré-requis

Les + de cette formation

- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions.

Programme

1 - Objectifs et structure du cours

2 - Principes et notions des fondamentaux SCADA et de leur sécurité

3 - État de l'art de la sécurité SCADA

4 - Les protocoles et leurs vulnérabilités
- S7
- Modbus
- DNPS
- ICCP / TASE

5 - Automates et IHM (Systèmes d'exploitation Windows)
- Services courants
- Vulnérabilités rencontrées
- Top 10 OWASP
- Windows et SCADA
- Déni de service et résilience

6 - Les normes de sécurité applicables aux environnements industriels
- IEC 62443-x
- NIST SPB00-82

7 - Les systèmes SCADA distants
- VPN
- Boîtiers de télétransmission
- Sans-fil (Wifi, liaisons radio)
- Exposition sur internet : risques et vulnérabilités

8 - Les architectures SCADA

9 - Sécurité organisationnelle d'un réseau SCADA

10 - Points sensibles et niveaux de classification ANSSI

11 - Mesures de sécurité en lien avec l'architecture
- Filtrage IP
- Cloisonnement
- Journalisation d'incidents

Réf. SE208
3 jours
(21h présentiel)

3 675 €HT
Paris 115 €HT

PARIS
17/10

Autres sites, nous consulter

30 Cursus Métier à découvrir

Pour vous permettre de disposer d'équipes toujours plus polyvalentes et rapidement opérationnelles, ib vous propose des cursus adaptés à leur évolution vers de nouveaux domaines de compétences. Étudiés pour favoriser une acquisition rapide de nouveaux savoirs, nos cursus métier couvrent les thématiques actuellement au cœur des préoccupations des entreprises.

Retrouvez tous nos Cursus Métier sur www.ib-formation.fr

Préparation à la Certification CISSP (Information Systems Security Profesionnal)

ACCESSIBLE À DISTANCE

La certification des professionnels de la Sécurité de l'information

La certification de référence CISSP® (Certified Information Systems Security Professional) est indépendante, pragmatique et internationalement reconnue. Créée et maintenue par des professionnels de la sécurité informatique en exercice, elle permet d'étalonner son niveau de compétence selon 3 axes : les connaissances techniques, les capacités d'analyse des risques et les aptitudes à l'audit des systèmes. La certification CISSP n'atteste pas seulement d'une bonne connaissance des technologies, elle démontre surtout une réelle capacité à les imbriquer et à les assembler pour répondre au mieux aux besoins des entreprises en matière de sécurité.

OBJECTIFS

- Connaître les thèmes, les domaines et rubriques du Common Body of Knowledge (CBK®)
- Maîtriser les fondamentaux de la sécurité des SI
- Se préparer à l'examen de certification CISSP

Public

- RSSI, DSI
- Consultants / Auditeurs
- Administrateurs Système et réseaux

Pré-requis

Justifier de cinq ans d'expérience professionnelle minimum dans au moins 2 des 8 domaines du CBK®

Certification

Cette formation prépare au test CISSP (en option) qui permet d'obtenir la certification Certified Information Systems Security Professional (CISSP). Inscription à l'examen de certification CISSP (en option au prix de 800 €).

Les + de cette formation

- Le contenu de la formation est sans cesse remanié et mis à jour pour refléter les dernières évolutions des questions de sécurité, des préoccupations et des contre-mesures actuelles.
- La formation est un véritable lieu d'échange où chaque participant est appelé à intervenir sur différents sujets des domaines du CBK.

Programme

1 - Sécurité des informations et gestion des risques

- Les concepts de confidentialité, intégrité et disponibilité
- Les principes de gouvernance de la sécurité
- La conformité
- Les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
- L'éthique professionnelle
- La politique de sécurité, les standards, les procédures et les guidelines
- Les exigences de continuité d'activité
- Les politiques de sécurité du personnel
- Les concepts de management des risques
- Le modèle de menace
- Les considérations de risque de sécurité dans la stratégie d'acquisition
- La sensibilisation, la formation et l'éducation à la sécurité de l'information

2 - La sécurité des assets

- Classification de l'information et support des assets
- Le maintien de la propriété
- Protéger la confidentialité
- Assurer la rétention appropriée
- Les mesures de sécurité des données
- Les exigences de manipulation

3 - Ingénierie de la sécurité

- Les processus d'engineering et les principes de conception sécurisée
- Comprendre les concepts fondamentaux des modèles de sécurité
- Les mesures et contre-mesures
- Les possibilités de sécurités offertes par les systèmes d'information
- Les vulnérabilités de sécurité des architectures, des conceptions, des solutions
- Evaluer et réduire les vulnérabilités de sécurité des systèmes web, mobiles et des systèmes embarqués
- La cryptographie
- Les principes de sécurité au site et à la conception de l'installation
- La sécurité physique

4 - Sécurité des télécommunications et des réseaux

- Les principes de conception sécurisée à l'architectures réseau
- Sécuriser les composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou limiter les attaques réseau

5 - La gestion des identités et des accès

- Contrôle d'accès physique et logique aux assets
- Gérer l'identification et l'authentification des personnes et des équipements
- L'identité en tant que service
- Les services d'identité tiers
- Les mécanismes d'autorisation
- Les attaques au contrôle d'accès
- Le cycle de vie des identités et du provisionnement des accès

6 - Évaluation de la sécurité et tests

- Les stratégies d'évaluation et de test de sécurité
- Tests de mesures de sécurité
- Les données des processus de sécurité
- Les résultats des tests
- Les audits internes ou third-party

7 - Continuité des opérations et plan de reprise

- Les investigations
- Les exigences des types d'investigations
- Les activités de monitoring et de logging
- Le provisionnement des ressources
- Les concepts fondamentaux de sécurité des opérations
- Les techniques de protection de ressources
- La gestion de incidents
- Opérer et maintenir des mesures de sécurité préventives
- La gestion des patchs et vulnérabilités
- Les processus de gestion des changements
- Les stratégies de reprise
- Les stratégies de reprise après sinistre
- Les plans de reprise après sinistre
- Le Plan de Continuité d'Activité
- La gestion de la sécurité physique
- Les problèmes de sécurité du personnel

8 - La sécurité du développement logiciel

- La sécurité dans le cycle de vie de développement logiciel
- Les mesures de sécurité dans les environnements de développement
- L'efficacité de la sécurité du logiciel
- Evaluer l'impact de la sécurité d'un logiciel acquis

Réf. MG211
5 jours
(35h présentiel)

3 690 €HT
Offerte

À DISTANCE
29/08, 24/10, 12/12
PARIS
29/08, 24/10, 12/12

Autres sites, nous consulter

Préparation à la certification CRISC (Risk and Information Systems Control)

Identifier, évaluer et répondre aux risques pour les atténuer

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

CRISC (Certified in Risk and Information Systems Control) est la seule certification permettant aux professionnels de l'informatique de relever les défis uniques de l'informatique et de la gestion des risques de l'entreprise, en les positionnant pour qu'ils deviennent des partenaires stratégiques. Depuis sa création en 2010, près de 17 000 professionnels ont obtenu la certification CRISC, élue Gold Award du meilleur programme de certification professionnelle aux SC Magazine 2013 Awards. Cette formation est conçue pour couvrir l'intégralité du programme du CRISC et vous préparer à réussir l'examen.

OBJECTIFS

- Connaître les concepts, approches, méthodes et techniques associés à 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
- Être en mesure de conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information
- Connaître les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Maîtriser les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Acquérir les compétences nécessaires afin de mener une étude EBIOS et en analyser et restituer les résultats

Public

- Candidats à l'examen du CRISC, professionnels de l'informatique et des métiers ayant une expérience en gestion des risques d'au moins 3 à 5 ans

Pré-requis

Une expérience de base sur la gestion des risques est un plus pour suivre la formation

Certification

Cette formation prépare au test CRISC (en option) qui permet d'obtenir la certification Certified in Risk and Information Systems Control (CRISC).

En option au prix de 400 € : un pack de préparation à l'examen incluant le manuel officiel de l'ISACA et l'accès à la base officielle de questions pour une durée de 12 mois.

L'inscription à l'examen se fait directement auprès de l'ISACA par le candidat avec son dossier https://www.isaca.org/credentialing/crisc/crisc-exam. L'examen se déroule sur 4 heures. Il est en anglais et comporte 150 questions à choix multiples.

Les frais d'inscription à l'examen ne sont pas compris dans le prix de la formation.

Les + de cette formation

- Formation accréditée par ISACA et animée par un formateur accrédité par ISACA pour les ateliers de préparation au CRISC.
- Manuel officiel de préparation au CRISC fourni dans le cadre de la session, au format électronique.
- Copie intégrale des slides de présentation (ISACA) utilisées par votre formateur pendant la formation (au format électronique).

Programme

1 - Introduction

2 - Réussir le CRISC

- Les pré-requis pour la certification
- A propos de l'examen CGEIT
- Étapes pour la certification

3 - Domaine 1 : Identification des risques TI

- Collecter et passer en revue les informations, y compris la documentation existante, concernant les environnements métier et informatiques, internes et externes de l'organisation afin d'identifier les impacts potentiels des risques informatiques sur les objectifs et les opérations de l'entreprise
- Identifier les menaces et vulnérabilités potentielles pour les personnes, les processus et la technologie de l'entreprise afin de permettre l'analyse des risques informatiques
- Développer un ensemble complet de scénarios de risque informatique basés sur les informations disponibles pour déterminer l'impact potentiel sur les objectifs et les opérations de l'entreprise
- Identifier les principaux intervenants dans les scénarios de risque informatique pour aider à établir la responsabilité
- Établir un registre des risques informatiques pour avoir l'assurance que les scénarios de risques informatiques identifiés sont comptabilisés et intégrés dans le profil de risque de l'entreprise
- Identifier l'appétit pour le risque et la tolérance définis par la direction et les principales parties prenantes afin de garantir l'alignement sur les objectifs de l'entreprise

4 - Domaine 2 : Évaluation des risques informatiques

- Analyser les scénarios de risque en fonction de critères organisationnels afin de déterminer la probabilité et l'impact d'un risque identifié
- Identifier l'état actuel des contrôles existants et évaluer leur efficacité pour l'atténuation des risques informatiques
- Passer en revue les résultats de l'analyse des risques et des contrôles afin d'évaluer tout écart entre les états actuel et souhaité de l'environnement de risque informatique
- Obtenir l'assurance que la propriété des risques est attribuée au niveau approprié pour établir des lignes de responsabilité claires
- Communiquer les résultats des évaluations des risques à la haute direction et aux parties prenantes appropriées pour permettre une prise de décision basée sur les risques
- Mettre à jour le registre des risques avec les résultats de l'évaluation des risques

5 - Domaine 3 : Réponse aux risques et atténuation

- Consulter les responsables des risques pour sélectionner et aligner les réponses au risque recommandées sur les objectifs de l'entreprise et permettre une prise de décision en connaissance de cause
- Consulter les responsables des risques ou les aider à prendre en charge l'élaboration de plans d'action pour faire en sorte que les plans incluent des éléments clés
- Consulter sur la conception et la mise en œuvre ou l'ajustement des contrôles d'atténuation pour s'assurer que le risque est géré à un niveau acceptable
- Obtenir l'assurance que la propriété du contrôle est attribuée afin d'établir des lignes de responsabilité claires
- Assister les propriétaires de contrôle dans le développement de procédures de contrôle et de la documentation afin de permettre une exécution efficace du contrôle
- Mettre à jour le registre des risques afin de refléter les changements dans les risques et la réponse des risques de la direction
- Valider que les réponses aux risques ont été exécutées conformément aux plans d'action des risques

6 - Domaine 4 : Surveillance des risques et des contrôles

- Définir et établir des indicateurs clés de risque (KRI) et des seuils basés sur les données disponibles, afin de permettre le suivi de l'évolution du risque
- Surveiller et analyser les indicateurs de risque clés (KRI) pour identifier les changements ou les tendances du profil de risque informatique
- Rendre compte des changements ou des tendances liés au profil de risque informatique afin d'aider la direction et les parties prenantes concernées à prendre des décisions
- Faciliter l'identification des métriques et des indicateurs de performance clés (KPI) afin de permettre la mesure de la performance du contrôle
- Surveiller et analyser les indicateurs de performance clés (KPI) afin d'identifier les changements ou les tendances liés à l'environnement de contrôle et de déterminer l'efficience et l'efficacité des contrôles
- Passer en revue les résultats des évaluations de contrôle pour déterminer l'efficacité de l'environnement de contrôle

7 - Administration et techniques pour l'examen

- Administration de l'examen
- Techniques pour l'examen
- Questions fréquentes

8 - Examen blanc

9 - Questions et conclusion

Réf. MG224
4 jours
(28h présentiel)

2 950 €HT
Offerte

À DISTANCE
07/06, 10/10

PARIS
07/06, 10/10

Autres sites, nous consulter

Préparation à la certification CISM (Information Security Manager)

Devenez "Certified Information Security Manager"

Créée par un groupe d'auditeurs experts dans le contrôle des systèmes d'information, l'ISACA est une association professionnelle internationale dont l'objectif est d'améliorer la gouvernance des systèmes d'information. Pour accompagner les personnes en charge de la sécurité informatique, l'ISACA a mis au point un programme de certification, le CISM (Certified Information Security Manager), qui couvre les différents aspects de la sécurité, de la gouvernance à la gestion des incidents. A l'issue de cette formation certifiante de 3 jours, les participants disposeront d'une bonne connaissance des schémas directeurs principaux de la sécurité de l'information.

OBJECTIFS

- **Découvrir et maîtriser les 4 grands domaines sur lesquels porte l'examen CISM**
- **Être capable d'assimiler le vocabulaire de la certification CISM et les idées directrices de l'examen**
- **Pouvoir s'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire**
- **Se préparer au passage de l'examen de certification CISM**

Public

- Professionnels en sécurité
- RSSI
- Consultants en sécurité
- Toute personne souhaitant acquérir des connaissances en la matière

Pré-requis

Connaissances de base dans le fonctionnement des systèmes d'information

Afin d'obtenir la certification CISM, il faudra justifier de 5 ans d'expérience dans la gestion de la sécurité de l'informations
Des dérogations sont néanmoins possibles pour un maximum de 2 ans

Certification

Cette formation prépare au test CISM (en option) qui permet d'obtenir la Certified Information Security Manager (CISM).

Les + de cette formation

- Une bonne préparation à l'examen CISM (Certified Information Security Manager), la certification professionnelle mondialement reconnue et délivrée par l'ISACA (Information Systems Audit and Control Association).
- Une pédagogie basée sur le partage d'expérience et de bonnes pratiques de la part d'un consultant spécialiste des métiers de la sécurité informatique.
- L'inscription à l'examen se fait directement et individuellement sur le site de l'organisme gestionnaire de l'examen de certification ISACA : www.isaca.org.
- Le support de cours fournit est en anglais.

Programme

1 - Gouvernance de la sécurité d'information

- Expliquer la nécessité et les résultats souhaités d'une stratégie efficace de sécurité de l'information
- Créer une stratégie de sécurité des informations alignée sur les buts et objectifs de l'entreprise
- Obtenir l'appui des parties prenantes à l'aide d'analyses de rentabilisation
- Identifier les rôles et responsabilités clés nécessaires à l'exécution d'un plan d'action
- Établir des métriques pour mesurer et surveiller les performances de la gouvernance de la sécurité

2 - Gestion des risques de l'information

- Expliquer l'importance de la gestion des risques en tant qu'outil pour répondre aux besoins de l'entreprise et développer un programme de gestion de la sécurité pour répondre à ces besoins
- Identifier, classer et répondre à un risque d'une manière appropriée, telle que définie par les directives de l'organisation
- Évaluer la pertinence et l'efficacité des contrôles de sécurité de l'information
- Signaler efficacement les risques liés à la sécurité de l'information

3 - Développement et gestion de programmes de sécurité de l'information

- Aligner les exigences du programme de sécurité des informations sur celles des autres fonctions de l'entreprise
- Gérer les ressources du programme de sécurité de l'information
- Concevoir et mettre en œuvre des contrôles de sécurité des informations
- Intégrer les exigences de sécurité de l'information dans les contrats, les accords et les processus de gestion tiers

4 - Gestion des incidents de sécurité de l'information

- Comprendre les concepts et les pratiques de la gestion des incidents
- Identifier les composants d'un plan d'intervention en cas d'incident et évaluer son efficacité
- Comprendre les concepts clés de la planification de la continuité des activités, ou de la planification de la continuité des opérations et de la reprise après sinistre, ou du DRP

5 - Exemple d'examen CISM

Réf. **MG212**
3 jours
(21h présentiel)

3 150 €HT

PARIS 12/09	Autres sites, nous consulter

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Préparation à la certification CISA (Information Systems Auditor)

Devenez "Certified Information Security Auditor"

Le CISA est une certification d'Audit des Systèmes d'Information reconnue dans le monde entier et définie par l'ISACA®. Destinée aux consultants qui disposent d'une première expérience dans le domaine de l'audit des systèmes d'information, elle atteste de la maitrise de la gouvernance, du management et du suivi des risques informatiques. Cette formation officielle de 5 jours permet aux participants de préparer le passage de la certification CISA dont le passage s'effectue en ligne après la formation.

OBJECTIFS

- Savoir analyser les différents domaines du programme sur lesquels porte l'examen
- Être capable d'assimiler le vocabulaire et les idées directrices de l'examen
- Pouvoir s'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire
- Se préparer au passage de l'examen de certification CISA

Public

- Auditeur, consultants IT, responsables IT, responsables de la sécurité, directeurs des SI

Pré-requis

Connaissances générales en informatique, sécurité et audit
Connaissances de base dans le fonctionnement des systèmes d'information

Certification

Cette formation prépare au test CISA (en option) qui permet d'obtenir la certification Certified Information Systems Auditor (CISA).

Les + de cette formation

- La formation prépare à la certification CISA (Certified Information Systems Auditor), seule certification reconnue mondialement dans le domaine de la gouvernance, de l'audit, du contrôle et de la sécurité des SI.
- Des aspects théoriques largement complétés de retours d'expériences de la part du consultant.
- L'inscription à l'examen se fait directement et individuellement sur le site de l'organisme gestionnaire de l'examen de certification ISACA : www.isaca.org.

Programme

1 - Domaine 1: processus d'audit des systèmes d'information
- Les standards d'audit
- L'analyse de risque et le contrôle interne
- La pratique d'un audit SI

2 - Domaine 2 : gouvernance et gestion des systèmes d'information
- La stratégie de la gouvernance du SI
- Les procédures et Risk management
- La pratique de la gouvernance des SI
- L'audit d'une structure de gouvernance

3 - Domaine 3 : acquisition, conception, implantation des SI
- La gestion de projet : pratique et audit
- Les pratiques de développement
- L'audit de la maintenance applicative et des systèmes
- Les contrôles applicatifs

4 - Domaine 4 : exploitation, entretien et soutien des systèmes d'information
- L'audit de l'exploitation des SI
- L'audit des aspects matériels du SI
- L'audit des architectures SI et réseaux

5 - Domaine 5 : Protection des actifs informationnels
- La gestion de la sécurité : politique et gouvernance
- L'audit et la sécurité logique et physique
- L'audit de la sécurité des réseaux
- L'audit des dispositifs nomades

6 - Préparation à l'examen

Réf. MG213
5 jours
(35h présentiel)

3 750 €HT

PARIS	Autres sites, nous consulter
24/10	

Pour vous inscrire à une formation... il y a toujours un moyen de nous contacter

Par téléphone

Nos Conseillers Formation sont joignables de 8h30 à 18h00 au 0 825 07 6000. Ils répondront à toutes vos questions concernant les formations, les dates de sessions, les opportunités de dernière minute...

Par e-mail

Une adresse unique : espace.clients@ib.cegos.fr pour toutes vos inscriptions ou demandes de renseignements.

Par Internet

Retrouvez sur www.ib-formation.fr l'intégralité de nos programmes ainsi que toutes les informations qui vous seront utiles : dates de sessions, plans d'accès, offres de dernière minute, informations sur les évènements ib....

Homologation de la sécurité - Référentiel Général de Sécurité (RGS) 2.0

ACCESSIBLE À DISTANCE

Mettre ses pratiques en conformité avec les obligations légales

Dans le cadre de la mise en œuvre de téléservices, les autorités administratives sont soumises à l'obligation légale de respecter l'ordonnance n° 2005-1516 du 8 décembre 2005 relative à leurs échanges électroniques avec leurs usagers. Cette ordonnance introduit le Référentiel Général de Sécurité (article 9) qui fixe les règles auxquelles les SI mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées. Les règles techniques et fonctionnelles imposées par ce référentiel modifient la gouvernance des SI au sein des autorités administratives notamment lors de la conception des nouveaux projets mais également lors du maintien en condition opérationnelle des systèmes numériques opérationnels. Cette formation vise à fournir tous les éléments juridiques, fonctionnels et techniques permettant d'intégrer les nouvelles exigences du RGS dans les processus opérationnels (métiers et informatique) et de définir les procédures adaptées au déploiement des mesures de sécurité.

OBJECTIFS

- **Comprendre comment appliquer les directives de protection des données à caractère personnel (Loi "Informatique et Libertés") dans le cadre de la mise en œuvre d'un téléservice**
- **Savoir mettre en œuvre la démarche permettant d'appliquer la sécurité des SI durant tout le cycle de vie d'un projet informatique (en conformité avec les principes énoncés dans le guide GISSIP de l'ANSSI)**
- **Connaître et savoir appliquer les directives du RGS en matière d'homologation de la sécurité des systèmes d'information**
- **Être en mesure d'appliquer les directives techniques (certificat, horodatage, authentification....) définies dans la dernière version du RGS en vigueur**
- **Savoir conduire une démarche d'appréciation des risques et d'audit conforme aux directives du RGS**
- **Être capable de définir les objectifs et la politique de sécurité adaptés aux enjeux de l'autorité administrative**

Public

- Responsable de la Sécurité du Système d'Information (RSSI), DPO, chefs de projet, Directeur des Systèmes d'Information, responsables métiers en charge de la mise en œuvre des téléservices

Pré-requis

Aucun

Les + de cette formation

- Une approche méthodologique participative permettant des échanges entre participants et le formateur sur des retours d'expériences concrets.
- Le support de formation est utilisé pour présenter les éléments théoriques des exigences du RGS et les applications pratiques des directives.
- Des documents annexes illustrent les cas concrets abordés durant la formation.
- Les nombreux exemples concrétisent les modèles théoriques proposés. Toutes les démarches proposées ont été éprouvées et mise en œuvre dans des autorités administratives.

Programme

1 - Introduction
- Cadre juridique du RGS (ordonnance du 8 décembre 2005 et arrêtés d'application)
- Périmètre d'éligibilité au RGS (organismes concernés par le RGS, ...)
- Historique de la sécurité des systèmes d'information
- Principes généraux relatifs à la protection des données à caractère personnel (Informatique et Libertés)

2 - Les principes généraux du référentiel général de sécurité
- Démarche de mise en œuvre du RGS pour tous les nouveaux téléservices
- Mise en conformité des téléservices opérationnels avant la parution du RGS
- L'homologation de la sécurité des systèmes d'information
- Les prestataires de services de confiance (PSCO)
- Les produits de sécurité labellisés ou certifiés
- Les fonctions techniques de sécurité
- La prise en compte de la sécurité dans les démarches projets

3 - La mise en place d'une filière sécurité au sein de l'autorité administrative
- Les instances de décisions
- L'autorité d'homologation
- Les acteurs de la filière SSI (RSSI, CIL, Référents SSI, ...)
- Les rôles et responsabilités collectives et individuelles de tous les personnels de l'autorité administrative
- Exemple de modèle organisationnel
- Exemple de document décrivant les rôles et les responsabilités

4 - L'homologation de la sécurité
- Le rôle du chef de projet dans le processus d'homologation
- La création du dossier de sécurité d'un nouveau projet informatique
- La présentation du dossier de sécurité à l'autorité d'homologation

5 - L'appréciation des risques et la définition des objectifs de sécurité
- Présentation du guide méthodologique de la CNIL
- Présentation de la méthode EBIOS de l'ANSSI
- Appréciation des risques dans le cadre d'un téléservice
- Analyse de la maturité du SI – présentation du guide de maturité de l'ANSSI
- Étude de cas basé sur l'utilisation du logiciel SCORE Priv@vy

6 - L'audit de la sécurité des systèmes d'information
- Les catégories d'audit
- Les exigences relatives aux choix d'un prestataire d'audit
- Les métriques d'audit et la présentation des résultats
- Présentation du guide de l'auditeur de l'ANSSI

7 - La formalisation de la PSSI
- Les objectifs de la PSSI, son périmètre
- Les sujets à aborder dans le cadre de la politique de sécurité
- La structure document d'une politique de sécurité
- Les chartes à destination des personnels internes ou externes
- Exemple de directives de sécurité, de PSSI et de chartes

8 - La sensibilisation des personnels
- La démarche de sensibilisation
- Construire son plan de sensibilisation
- Exemple de support et d'outils de sensibilisation
- Le suivi de la sensibilisation

9 - La prise en compte de la SSI dans les nouveaux projets
- Présentation du guide GISSIP de l'ANSSI
- Les livrables de sécurité attendus à chaque étape d'un nouveau projet
- La formalisation d'un dossier de sécurité
- Exemple de création d'un dossier de sécurité en utilisant le logiciel SCORE Priv@cy

10 - Les fonctions techniques de sécurité informatique
- Les règles relatives à la cryptographie
- Les règles relatives à la protection des échanges électroniques
- Les règles relatives aux accusés d'enregistrement et aux accusés de réception

11 - Le plan de traitement des incidents et de reprise d'activité
- Principes généraux relatifs à la gestion des incidents
- Introduction à la mise en œuvre d'un PCA / PRA (basé sur la norme ISO 22301)
- Procédures d'alertes et de gestion d'un cyber-crise on

12 - La maintenance et le suivi de la sécurité des systèmes d'information
- La mise en place d'une démarche d'amélioration continue basée sur la norme ISO 27001
- La veille technique et juridique de la sécurité des systèmes d'information
- Les tableaux de bord de suivi de la sécurité des systèmes d'information

Réf. **MG822**
2 jours
(14h présentiel)

ORGANISÉ SUR DEMANDE, NOUS CONSULTER

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

RGPD - Sensibilisation aux nouvelles règles relatives à la protection des données

Impacts organisationnels du nouveau règlement Européen

SÉMINAIRE S — ACCESSIBLE À DISTANCE — FORMATION MIXTE

Le règlement n° 2016/679, dit règlement général sur la protection des données (RGPD / GDPR), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Il introduit de nouveaux droits pour les individus et de nouvelles obligations pour les entreprises dont les modalités de mise en œuvre doivent être appliquées. Ce séminaire permet de faire le point sur les impacts du règlement européen pour l'entreprise et de proposer un plan de mise en conformité type.

OBJECTIFS

- Connaître les évolutions réglementaires imposées par le RGPD
- Mesurer les impacts du RGPD sur les aspects organisationnels et sur les procédures internes
- Savoir préparer un plan d'actions de mise en conformité

Public

- Dirigeants, responsables juridiques et juristes, responsables informatiques, DSI, RSSI, responsables conformité, responsables RH
- Toute personne concernée par le traitement des données personnelles ou la mise en conformité des traitements au sein de son organisme

Pré-requis

Aucun

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €). L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de ce séminaire

- L'intervenant de ce séminaire est également consultant et propose une approche très pragmatique du sujet.
- La méthode participative favorise les échanges entre les participants et l'intervenant qui illustre ses propos de nombreux exemples concrets.
- Support de cours remis sur clé USB.

Réf. **MG818**
2 jours
(14h présentiel)

1 810 €HT
Offerte

À DISTANCE	22/09, 07/11
PARIS	22/09, 07/11
AIX-EN-PROVENCE	17/11
BORDEAUX	08/09
LILLE	01/09
LYON	24/11
NANTES	15/09
RENNES	15/09
ROUEN	07/11
SOPHIA-ANTIPOLIS	17/11
STRASBOURG	01/09
TOULOUSE	01/09

Programme

1 En présentiel

1ÈRE partie : connaître les nouveautés apportées par le règlement

1 - Introduction
- Les enjeux du nouveau règlement européen et les objectifs recherchés
- Les définitions relatives aux données, aux fichiers et aux traitements
- Les définitions relatives aux acteurs impliqués dans les traitements (responsable de traitement, tiers, sous-traitant, destinataire, personne concernée, ...)
- Les nouvelles définitions introduites par le règlement européen (violation de données, profilage, limitation de traitement, portabilité, ...)

2 - Les nouvelles règles de gestion imposées par le règlement
- Transparence concernant les traitements de données à caractère personnel
- La simplification des démarches administratives auprès de l'autorité de contrôle
- Les nouvelles sanctions imposées par le règlement
- La gouvernance européenne en matière de protection des données (comité européen, guichet unique, rôle des autorités de contrôle, ...)

3 - Les obligations du responsable de traitement et du sous-traitant
- Les nouvelles obligations imposées au responsable de traitement (preuve du respect du règlement, sécurité des données, PIA, Privacy by Design, notification de violation de données,...)
- Les nouvelles obligations imposées au sous-traitant et les clauses contractuelles à intégrer dans les contrats
- Les actions à mener par l'entreprise pour se mettre en conformité

4 - Les droits des personnes concernées
- Les nouveaux droits des personnes concernées et les évolutions des droits existants concernant le traitement de leurs données
- Les nouveaux doits de recours des personnes concernées

5 - Le délégué à la protection des données
- Son rôle, ses responsabilités et ses missions
- Sa désignation et son positionnement
- Les contrôles de conformité au règlement

6 - Les transferts de données à caractère personnel en dehors de l'UE

2ÈME partie : Prévoir un plan d'actions pour se mettre en conformité

1 - Introduction
- Descriptions des actions à prévoir pour se mettre en conformité
- La démarche méthodologique pour mettre en œuvre le plan d'actions de mise en conformité
- Les étapes du plan d'actions à prévoir pour se mettre en conformité

2 - Organisation et référentiel
- La sensibilisation de la direction générale
- La nomination d'un chef de projet ou DPO
- L'organisation d'un comité de pilotage, arbitrage, suivi et validation
- La définition et la communication des politiques protection de la vie privée (interne et externe) et sécurité des données à caractère personnel, déclinaison dans la PSSI
- Les articulations avec les autres filières, (SSI, protection des installations, conservation des documents, ...)
- La modification des contrats
- La sensibilisation de l'encadrement et des collaborateurs
- La cartographie des traitements de données à caractère personnel
- La constitution du registre
- Les procédures de respect des obligations liées au consentement et aux devoirs d'informations
- Les procédures de gestion des demandes d'accès, rectification, limitation, portabilité, et destruction des données à caractère personnel
- La définition des niveaux de dommages sur la vie privée et la notification de violation de données à caractère personnel
- La formalisation des points de contacts

3 - Les transferts de données à caractère personnel en dehors de l'UE
- Les pays adéquats
- Les garanties, les contrats, les règles d'entreprise contraignantes
- Les dérogations

4 - Sécurité
- Security by default : contrôle d'accès, identification, authentification, habilitation ; protection des échanges et des supports de données à caractère personnel
- Security by design et méthodologie PIA : les acteurs, les étapes, la validation, les outils
- Le cas de l'externalisation : les PAS

5 - La gestion de la preuve
- Le contrôle
- La labellisation
- Les agréments
- La certification
- Les outils

3 Après le présentiel

Retrouvez sur le Learning Hub ib :
- Des vidéocasts pour revenir sur les points clés de la formation

RGPD - Devenir délégué à la protection des données (DPO/DPO)

ACCESSIBLE À DISTANCE

Formation de 35 h préparant à l'examen de certification du DPO AFNOR/CNIL

Le Délégué à la Protection des Données (DPD / DPO) est chargé, en toute indépendance, de conseiller et d'assister le responsable des traitements à garantir la conformité de l'organisme avec la règlementation sur la protection des données à caractère personnel. Il doit posséder des connaissances afin de s'assurer que les traitements de données respectent les exigences, notamment en ce qui concerne la vie privée des personnes concernées.
Cette formation a pour objectif de fournir aux participants, le socle de connaissances théoriques nécessaires pour passer l'examen de certification validé par la CNIL. Aussi, par une approche résolument pratique et alignée sur les problèmes concrets auxquels un DPO est confronté, cette formation a vocation à leur fournir les éléments indispensables pour mener à bien leur nouvelle mission. Pour valider ses compétences, le stagiaire peut, s'il le souhaite, s'inscrire à l'examen de certification du DPO AFNOR, seul organisme de certification agréé par la CNIL.

OBJECTIFS

- Acquérir les connaissances indispensables à l'accomplissement de la mission de DPO
- Connaître les bonnes pratiques pour mettre en place un processus de mise en conformité
- Acquérir les connaissances et la pratique pour jouer un rôle de conseil sur tout nouveau projet de traitement
- Savoir mettre en place les outils de communication et de sensibilisation
- Connaitre les points essentiels de contrôle
- Répondre à l'exigence de 35h de formation (en plus d'une expérience professionnelle de 2 ans tous domaines au minimum) pour passer la certification des compétences du DPO AFNOR agréé par la CNIL

Public

- DPO désigné ou en cours de désignation, relais ou référents protection des données
- Toute personne dont la mission est d'assurer le respect de la protection des données personnelles au sein de son organisation publique ou privée

Pré-requis

Avoir des connaissances de base sur le RGPD et la loi Informatique et Libertés modifiée ou avoir suivi la formation "RGPD - Sensibilisation aux nouvelles règles relatives à la protection des données" (MG818)

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €). L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de cette formation

- Cette formation et son contenu répondent à l'exigence de 35h de formation (en plus d'une expérience professionnelle de 2 ans tous domaines au minimum) pour passer la certification des compétences du DPO. Il revient au stagiaire de s'inscrire auprès des organismes agréés par la CNIL (AFNOR et autres organismes en cours de certification).
- La formation alterne entre présentation de fondamentaux théoriques et études de cas.
- Le formateur, qui a accompagné les DPO d'organismes privés ou publics, apporte son expérience en s'appuyant sur des exemples concrets.
- Support de cours remis sur clé USB.

Programme

1 - Rappels juridiques, responsabilités civiles et pénales

2 - Définitions
- Introduction et rappel historique
- Définitions
- Champ d'application matériel
- Champ d'application géographique
- Formalités préalables à la mise en œuvre des traitements
- Les responsabilités du Responsable de Traitement et du Sous-Traitant
- Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing
- Les droits et obligations propres aux traitements dans le secteur des communications
- Les dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées

3 - Le rôle du DPO
- Les conditions obligatoires de nomination du DPO
- L'expertise et les compétences attendues du DPO
- Les fonctions et missions du DPO
- Rôle du DPO dans les analyses d'impact relatives à la protection des données
- Rôle du DPO dans la constitution du registre
- Les relations entre la CNIL et le DPO
- Les conditions et la procédure relative à la fin de mission du DPO

4 - Les principes fondamentaux relatifs aux traitements de données à caractère personnel
- Introduction – Les principes fondamentaux précisés dans les textes
- Le principe de licéité et de loyauté des traitements / consentement
- Le principe de finalité
- Le principe de pertinence et d'adéquation des données à la finalité poursuivie
- Le principe de conservation limitée des données
- Le principe de sécurité et de confidentialité des données
- Le cas particulier des données sensibles / particulières / exemples
- Les droits des personnes concernées

5 - L'encadrement des transferts de données à caractère personnel hors de l'Union Européenne
- Les principes relatifs aux transferts de données hors de l'Union Européenne
- Les différents moyens destinés à encadrer le transfert de données de caractère personnel en dehors de l'Union Européenne
- Les formalités préalables applicables au transfert de données à caractère personnel en dehors de l'Union Européenne
- Les obligations de responsable traitement concernant l'information des personnes concernées par le transfert des données hors Union Européenne
- Le cas particulier du transfert des données vers les États-Unis

6 - Codes de conduite et certification
- Les labels
- Les codes de conduite
- Les certifications

7 - Les exigences relatives à l'encadrement des traitements dans le domaine de la santé
- Principes et définitions
- Le régime de formalités préalables applicables aux traitements ayant pour objet la recherche, l'étude ou l'évaluation
- Le dossier à présenter à la CNIL
- Les conditions de mise en œuvre des traitements de recherche, étude ou évaluation
- Les méthodologies de référence
- Les droits des personnes qui participent à une recherche ou une évaluation
- Les dérogations
- Les conditions de sécurité
- L'externalisation des données de santé

8 - Présentation de la CNIL et de ses missions
- Introduction et quelques chiffres clés
- Le statut de la CNIL
- La composition de la CNIL
- L'organisation de la Commission plénière et restreinte
- Les pouvoirs de contrôle de la CNIL
- Assistance mutuelle et opérations conjointes des Autorités de Contrôle
- Procédure d'urgence
- Les différentes missions de la CNIL

9 - Présentation des dispositions réglementaires associées au non-respect de la LIL et du RGPD
- Rappels
- Les sanctions pénales
- Les amendes administratives

10 - La formalisation du plan d'actions
- Recommandation pour l'élaboration d'un plan d'actions

Réf. MG805
5 jours (3+2)
(35h présentiel)

3 060 € HT
Offerte

À DISTANCE
26/09 & 10/10, 21/11 & 05/12
PARIS
26/09 & 10/10, 21/11 & 05/12

Autres sites, nous consulter

RGPD - Délégué à la protection des données : missions, rôle et obligations

Devenir DPO

CERTIFIANT

ACCESSIBLE À DISTANCE

La formation Délégué à la Protection des Données fournit les connaissances, aptitudes et compétences nécessaires pour mettre en œuvre et gérer efficacement un cadre de conformité en matière de protection des données personnelles. Après avoir maîtrisé l'ensemble des concepts relatifs au règlement général sur la protection des données (RGPD) et avoir appréhendé les spécificités de la mission du DPO/DPD, les participants pourront se présenter à l'examen et postuler au titre de "PECB Certified Data Protection Officer" (DPO). L'obtention de la certification attestera de la capacité à identifier précisément l'écart entre le règlement général sur la protection des données et les processus organisationnels d'une entreprise (politiques de confidentialité, procédures, instructions de travail, formulaires de consentement, ...) et à accompagner sa mise en conformité au RGPD.

OBJECTIFS

- Connaître l'histoire de la protection des données personnelles en Europe
- Comprendre les concepts et approches nécessaires à l'alignement efficace avec le règlement général sur la protection des données
- Comprendre les nouvelles exigences que le RGPD impose aux organisations de l'UE et aux organisations non-UE savoir quand les mettre en œuvre
- Acquérir l'expertise nécessaire pour aider un organisme à évaluer la mise en œuvre de ces nouvelles exigences et le conseiller sur la gestion des données personnelles
- Savoir gérer une équipe implémentant le RGPD
- Acquérir l'expertise nécessaire pour prendre des décisions dans le contexte de la protection des données personnelles

Public

- Correspondant "Informatique et libertés", DPO désigné ou en cours de désignation
- Toute personne dont la mission est d'assurer le respect de la protection des données personnelles au sein de son organisation

Pré-requis

Une compréhension fondamentale du RGPD et des connaissances de base sur les exigences légales actuelles en matière de protection des données ou avoir suivi la formation "RGPD - Sensibilisation aux nouvelles règles relatives à la protection des données" (MG818)

Certification

Cette formation prépare au test PECB Certified Data Protection Officer Exam qui permet d'obtenir la certification PECB Certified Data Protection Officer.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cette formation dispensée par un instructeur certifié est basée sur le règlement et les meilleures pratiques.
- Les apports théoriques sont illustrés par des exemples, des exercices pratiques, des jeux de rôle et des discussions basés sur des études de cas.
- Un programme étudié pour permettre aux participants de préparer le passage de la certification dans les meilleures conditions. Les tests pratiques sont similaires à ceux proposés lors de l'examen.

Programme

1 - Introduction au GDPR et initialisation de conformité réglementaire
- Objectifs et structure du cours
- Introduction au General Data Protection Regulation (GDPR)
- Principes fondamentaux du GDPR
- Initialisation de la mise en œuvre du GDPR
- Comprendre l'organisation et clarifier les objectifs de la protection des données
- Analyse du système existant

2 - Planification de la mise en œuvre du GDPR
- Leadership et approbation du projet de conformité GDPR
- Politique de protection des données
- Définition de la structure organisationnelle de la protection des données
- Classification des données
- Évaluation du risque associé au GDPR

3 - Déploiement du GDPR
- PIA, Privacy Impact Assesment
- Conception des contrôles de sécurité, des procédures et politiques spécifiques
- Définition du processus de gestion de la documentation
- Plan de communication
- Plan de formation et de sensibilisation

4 - Suivi et amélioration continue de la conformité au GDPR
- Gestion des opérations
- Gestion des incidents
- Monitoring, mesure, analyse et évaluation
- Audits internes
- Brèche de données et actions correctives

5 - Passage de l'examen de certification "PECB Certified Data Protection Officer" (en ligne après la formation)
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Toutes les étapes sont détaillées sur https://pecb.com/help/wp-content/uploads/2018/07/Guide-de-préparation-a-l'examen-en-ligne-de-PECB.pdf
- Passage de l'examen de certification en français en 3 heures
- Un score minimum de 70% est exigé pour réussir l'examen
- Les candidats sont autorisés à utiliser les supports de cours et les notes qu'ils auront prises lors de la formation
- En cas d'échec ils bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- L'examen couvre les domaines de compétences suivants:
  - Domaine 1: Concepts de protection des données et exercice des droits par la personne concernée
  - Domaine 2: Le responsable du traitement des données, le sous-traitant, et le Délégué à la protection des données
  - Domaine 3: Planification du projet de conformité GDPR
  - Domaine 4: Analyse d'impact relative à la protection des données et étude d'impact sur la vie privée
  - Domaine 5: Mesures et approches de la protection des données
  - Domaine 6: Évaluation des performances, suivi et mesure du projet de conformité RGPD

Réf. **MG826**
4,5 jours
(31,5h présentiel)

3 650 €HT
Offerte

À DISTANCE	BORDEAUX	NANTES	SOPHIA ANTIPOLIS
13/06, 05/09, 24/10, 12/12	10/10	24/10	19/09
PARIS	**LILLE**	**RENNES**	**STRASBOURG**
13/06, 05/09, 24/10, 12/12	24/10	24/10	05/09
AIX-EN-PROVENCE	**LYON**	**ROUEN**	**TOULOUSE**
19/09	10/10	07/06, 19/12	30/05, 19/09

RGPD - Préparer la certification DPO AFNOR

Certifiez vos compétences de DPO

ACCESSIBLE À DISTANCE

Depuis le 25 mai 2018, la désignation d'un DPO (Data Protection Officer) est obligatoire pour les organisations publiques et privées qui sont amenées à traiter des données sensibles à grande échelle. Acteur clé de la conformité au RGPD, le DPO (ou DPD) doit disposer de connaissances spécialisées du droit et des pratiques en matière de protection des données. L'AFNOR est le 1er organisme agréé par la CNIL pour certifier les compétences des ou DPO. Le certificat constitue un vecteur de confiance à la fois pour l'organisme faisant appel à ces personnes certifiées mais également pour ses clients, fournisseurs, salariés ou agents. Dans le cadre de cette journée de préparation à la certification, vous pourrez évaluer vos connaissances sur la base d'un QCM de 100 questions conçu par des experts selon les exigences de la CNIL. La correction en séance du quizz constitue en outre une excellente révision dans la perspective de l'examen.

OBJECTIFS

- Se mettre en conditions réelles de passer l'examen de certification AFNOR
- Se préparer aux typologies de questions
- Savoir organiser son programme de révision afin de se donner toutes les chances de réussir l'examen de certification
- Passer l'examen à blanc

Public

- DPO, référents protection des données personnelles en fonction ou ayant suivi une formation (ou plusieurs formations) pour un total de 35 heures.
- A noter, il n'est pas exigé d'être désigné en tant que délégué pour être candidat à la certification des compétences du DPO.

Pré-requis

Justifier d'une expérience professionnelle d'au moins 2 ans
ET avoir suivi une formation de 35 h en matière de protection des données personnelles reçue par un organisme de formation
Ou justifier d'une expérience professionnelle d'au moins 2 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles
Avoir une bonne connaissance du RGPD et ses considérants

Certification

Cette formation prépare à la certification DPO AFNOR (en option au tarif de 800 €).

Les + de cette formation

- Cette formation est animée par un formateur certifié DPO par l'AFNOR (organisme agréé par la CNIL)
- Les participants passent un examen blanc durant la formation
- Le participant s'inscrit à la date choisie à l'issue de sa formation (sessions toutes les semaines dans les locaux d'AFNOR à Saint Denis).
- Support de cours remis sur clé USB.

Programme

1 - Introduction
- Déroulement de l'examen
- Les conditions d'obtention de la certification

2 - Le contenu de l'évaluation
- Étude des compétences et des savoir-faire évalués dans la délibération n°2018-318 du 20 septembre 2018
- Thèmes fondamentaux
- Étude de la typologie et la tournure des questions

3 - Examen blanc
- Quizz de 100 questions inspirée de l'examen en vigueur

4 - Corrections du quizz et explications
- Reprise du Quizz avec la correction instantanée, question par question

5 - Échanges sur les thèmes problématiques et questions supplémentaires
- Discussion sur les questions dites "pratiques" et partage d'expériences
- Salves de questions corrigées

6 - Conclusion

Réf. MG838
1 jour
(7h présentiel)

970 € HT
Offerte

À DISTANCE Autres sites, nous consulter
09/06, 12/10, 07/12
PARIS
09/06, 12/10, 07/12

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

RGPD - Le rôle de la DSI dans la mise en conformité

Rôles et responsabilités des acteurs de la DSI

ACCESSIBLE À DISTANCE

Dans un environnement ultra-concurrentiel et en constante transformation, où les entreprises sont de plus en plus exposées aux risques opérationnels et juridiques, une meilleure appréhension des dispositifs de sécurité à mettre en place pour protéger la vie privée des personnes concernées fournira un avantage compétitif majeur. Les organismes doivent mettre en cohérence la gouvernance de la protection de l'information et de la protection de la vie privée. Les exigences SI et SSI de protection de la vie privée entrainent une adaptation des méthodes de concertation entre la DSI, la SSI et la protection de la vie privée. Dans tous les cas, le chef d'entreprise ou le DPO devront s'appuyer sur la DSI et le RSSI quand il est nommé. Ceux-ci seront particulièrement sollicités pour documenter et mettre en place les démarches de protection, afin d'assurer la partie de preuve qu'il incombe au maitre d'œuvre, de la preuve de la conformité, la disponibilité, l'intégrité, la confidentialité et la traçabilité des traitements de données personnelles. Cette formation permettra aux acteurs de la DSI de mieux appréhender la protection de la vie privée et la sécurité des données à caractère personnel, améliorer le dialogue avec le DPO, les directions métiers et la fonction juridique.

OBJECTIFS

- Être capable de sensibiliser et former les équipes de la DSI à la protection des données à caractère personnel
- Savoir définir les responsabilités : responsable de traitement et du sous-traitant
- Savoir définir la gouvernance à mettre en place dans le cas d'une externalisation des données à caractère personnel
- Pouvoir initier les acteurs de la DSI aux analyses d'impact relatives à la protection des données (AIPD) et au Privacy by Design (intégration de la protection des données dans les projets)
- Être en mesure de définir un programme d'audit et de pilotage de la sécurité

Public

- DSI, RSSI, chefs de projet et directions métiers, DPO

Pré-requis

Notions sur la protection des données personnelles

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €). L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de cette formation

- Ce programme vise à expliquer les principes fondamentaux de prise en compte de la protection de la vie privée et de la mise en conformité au RGPD auprès des acteurs de la DSI.
- Cette formation est animée par un formateur expérimenté ayant mis en conformité plusieurs organismes publics et privés.
- Il apportera son expérience en s'appuyant sur des exemples concrets.

Programme

1 - Présentation de la loi informatique et libertés en complément du RGPD
- Principes
- Augmentation des droits des personnes concernées
- Renforcement des obligations de sécurité
- Augmentation des responsabilités du responsable de traitement et du sous-traitant
- Obligation de preuve / Accountability
- Définitions des notions clés
- Les acteurs : responsable de traitement, sous-traitant, destinataire, personne concernée, tiers autorisé

2 - Les responsabilités du responsable de traitement et du sous-traitant
- La logique de formalités préalables laisse la place à celle de responsabilisation des acteurs : mettre en place un registre des traitements, veiller à encadrer l'information des personnes concernées, formaliser les rôles et responsabilités du responsable de traitement et du sous-traitant, nommer un DPO, mener des AIPD, encadrer les contrats avec les prestataires, sécuriser

3 - La gouvernance à mettre en place pour l'externalisation des données
- La voie hiérarchique et les voies fonctionnelles SSI et vie privée : le COPIL, le RSSI, le DPO, la DSI, le sous-traitant hébergeur et les directions métiers déléguées par le responsable des traitements
- Proposition d'une table RACI
- Formalisation du référentiel SSI et vie privée : lettre d'engagement, PGPI, politique de protection de la vie privée à usage interne, politique de protection de la vie privée à usage externe, PSSI et référentiels PGSSI S ou PSSI MCAS, Plan d'Assurance Sécurité à annexer au contrat, guides et procédures, chartes, tableaux de bords et guide d'audit

4 - Les AIPD à réaliser
- Liste des types d'opérations de traitement de données de santé pour lesquelles une AIPD est requise
- Les étapes
- La rédaction du rapport PIA

5 - L'intégration de la vie privée en complément de la SSI par défaut
- Les bonnes pratiques

6 - L'intégration de la vie privée en complément de la SSI dans les projets dès la conception
- L'approche en V
- L'approche Agile

7 - Les audits
- Conformité, organisationnel, architecture, code, ...
- Efficacité
- Performance

8 - Les tableaux de bords
- Stratégique
- Pilotage
- Opérationnel

9 - Conclusion

Réf. **MG833**
2 jours
(14h présentiel)

1 930 €HT
Offerte

À DISTANCE
30/06, 02/11
PARIS
30/06, 02/11

Autres sites, nous consulter

RGPD - Auditer sa conformité et se préparer à un contrôle de la CNIL

Anticiper et réduire les risques en cas de contrôle de la CNIL

ACCESSIBLE À DISTANCE

Le nouveau règlement européen (GDPR) introduit l'obligation pour le responsable de traitement de démontrer le respect au règlement européen et au délégué à la protection des données (DPO) de réaliser une mission de contrôle. En outre, il confirme les autorités compétentes dans leur rôle de contrôle et l'application de sanctions administratives. Cette formation vise à présenter la démarche à adopter pour auditer la conformité au RGPD en interne et se préparer efficacement à un contrôle de la CNIL.

OBJECTIFS

- **Être capable de définir la démarche à entreprendre dans le cadre d'un contrôle de conformité organisationnel au GDPR**
- **Comprendre comment dérouler un audit de contrôle organisationnel au GDPR**
- **Se préparer à un contrôle de la CNIL**

Public

- Auditeurs, DPO et DPD, dirigeants, responsables juridiques

Pré-requis

Avoir une bonne connaissance du RGPD de la loi Informatique et Libertés modifiée

Les + de cette formation

- Une approche méthodologique participative permettant des échanges entre participants et le formateur sur des retours d'expériences concrets.
- La démarche d'audit proposée a été utilisée dans des cas réels d'entreprise.
- L'expérience du formateur lui permet de s'appuyer sur des exemples concrets facilitant les retours d'expérience.

Programme

1 - Rappel synthétique du contexte réglementaire et des notions fondamentales de la protection des données à caractère personnel

- Enjeux, concepts, définitions, acteurs, responsabilités, personnes concernées, mesures de sécurité, AIPD, Privacy by design, notification d'une violation de données, le principe d'accountability

2 - Les acteurs du contrôle : rôle essentiel du DPO dans l'analyse de conformité

- Rôle, missions et positionnement du DPO
- Les autres acteurs
- Les acteurs et les niveaux de contrôle

3 - Les niveaux de maturité et de conformité effectifs

- Les instruments de mesure

4 - Réaliser un audit de conformité

- Organisation de l'audit
- Les référentiels d'audit
- Les outils de l'audit

5 - Les contrôles de la CNIL

- Pouvoir de sanction
- Pourquoi mon organisme est-il contrôlé par la CNIL ?
- Quels sont les types de contrôles opérés par la CNIL?
- Comment anticiper un contrôle de la CNIL?
- Comment gérer un contrôle CNIL ?
- Quelles actions mettre en place à la suite d'un contrôle CNIL ?
- Quelles sont les suites que la CNIL peut donner à un contrôle ?

6 - Un exemple de rapport d'audit flash RGPD

7 - Annexe : Rappel détaillé des principes de la protection de la vie privée

Réf. MG823
1 jour
(7h présentiel)

970 €HT
Offerte

À DISTANCE
17/06, 21/10
PARIS
17/06, 21/10

Autres sites, nous consulter

L'aide au recrutement avec la POE (Préparation Opérationnelle à l'Emploi)

Vous rencontrez des difficultés pour recruter des collaborateurs dont les profils et les compétences sont en adéquation avec vos besoins ?

ib vous propose un dispositif complet qui répond précisément à cette problématique. En associant pré-recrutement et formation préalable à l'embauche, ib vous propose une solution clé en main qui vous permettra d'intégrer des collaborateurs immédiatement opérationnels sur des métiers en tension.

A travers notre dispositif qui associe aux avantages liés à la POEI des services à forte valeur ajoutée, nous apportons une réponse efficace aux problèmes de pénuries de compétences et d'employabilité auxquels sont aujourd'hui confrontées les entreprises.

Pour en savoir plus, contactez-nous au 0 825 07 6000

RGPD - Réaliser une analyse d'impact sur la vie privée (AIPD/PIA)

ACCESSIBLE À DISTANCE

Mener une analyse d'impact sur la protection des données personnelles

L'analyse d'impact relative à la protection des données et à la vie privée (AIPD) ou Privacy Impact Assessment (PIA) est un instrument incontournable de la protection des données. Elle est la pierre angulaire de la mise en œuvre du principe de prise en compte des risques d'atteinte à la vie privée dès la conception d'une application ou d'un traitement de données ("privacy by design", selon l'article 23 du règlement européen). Cette formation de 2 jours vise à expliquer, au travers d'un cas pratique, comment mener à bien les différentes étapes de réalisation d'un PIA au sein de son organisation.

OBJECTIFS

- Comprendre et assimiler la démarche AIPD/PIA
- Savoir identifier les traitements nécessitant un PIA
- Être capable d'accompagner et de documenter la décision de mise en œuvre d'un traitement de donnée à caractère personnel
- Être en mesure de dérouler une analyse d'impact sur la vie privée

Public

- DPO, RSSI, référents protection des données personnelles, juristes, DSI, chefs de projet, développeurs

Pré-requis

Avoir suivi la formation "RGPD - Sensibilisation aux nouvelles règles relatives à la protection des données" (MG818) ou la formation "RGPD - Devenir délégué à la protection des données (DPD/DPO)" (MG805) ou disposer des connaissances de base en matière de protection des données personnelles

Certification

Cette formation prépare à la certification DiGiTT (en option au tarif de 115 €) . L'examen se déroule en ligne en français et dure environ 90 minutes.

Les + de cette formation

- La formation est animée par un formateur expérimenté ayant mis en application la démarche AIPD dans plusieurs organismes publics et privés. Il apportera son expérience en s'appuyant sur des exemples concrets.
- Une étude de cas complète permet aux participants de mettre immédiatement en pratique leurs nouveaux acquis et d'acquérir une première expérience de la conduite d'une analyse d'impact sur la vie privée.

Programme

1ÈRE partie : présentation de la démarche AIPD / PIA

1 - Introduction

- Rappel du contexte réglementaire
- Rappel des obligations du responsable des traitements
- Présentation des traitements nécessitant un PIA
- Présentation des objectifs et des enjeux d'une démarche PIA
- Le management du risque : principes et lignes directrices

2 - La démarche PIA proposée par la CNIL

- La démarche méthodologique proposée par la CNIL
- Les rôles et les responsabilités dans la réalisation d'un PIA
- Présentation des phases de la démarche PIA
- Présentation des guides et outillage proposés par la CNIL

2ÈME partie : exercices pratiques de mise en œuvre de la méthode

- Exercice 1 : Description du contexte et du périmètre du traitement retenu dans l'étude de cas
- Exercice 2 : Description des mesures de nature juridique et de sécurité mises en œuvre
- Exercice 3 : Description des risques pesant sur la vie privée des personnes concernées
- Exercice 4 : Décision de l'acceptabilité des résultats du PIA
- Exercice 5 : Rédaction du rapport de PIA

3ÈME partie : conclusion

- Retour d'expérience sur le cas pratique : les points forts et les points faibles de la méthode de la CNIL
- Impact de la mise en œuvre de la méthode au sein de l'entreprise
- Axe d'amélioration / d'optimisation de la méthode et des référentiels

Réf. MG832
2 jours
(14h présentiel)

1 870 €HT
Offerte

À DISTANCE
09/06, 29/09
PARIS
09/06, 29/09

Autres sites, nous consulter

Les implantations

En mettant à votre disposition des équipes commerciales dans chacune de nos agences, nous vous apportons la garantie d'une vraie relation de proximité. Quel que soit votre besoin, vous bénéficiez de l'accompagnement d'experts géographiquement et culturellement proches de vous :

PARIS	LILLE	RENNES	STRASBOURG
AIX-EN-PROVENCE	LYON	ROUEN	TOULOUSE
BORDEAUX	NANTES	SOPHIA-ANTIPOLIS	

RGPD - Répondre à une demande d'exercice des droits des personnes concernées

Tout mettre en œuvre pour appliquer le règlement

ACCESSIBLE À DISTANCE

Le RGPD et la loi informatique et libertés modifiée mettent au centre de la règlementation les personnes concernées. Ainsi, l'article 1er de la loi informatique et libertés modifiée dispose que "toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant". L'article 84 du RGPD prévoit quant à lui qu'une non-conformité en matière de droits des personnes concernées peut être sanctionnée à un niveau le plus élevé (amende administrative pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4% du CA annuel mondial total). Cette formation permettra au participant de comprendre les droits des personnes concernées, d'en connaitre les limites et de mettre en place une organisation interne afin d'être capable de répondre dans les délais et formes imposés par le RGPD et la loi Informatique et Libertés modifiée.

OBJECTIFS

- Connaître les droits des personnes concernées
- Pouvoir comprendre les conditions de recevabilité et les limites des droits des personnes
- Être capable de mettre en place une organisation interne permettant de s'assurer du traitement efficace des demandes d'exercice de droits
- Savoir répondre à une demande d'exercice de droits à travers des cas pratiques

Public

- DPO
- Service Qualité
- Service Juridique
- Direction Générale
- DSI

Pré-requis

Connaissance du RGPD
Avoir suivi une formation DPO

Les + de cette formation

- Cette formation vise à expliquer, au travers de cas pratiques de quelle manière répondre à une demande d'exercice des droits des personnes concernées afin mettre en place un process interne conforme à la réglementation en vigueur.
- Cette formation est animée par un formateur expérimenté ayant mis en place ce process dans plusieurs organismes publics et privés. Il apportera son expérience en s'appuyant sur des exemples concrets.
- Support de cours remis sur clé USB.

Programme

1ère partie : Introduction - Rappel du contexte réglementaire

2ème partie : définition et objets des droits des personnes concernées

1 - L'information des PC (articles 13 et 14 RGPD)

2 - Le droit d'accès et communication des données (article 15 RGPD)
- Définition
- Droit d'accès direct et indirect
- Cas particulier de l'accès au dossier médical

3 - Le droit de rectification (article 16 RGPD)

4 - Le droit à l'effacement ou droit à l'oubli (article 17 RGPD)
- Définition
- Cas particulier du déférencement d'un moteur de recherche

5 - Le droit à la limitation du traitement (article 18 RGPD)

6 - Le droit à la portabilité (article 20 RGPD)

7 - Le droit d'opposition (article 21 RGPD)
- Définition
- Cas particulier du droit d'opposition à la prospection commerciale

8 - Profilage et décision automatisée (article 22 RGPD)

3ème partie : Éléments structurants permettant de répondre à une demande d'exercice de droit

1 - Conditions de recevabilité d'une demande d'exercice de croits

2 - Limites aux droits des personnes concernées
- Respect des droits d'autrui
- Limites au droit d'accès
- Limites au droit d'effacement
- Limites au droit à la portabilité
- Limitations posées par l'article 23 du RGPD (fichiers de police, gendarmerie et renseignement)

3 - Forme et délais d'une réponse à une demande d'exercice de droits
- Parallélisme des formes de la demande et de la réponse à apporter à la personne concernée
- Mentions obligatoires
- Délais de réponse et conditions de prolongation du délai
- Principe de gratuité dans le traitement des demandes
- Principe de sécurité et de confidentialité dans le traitement des demandes

4 - Organisation et procédure à mettre en œuvre pour être capable de répondre à une demande d'exercices des droits
- Les acteurs internes
- Les procédures à mettre en œuvre

4ème partie : Conséquences d'un défaut de réponse à une demande d'exercice de droit

1 - Les droits de recours (article 77 et suivants RGPD)

2 - Le pouvoir de sanctions de la CNIL

5ème partie : Cas pratique

6ème partie : Conclusion de la formation et questions/réponses

Réf. MG834
1 jour
(7h présentiel)

970 €HT
Offerte

À DISTANCE
07/07, 04/11
PARIS
07/07, 04/11

Autres sites, nous consulter

Toutes nos formations en détail sur...

www.ib-formation.fr

Avis de l'expert, parcours pédagogiques, publics, dates, ...
tout ce qu'il faut savoir sur nos formations est sur notre site.
Découvrez également nos tests de pré-requis en ligne et nos conseils pour aller plus loin dans l'expertise.

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

RGPD - Conformité et sécurité des traitements de données de santé

Le cas particulier des données de santé

ACCESSIBLE À DISTANCE

Le RGPD encadre la collecte et le traitement des données à caractère personnel et notamment les données sensibles. L'encadrement de ces traitements dans le domaine de la santé a pour objet de protéger ces données, et cela dans la mesure où leur divulgation ou leur mauvaise utilisation est susceptible de porter atteinte aux droits et libertés des personnes. Le responsable de traitement doit donc veiller au respect des règles de protection des informations des personnes concernées. En cas de non-respect de ces règles, le responsable de traitement pourrait voir sa responsabilité pénale engagée.
Cette formation intègre les nouvelles mesures et directives de la nouvelle Loi Santé, de la CNIL, l'ASIP Santé et du Règlement Européen.

OBJECTIFS

- **Comprendre les exigences concernant les traitements de données de santé**
- **Acquérir les compétences juridiques, organisationnelles et techniques nécessaires pour mettre en conformité les traitements de données de santé**
- **Connaître les bonnes pratiques**

Public

- DPO du secteur de la santé et toute personne dont la mission est d'assurer le respect de la protection des données personnelles de santé au sein de son organisation (établissements de santé, hébergeurs de données de santé, professions paramédicales, assurances, ...)

Pré-requis

Avoir une bonne connaissance du RGPD de la loi Informatique et Libertés modifiée

Les + de cette formation

- La formation alterne entre présentation de fondamentaux théoriques et études de cas.
- Les échanges entre participants et l'expérience du formateur dans le secteur de la santé facilitent les retours d'expérience.

Programme

1 - Définitions, champ d'application et responsabilités
- Introduction et rappel historique
- Le RGPD vision synthétique
- Définitions dans le domaine de la santé
- Les formalités
- Les AIPD
- Le registre
- Synthèse

2 - La gouvernance
- Le DPO / DPD
- L'organisation l'articulation avec les autres acteurs
- Les référentiels
- La sous-traitance et les agréments HDS

3 - Les principes appliqués dans le domaine de la santé
- Introduction - Les principes fondamentaux précisés dans les textes
- Le principe de licéité et de loyauté des traitements / consentement
- Le principe de finalité
- Le principe de pertinence et d'adéquation des données à la finalité poursuivie
- Le principe de conservation limitée des données
- Le principe de sécurité et de confidentialité des données
- L'AIPD
- Les droits des personnes

3 - Les exigences relatives à l'encadrement des traitements ayant pour objet a recherche, l'étude ou l'évaluation
- Principes et définitions
- Le régime de formalités préalables applicables aux traitements ayant pour objet la recherche, l'étude ou l'évaluation
- Le dossier à présenter à la CNIL
- Les conditions de mise en œuvre des traitements de recherche, étude ou évaluation
- Les méthodologies de référence : MR-001, MR-002, MR-003, MR-004, MR-005 et MR-006
- Les droits des personnes qui participent à une recherche ou une évaluation
- Les dérogations

Réf. **MG839**
1 jour
(7h présentiel)

970 €HT
Offerte

À DISTANCE
30/09, 02/12
PARIS
30/09, 02/12

Autres sites, nous consulter

Privacy by Design - Prise en compte native de la protection des données dans les projets SI

Intégrer au plus tôt les principes du RGPD

ACCESSIBLE À DISTANCE

Le Privacy by Design est l'une des notions au cœur du RGPD. Pourtant, ce concept n'est pas une nouveauté : c'est une idée développée durant les années 1990 par la Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada) (Ann Cavoukian). Chaque nouvelle technologie traitant des données à caractère personnel ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation le plus haut niveau possible de protection des données. Cette idée a notamment été plébiscitée par une résolution de la 32ème conférence internationale des préposés à la protection des données les 27-29 octobre 2010, qui recommande aux Etats d'intégrer ce concept à leur législation. Ce concept, intégré au RGPD en son article 25, impose aux entreprises d'intégrer les principes du RGPD dès la conception d'un projet, d'un service ou de tout autre outil lié à la manipulation de données personnelles. Une prise en compte optimale de ces principes peut améliorer la réputation de la marque et la confiance des clients. Le concept de "Privacy by Design" est étroitement lié à celui de "Privacy by Default", selon lequel chaque entreprise traitant des données personnelles doit garantir par défaut le plus haut niveau possible de protection des données.

OBJECTIFS

- Comprendre le concept juridique du Privacy by Design
- Comprendre les impacts pratiques du Privacy by Design
- Appréhender concrètement le principe du Privacy by Design à travers un cas pratique

Public

- DPO, référents protection des données personnelles, RSSI, DSI, juristes, chefs de projet, développeurs, directions métiers

Pré-requis

Disposer des connaissances de base en matière de protection des données personnelles ou avoir suivi une des formations suivantes "RGPD - Sensibilisation aux nouvelles règles relatives à la protection des données" (MG818), "RGPD - Devenir délégué à la protection des données (DPD/DPO)" (MG805), "RGPD - Délégué à la protection des données : missions, rôle et obligations - Certification DPO incluse" (MG826)

Les + de cette formation

- Cette formation vise à expliquer, au travers de cas d'exercices pratiques, les principes fondamentaux de prise en compte de la protection de la vie privée dès la conception.
- Cette formation est animée par un formateur expérimenté ayant mis en application la démarche Privacy By Design dans plusieurs organismes publics et privés. Il apportera son expérience en s'appuyant sur des exemples concrets.

Programme

1 - Introduction : Rappel du contexte réglementaire et des notions fondamentales de la protection des données à caractère personnel

2 - Comprendre le concept juridique de Privacy by Design

- Le concept juridique du Privacy By Design
- Les avantages du Privacy By Design
- Privacy By Design et AIPD
- Le rôle essentiel du DPO dans la mise en œuvre du Privacy By Design
- Le Privacy By Design et la gouvernance du projet
- Le développement de la culture "Privacy"
- Les conséquences en cas de non-respect du Privacy By Design

3 - Comprendre les impacts pratiques du Privacy by Design

- Intégration des étapes du Privacy By Design dans la démarche projet
- Intégrer la sécurité numérique en démarche Agile
- Risques liés au déploiement d'un site Web
- La sécurité des données à caractère personnel
- Les principes essentiels en matière de SSI
- Les bonnes pratiques du développeur

4 - Appréhender concrètement le principe de Privacy by Design à travers un cas pratique

- Élaborer une grille d'analyse de conformité type
- Étude de cas

Réf. MG831
1 jour
(7h présentiel)

970 €HT
Offerte

À DISTANCE
08/07, 28/10
PARIS
08/07, 28/10

Autres sites, nous consulter

Le learning hub ib

Vous êtes inscrit à une formation mixte ib ?
Retrouvez sur le Learning Hub l'ensemble des activités digitales intégrées à votre parcours (quiz, vidéocasts, modules e-learning,...).

Avec le Learning Hub, confortez vos pré-requis grâce à des quiz pédagogiques, des vidéos ou des modules e-learning, testez vos acquis et approfondissez les sujets de votre choix avec nos quiz post-formation et nos vidéocasts. Consultez enfin nos vidéos-tutos pour bénéficier de l'accompagnement de nos experts dans la mise en œuvre de vos nouveaux savoirs.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Sécurité systèmes et réseaux - Les fondamentaux

Comprendre les concepts pour se protéger des attaques et garantir la fiabilité de vos données

ACCESSIBLE À DISTANCE

Avec Internet, les réseaux sont dorénavant ouverts et par conséquent, beaucoup plus exposés aux attaques virales ou autres actes de piratage. Il est donc devenu primordial de savoir faire face à ces différents risques pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information. Au cours de cette formation, les participants découvriront les principaux concepts liés à la sécurité des réseaux ainsi les outils permettant de protéger les infrastructures d'entreprise.

OBJECTIFS

- **Pouvoir évaluer les risques internes et externes liés à l'utilisation d'Internet**
- **Comprendre quels sont les mécanismes qui permettent de garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes**
- **Disposer d'une première approche des concepts techniques, pour comprendre la sécurité des systèmes d'information**

Public

- Responsables de l'informatique
- Administrateurs réseaux
- Techniciens
- Webmasters
- Responsables de la sécurité informatique

Pré-requis

Il est nécessaire d'avoir une bonne connaissance générale des réseaux et des systèmes d'exploitation courants

Les + de cette formation

- L'assimilation d'une méthodologie pour la mise en œuvre d'une sécurité performante des réseaux.
- Une formation rythmée par une pédagogie qui repose sur des exemples concrets.
- Les conseils de consultants experts en sécurité du SI.
- Les participants intéressés par une mise en pratique opérationnelle de la sécurité préfèreront la formation "Sécurité systèmes et réseaux - Mise en œuvre" (SR211).

Programme

1 - L'environnement
- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hackers, responsables sécurité, auditeurs, vendeurs et éditeurs)
- La veille technologique
- Les organismes officiels

2 - Les méthodes des attaquants
- Les scénarios d'attaques intrusion, DDOS, ...
- Les attaques sur les protocoles réseaux
- Les faiblesses des services : Web, VoIP, Messagerie
- Le code vandale : virus, vers et chevaux de Troie

3 - La sécurité des accès, firewall, WAF, Proxy, NAC
- L'accès des stations aux réseaux d'entreprise,802.1X, NAC
- Les différents types de firewalls
- Les règles de filtrage
- Les règles de la translation d'adresse (NAT)
- La mise en œuvre d'une zone démilitarisée (DMZ)
- La détection et surveillance avec les iDS
- L'intégration d'un firewall dans le réseau d'entreprise
- La gestion et l'analyse des fichiers log

4 - La sécurité des systèmes d'exploitation
- Le hardening de Windows
- Le hardening d'Unix/Linux
- Le hardening des nomades : IOS / Android

5 - La sécurité des applications avec exemple d'architectures
- Les serveurs et clients Web
- La messagerie électronique
- La VoIP IPbx et téléphones

6 - La sécurité des échanges, la cryptographie
- L'objectif du cryptage et fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap, chap, Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN réseau privé virtuel site à site et nomade

Réf. SR220
4 jours
(28h présentiel)

2 560 €HT
Offerte

À DISTANCE
05/09, 28/11
PARIS
05/09, 28/11

Autres sites, nous consulter

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Sécurité systèmes et réseaux - Mise en œuvre

Protéger efficacement matériel et données

ACCESSIBLE À DISTANCE

La protection des données de l'entreprise passe par une politique de sécurité capable de résister à toutes menaces extérieures. Loin d'être un domaine spécifique, la sécurité doit être prise en compte aussi bien pour les équipements réseaux que pour les systèmes. Même s'il n'est pas un expert, l'administrateur ne doit pas ignorer les risques encourus et doit être capable de mettre en œuvre une architecture de sécurité répondant aux exigences de l'entreprise.

OBJECTIFS

- Savoir concevoir et réaliser une architecture de sécurité adaptée
- Pouvoir mettre en œuvre les principaux moyens de sécurisation des réseaux
- Disposer d'une première approche sur la sécurisation des serveurs
- Découvrir en quoi la cryptographie est utile pour sécuriser les échanges d'informations

Public

- Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

Pré-requis

Avoir suivi les formations "Pratique des réseaux" (SR200) et "Soyez autonome avec TCP/IP" (SR230) ou connaissances équivalentes

Certification

Cette formation prépare au test ENI-TCP/IP (en option au tarif de 180 €) qui permet d'obtenir la certification IT - Mise en œuvre d'un réseau local TCP/IP

Les + de cette formation

- Une formation très pratique : les participants sont amenés à mettre en œuvre la sécurité d'un réseau d'entreprise à travers de nombreux TP.
- Un point précis sur les obligations légales en termes de sécurité.
- Le passage en revue des solutions disponibles sur le marché.

Programme

1 - L'environnement
- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Les risques
- La protection
- La prévention
- La détection

2 - Les attaques
- Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil
- Les intrusions de niveau 3 (IP) : IP spoofing, déni de service, scanSniffer, man-in-the-middle, les applications stratégiques (DHCP, DNS, SMTP), les applications à risques (HTTP)
- Les attaques logiques : virus, ver, cheval de Troie, spyware, phishing, le craquage de mot de passe
- Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)

3 - Les protections
- Au niveau des commutateurs d'accès : port sécurisé sur mac-adresse, utilisation du protocole 802.1x, VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtre BPDU, root guard
- Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)
- Au niveau IP : les pare-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au dessus de 3), les UTM, les proxys
- Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC
- Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs

4 - Monitoring et prévention
- Sondes IDS
- SysLog Serveur
- Exploitations des logs
- IPS : boîtiers dédiés, fonctionnalité du routeur

5 - Exemples d'architectures
- Exemple d'une entreprise mono-site
- Connexion des nomades
- Exemple d'entreprise multi-site

6 - La sécurité des échanges, la cryptographie
- L'objectif du cryptage et fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN (réseau privé virtuel) site à site et nomades

Réf. SR211
5 jours
(35h présentiel)

2 930 € HT
Offerte

À DISTANCE	BORDEAUX	NANTES	SOPHIA ANTIPOLIS
18/07, 17/10, 05/12	28/11	13/06, 28/11	17/10
PARIS	**LILLE**	**RENNES**	**STRASBOURG**
18/07, 17/10, 05/12	10/10	13/06, 28/11	27/06, 14/11
AIX-EN-PROVENCE	**LYON**	**ROUEN**	**TOULOUSE**
17/10	21/11	18/07, 05/12	28/11

Sécurité VPN, sans-fil et mobilité

Découvrir et évaluer la sécurité des technologies sans-fil

SÉMINAIRE

ACCESSIBLE À DISTANCE

Les réseaux sans-fil sont des facteurs essentiels du développement de la mobilité des outils et solutions informatiques. Cette évolution favorise entre autres le phénomène BYOD (Bring Your Own Device) qui se manifeste par l'utilisation de dispositifs personnels (smartphones, tablettes...) dans les locaux de l'entreprise. Si ce phénomène de portabilité des applications métier en facilite l'accès aux utilisateurs, il subsiste malheureusement un écueil essentiel à considérer : les risques et failles de sécurités engendrés par la proximité des usages d'applications professionnelles et privées. C'est précisément la sécurisation de ces canaux de transport de données sur les réseaux mobiles qui est couverte par cette formation. Durant ces 3 jours, les participants évaluent les vulnérabilités des protocoles de communication sans-fil (WiFi, Bluetooth, GSM, 3G/4G, etc..), pour s'approprier les différents moyens de protection et de sécurisation à leur disposition.

OBJECTIFS

- **Former et sensibiliser des équipes techniques aux problématiques de sécurité liées aux réseaux sans-fil, dans le contexte actuel de forte mobilité des outils technologiques**

Public

- Administrateurs systèmes et réseaux
- Experts en sécurité

Pré-requis

Maîtrise de l'administration système et réseau

Maîtrise des technologies de virtualisation (Virtualbox)

Utilisation autonome de l'invite de commande Linux

Notions de Scripting (Shell, Python)

Les + de ce séminaire

- Une formation très opérationnelle : 70% du temps de la formation est consacré aux exercices pratiques et démonstrations.
- Mise à disposition d'outils radio.

Réf. SR241
3 jours
(21h présentiel)

ORGANISÉ SUR DEMANDE, NOUS CONSULTER

Programme

1 - WiFi
- Rappels sur les technologies WiFi
- Revue des modes de chiffrement
- Présentation du matériel offensif
- Description des différentes techniques d'attaque
- Présentation des moyens de protection

2 - TP WiFi
- Configuration d'un routeur dans les différents modes
- Attaques dans les différents cas de figure (dont injections avec une carte Alpha)
- Durcissement de la configuration
- Présentation du WiFi Pineapple

3 - VPN
- Présentation des différentes technologies et protocoles
- Sécurisation du transport des données
- Limites et exemples d'attaques

4 - TP VPN
- Mise en place d'un tunnel IPSEC
- Sniffing
- Illustration d'une attaque : le mode agressif

5 - SDR, HackRF One et GnuRadio Companion
- Introduction basique aux technologies radio
- Explications sur les principes SDR
- Reconnaître les principaux types de modulation
- Méthodes pour décoder un signal et présentation des principaux outils libres
- Présentation du HackRF One et du Yard Stick One

6 - TP SDR
- Prise en main du HackRF One, GnuRadio, etc.
- Étude d'un carillon sans-fil
- Attaque par rejeu
- Décodage du signal et modulation avec le Yard Stick One

7 - Bluetooth
- Principes de fonctionnement du Bluetooth (BR, EDR et Low Energy)
- Les principaux risques
- Le paradoxe de la difficulté de détection (attaque et défense)
- Présentation de l'Urbertooth One

8 - TP Bluetooth
- Prise en main de l'Ubertooth
- Sniffing du trafic BLE

Hacking et Sécurité - Les fondamentaux

Connaître les différents types d'attaques système pour mieux se protéger

ACCESSIBLE À DISTANCE

L'origine du hacking remonte au milieu des années 50 quand les premiers ordinateurs disponibles dans les universités américaines sont rapidement devenus la proie de d'étudiants avides de "bidouiller" pour s'approprier le système. Ainsi sont nés les hackers qui, profitant de l'avènement d'Internet des décennies plus tard, n'ont cessé de prendre pour cible des systèmes informatiques de plus en plus perfectionnés, allant même jusqu'à pirater des systèmes gouvernementaux. Pour faire face à ces menaces sans cesse croissantes, les DSI attendent des ingénieurs et techniciens qu'ils soient à même de protéger efficacement les systèmes informatiques de leurs organisations. L'objet de cette formation est précisément de leur fournir les compétences et connaissances qui leur permettront de mener à bien cette mission.

OBJECTIFS

- **Comprendre comment il est possible de s'introduire frauduleusement sur un système distant**
- **Connaître les mécanismes en jeu dans le cas d'attaques système**
- **Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes**

Public

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Toute personne intéressée par la pratique de la sécurité

Pré-requis

Connaissances de base de Windows ou Linux

Les + de cette formation

- Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiques.
- Un accent particulier est mis sur la pratique des différentes formes d'attaques existantes.
- Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - Introduction sur les réseaux
- Prise d'informations (Prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants)
- Informations publiques
- Localiser le système cible
- Énumération des services actifs

2 - Attaques à distance
- Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants, et prise de contrôle des postes utilisateurs par troyen
- Authentification par brute force
- Recherche et exploitation de vulnérabilités
- Prise de contrôle à distance

3 - Attaques systèmes
- Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion
- Attaque du Bios
- Attaque en local
- Cracking de mot de passe
- Espionnage du système

4 - Sécuriser le système
- Outils de base permettant d'assurer le minimum de sécurité à son S.I.
- Cryptographie
- Chiffrement des données
- Détection d'activité anormale
- Initiation à la base de registre
- Firewalling
- Anonymat

Réf. SE100
4 jours
(28h présentiel)

2 660 €HT
Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
04/07, 05/09, 24/10	03/10	
PARIS	**LYON**	
04/07, 05/09, 24/10	14/11	

Hacking et Sécurité - Niveau avancé

Pratiquez les attaques avancées pour mieux vous défendre

ACCESSIBLE À DISTANCE

Ce n'est pas un hasard si certaines des sociétés spécialisées en sécurité informatique les plus performantes comptent parmi leurs effectifs d'anciens hackers repentis. On en comprend d'ailleurs aisément la logique tant il parait évident que les personnes les plus à même d'identifier les failles d'un SI sont celles qui sont-elles mêmes capables de l'attaquer. C'est précisément sur cette logique qu'a été conçue cette formation qui propose aux spécialistes informatiques impliqués dans la protection d'un SI d'adopter la position des hackers pour identifier ses éventuelles vulnérabilités et mener à bien les actions permettant de les corriger.

OBJECTIFS

- **Comprendre comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables**
- **Savoir identifier les "faiblesses" des éléments constitutifs du SI par des prises d'empreintes**
- **Disposer des compétences techniques nécessaires pour réaliser différentes attaques et ainsi en comprendre les subtilités**
- **Être en mesure de protéger le SI par un système de contre-mesures adaptées**

Public

- Consultants en sécurité, Ingénieurs / Techniciens, administrateurs systèmes / réseaux, développeurs

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Les fondamentaux " (SE100) ou connaissances équivalentes

Connaissances de TCP/IP

La maîtrise de Linux en ligne de commande est un plus

Les + de cette formation

- Une formation très pratique : 80% du temps de la formation est consacré aux ateliers pratiques.
- Une approche pratique : un panorama des techniques utilisées dans le cadre d'intrusions sur des réseaux d'entreprises, complétée par un atelier pratique sur un laboratoire spécialement créé pour la formation.
- Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).
- Une pédagogie basée sur le partage d'expériences et de bonnes pratiques de la part d'un consultant spécialiste de la sécurité informatique.

Programme

1 - Introduction
- Rappels sur TCP/IP

2 - Introduction à la veille
- Vocabulaire
- Base de données de vulnérabilité et exploitation
- Informations générales

3 - Prise d'informations
- Informations publiques
- Moteur de recherches
- Prise d'information active

4 - Scan et prise d'empreinte
- Énumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

5 - Vulnérabilités informatiques
- Vulnérabilités réseau
- Vulnérabilités applicatives
- Vulnérabilités web
- Exploitation des vulnérabilités
- Maintien de l'accès à une machine

6 - Atelier pratique en laboratoire
- Mise en œuvre d'une stratégie d'attaque sur un laboratoire créé spécialement pour la formation
- Lancement de l'attaque et tentative d'exploitation
- Capture de drapeau
- Étude des contre-mesures appropriées

Réf. SE101
5 jours
(35h présentiel)

3 570 €HT
Offerte

À DISTANCE
01/08, 26/09, 14/11
PARIS
01/08, 26/09, 14/11

Autres sites, nous consulter

Toutes nos formations en détail sur...

www.ib-formation.fr

Avis de l'expert, parcours pédagogiques, publics, dates, ...
tout ce qu'il faut savoir sur nos formations est sur notre site.
Découvrez également nos tests de pré-requis en ligne et nos conseils pour aller plus loin dans l'expertise.

Hacking et Sécurité - Niveau expert

Protéger étape par étape un système d'information

ACCESSIBLE À DISTANCE

L'actualité nous le rappelle quasi quotidiennement, les intrusions dans des systèmes informatiques publics ou privés existent. Et bien souvent, les entreprises qui en sont victimes sont pointées du doigt pour n'avoir pas su correctement protéger leurs données. Si le risque 0 n'existe pas, il apparait presque évident qu'en éprouvant son SI régulièrement, les équipes en charge de garantir la sécurité peuvent être amenées à détecter de nouvelles failles ou menaces et ainsi mettre en œuvre la correction ad' hoc... Durant cette formation très pratique qui consiste en une série d'ateliers ponctuée d'échanges, les participants auront à disposition un environnement technique complexe qu'ils pourront attaquer à loisir pour mieux le protéger par la suite, apprenant ainsi à le protéger un système de bout en bout.

OBJECTIFS

- Savoir protéger son système d'information
- Comprendre comment sécuriser tous les aspects d'un SI : réseau, applicatifs et Web
- Acquérir les connaissances et compétences nécessaires pour détecter des failles et mettre en œuvre des parades
- Savoir correctement réagir en cas d'attaque soudaine
- Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Public

- Développeurs
- Administrateurs systèmes / réseaux
- Ingénieur sécurité
- Consultant sécurité

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes

Les + de cette formation

- Le passage en revue des principales techniques de défense et outils utilisés.
- L'utilisation d'outils d'analyse et d'automatisation des attaques.
- Une formation très pratique : l'essentiel de la formation portera sur des contre-mesures concrètes techniques que chacun peut mettre en œuvre dans son entreprise.
- L'apport de consultants experts en audits techniques des SI.

Programme

1 - Introduction
- Définition du hacking
- Panorama 2018/2019
- Référentiel de sécurité (ANSSI, ENISA, CLUSIF, Cybermalvaillance.gouv etc...)
- Les différents types de hackers
- Les différents types d'attaques
- Les différents outils utilisés par le hacker
- Le cycle de l'attaquant

2 - Le hacking
- Scan de réseau/ports/versions
- Exploitation de CVE
- Élévation de privilège
- Mise en place d'une backdoor
- Récupération d'informations, création d'un dictionnaire + Bruteforce
- Payload msfvenom MITM
- Saut de VLAN (yersinia et/ou table overflow)

3 - Les piliers de la sécurité
- Confidentialité
- Intégrité
- Disponibilité
- Traçabilité

4 - Les grands principes de la sécurité
- IAAA
- Authentification
- Need to know
- Least Privilege
- Non répudiation
- Défense en profondeur

5 - La sécurité physique
- Notion de sécurité physique
- Mise en correspondance des notions avec les principes précédents

6 - Sécuriser le réseau
- La sécurité de la couche 2 : Port security, vLlan, Ssh, dhcp snooping, Defense contre arp MITM, Sécurité pour DTP,CDP,VTP,STP.
- La sécurité de la couche 3 : IPSec, routeur filtrant
- La sécurité de la couche 4 : Explication de la passerelle d'interconnexion de l'ANSSI, Travaux pratiques sur PFsense, explication des IDS/IPS , présentation de Snort, travaux pratiques sur Snort
- La sécurité de la couche 5 : Le proxy

7 - Sécuriser le système
- Hardenning sur Linux
- Hardenning sur Windows
- Mise en place d'HIDS

8 - Supervision de la sécurité
- Présentation SOC
- Présentation SIEM
- Présentation de ELK et Splunk
- Mise en place de ELK ou Splunk pour analyser les Logs

9 - Réponse à incident
- Rejouer les attaques
- Analyser les logs
- Utiliser WireShark

Réf. SE104
5 jours
(35h présentiel)

3 570 €HT
Offerte

À DISTANCE
27/06, 19/09, 28/11
Autres sites, nous consulter

PARIS
27/06, 19/09, 28/11

290 formations au format mixte en 2022

Des solutions multi-modales et digitales pour une nouvelle expérience d'apprentissage

Notre offre intègre de nombreuses formations mixtes (blended) qui associent à la formation en salle des activités digitales de différentes natures : modules e-learning, vidéocasts, rich média, classes virtuelles, Rapid Learning, quiz,...

Nous proposons ainsi des **dispositifs d'apprentissage entièrement tournés vers l'apprenant** qui reposent sur une combinaison optimisée de différentes modalités et qui renforcent ainsi l'efficacité et la rapidité de l'apprentissage.

Conçus par nos experts, les contenus digitaux qui enrichissent nos formations tout en permettant dans de nombreux cas d'en optimiser la durée sont accessibles à distance sur le Learning Hub ib avant, pendant ou après les phases de présentiel.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Hacking et sécurité - Utilisation de Metasploit

Détecter les failles de sécurité informatique de l'entreprise

ACCESSIBLE À DISTANCE

Metasploit est un framework qui permet aux professionnels de la sécurité informatique de réaliser des tests d'attaques et de pénétration. Gratuit et polyvalent, Metasploit propose un large panel d'outils et techniques permettant de réaliser et d'automatiser des tests d'attaques sur de nombreuses cibles (systèmes, applications, serveurs, sites web...). Son succès dans le milieu du hacking Black (hackeurs mal intentionnés) est la preuve de son efficacité. Tous ces outils et tests sont utilisés et pratiqués durant cette formation. Au sortir de ces 5 jours, les participants seront donc en mesure tirer profit de Metasploit pour renforcer la sécurité des outils et matériels sensibles de leur entreprise.

OBJECTIFS

- **Exploiter toutes les capacités du Framework Metasploit**
- **Créer différentes sortes de modules pour Metasploit**
- **Comprendre le fonctionnement de Rex**
- **Concevoir des extensions Meterpreter**
- **Comprendre comment utiliser les fonctionnalités avancées de Metasploit**

Public

- Auditeurs techniques expérimentés

Pré-requis

Posséder de bonnes connaissances des environnements Linux et Windows
Maîtriser les langages C et C++
Avoir une connaissance de Visual Studio

Les + de cette formation

- La formation, se voulant très pragmatique, est composée de 70% de pratique pour 30% de théorie.
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - Introduction
- Structure de Metasploit
- REX
- Cycle d'un pentest avec Metasploit
- Meterpreter
- Armitage

2 - Les scripts
- Prise en main du langage Ruby
- Le shell Ruby
- Les modules de Metasploit
- Concevoir un module
- Réalisation de scripts pour Meterpreter

3 - Exploitation avec RailGun
- Réalisation de scripts pour Meterpreter
- Travailler avec RailGun
- Scripts RailGun
- Manipulation d'API Windows
- Scripts sophistiqués avec RailGun
- Réalisation d'un exploit
- Structure
- Les architectures
- Construction de la base d'un exploit

4 - Portage d'un exploit
- Utilisation avancée des outils de Métasploit...
- Avec PERL
- Avec Python
- Pour le web

5 - Utilisation avancée des outils de Métasploit...
- Meterpreter
- Msfencode
- Msfvenom
- Metasploit browser autopvm
- PHP Meterpreter

Réf. **SE106**
5 jours
(35h présentiel)

**ORGANISÉ SUR DEMANDE,
NOUS CONSULTER**

Evaluations des pré-requis

Testez vos pré-requis en ligne

Parce qu'il est important de ne pas se tromper dans le choix d'une formation, nous avons développé des tests d'évaluation des pré-requis permettant aux stagiaires de s'assurer qu'ils disposent des connaissances nécessaires pour suivre les formations dans de bonnes conditions.

Généralement constitués d'une dizaine de questions à choix multiples, ces évaluations sont disponibles sur les fiches formation présentées sur notre site web (rubrique pré-requis).

Hacking et sécurité - Utilisation de WireShark

Utiliser WireShark pour protéger et optimiser les performances réseaux de l'entreprise

ACCESSIBLE À DISTANCE

WireShark est un outil d'analyse de paquets très répandu chez les professionnels de la sécurité informatique. Opérationnel sur différents environnements (Unix, openBSD, macOS, Windows,...) il facilite les captures, le décodage et l'analyse de paquets transmis sur tous les types de réseaux (VoIP, Ethernet, Wi-Fi, réseaux mobiles, trafic sur les clés USB, ...). Durant cette formation de 4 jours, les participants s'approprieront l'utilisation des différentes fonctionnalités de WireShark pour diagnostiquer, protéger et optimiser les performances réseaux de leur entreprise.

OBJECTIFS

- Savoir positionner WireShark dans le domaine de la sécurité informatique
- S'approprier les paramétrages avancés de WireShark
- Savoir exploiter et interpréter les analyses de paquets obtenues avec WireShark

Public

- Administrateurs réseaux
- Professionnels de la sécurité informatique

Pré-requis

Notions de sécurité informatique
Expériences dans l'administration des réseaux (LAN et WAN)

Les + de cette formation

- Une formation très pragmatique : 70% de pratique pour 30% de théorie.
- Les participants bénéficient du partage d'expériences du formateur expert.

Programme

1 - Introduction
- Définition du Forensic
- Les types de Forensics
- Forensic réseau
- Wireshark, principes et fonctions de base

2 - Paramétrage avancé de Wireshark
- Filtres de capture et filtres d'affichage
- Création de profiles
- Techniques essentielles
- Sniffing réseau en lignes de commandes

3 - Analyse des menaces de sécurité sur les LAN
- Analyse de trafic en clair
- Analyse d'attaques de sniffing
- Analyse des techniques de reconnaissance réseau
- Détection des tentatives de craquage de mots de passe
- Autres attaques
- Outils complémentaires de Wireshark
- Filtres d'affichages importants

4 - Analyse des communications email
- Forensic d'email
- Analyse d'attaques sur les communications email
- Filtres importants

5 - Inspection du trafic malware
- Préparation de Wireshark
- Analyse de trafic malveillant
- Botnets IRC

6 - Analyse des performances réseau
- Création d'un profile spécifique au dépannage réseau
- Optimisation avant analyse
- Problèmes liés à TCP/IP

Réf. SE107
4 jours
(28h présentiel)

2 830 €HT
Offerte

À DISTANCE
25/07, 19/12
PARIS
25/07, 19/12

Autres sites, nous consulter

1 050 formations accessibles à distance

Avec ses classes à distance, ib facilite l'accès à la formation

Avec notre solution de classes à distance, suivez les formations animées par nos formateurs depuis n'importe quel lieu équipé d'une connexion internet.

Grâce à des infrastructures matérielles et logicielles de dernière génération et une pédagogie adaptée, nous vous proposons une expérience très proche d'une formation en présentiel : 100% de face à face avec le formateur, échanges entre participants, mises en situation, travaux de groupes...

96,7% de participants satisfaits en 2021

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Écriture de scripts Python pour les tests d'intrusion

Développement et exploitation avec Python pour le Pentest

OBJECTIFS

- Être capable de faciliter le développement d'exploits en Python
- Comprendre comment automatiser le traitement de tâches et automatiser les exploitations
- Apprendre à contourner les solutions de sécurité
- Savoir interfacer différents langages avec Python

Public

- RSSI
- Consultants en sécurité
- Ingénieurs et techniciens
- Administrateurs systèmes et réseaux

Pré-requis

Connaissances en Python

Les + de cette formation

- Cette formation arbore les différents modules et cas d'utilisations de Python lors de tests d'intrusions.
- Une formation très pratique : les participants traiteront de nombreuses problématiques rencontrées lors d'audits et les solutions pouvant être mises en place rapidement grâce au scripting Python afin d'automatiser les tâches complexes et spécifiques (80% du temps de la formation est consacré aux TP).

Programme

1 - Python pour HTTP, requests
- Développement d'un système de recherche exhaustive
- Contournement de captcha

2 - Développement d'un module Python BurpSuite
- Introduction à BurpSuite
- Développement d'un module de détection passif de Web Application Firewalls

3 - Exploitation d'une injection SQL en aveugle
- Extraction bit à bit et analyse comportementale

4 - Introduction aux tâches distribuées
- Introduction à l'attaque Slowloris
- Développement d'un exploit slowloris distribué

5 - Python et l'altération HTTP
- Introduction à MITMProxy
- Développement d'un module "SSL Striping"

6 - Python et le forensics
- Volatility
- Hachoir
- Network Forensics avec Scapy

7 - Le C et Python, Cython
- ctypes
- Développement d'un module Cython Antivirus et Backdoors

8 - Antivirus et backdoors
- Shellcodes
- Création d'une porte dérobée avancée

9 - Chaîne d'exploitation
- Exploitation de multiples vulnérabilités
- Création d'un exploit complet (POC)

10 - TP Final
- Capture the Flag

Réf. SE108
4 jours
(28h présentiel)

2 950 €HT

PARIS
13/06, 21/11

Autres sites, nous consulter

Tests d'intrusion - Mise en situation d'audit

Le Pen Test par la pratique

ACCESSIBLE À DISTANCE

En bon professionnel, tout responsable de la sécurité informatique doit remettre en question les protocoles et techniques employés pour sécuriser son réseau à intervalle régulier. En effet, chaque semaine, de nouveaux virus apparaissent, de nouvelles failles sont détectées pour un OS ou un matériel et devant ces nouveaux risques il convient de s'assurer que la sécurité n'est pas menacée. L'audit est une réponse adaptée à ce challenge : le Pen Test (de l'anglais "Penetration Test") est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations. Les participants à cette formation avancée apprendront à mettre en place une véritable procédure d'audit de type Pen Test et ainsi évaluer les risques et décider des actions à mettre en œuvre.

OBJECTIFS

- Savoir organiser une procédure d'audit de sécurité de type test de pénétration sur son SI
- Se mettre en situation réelle d'Audit
- Mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle
- Être en mesure de rédiger un rapport d'audit professionnel

Savoir présenter et transmettre un rapport d'audit

Public

- RSSI
- Consultants en sécurité
- Techniciens
- Auditeurs amenés à faire du Pen Test ou ceux qui veulent se perfectionner en Pen Test
- Administrateurs systèmes / réseaux

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes

Les + de cette formation

- Le passage en revue des principales techniques d'attaques et outils utilisés.
- L'utilisation d'outils d'analyse et d'automatisation des attaques.
- Une formation très pratique : une mise en situation d'audit sera faite afin d'appliquer sur un cas concret les outils méthodologiques et techniques vus lors de la première journée. Le système d'information audité comportera diverses vulnérabilités (web, applicatives, etc.) plus ou moins faciles à découvrir et à exploiter. L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information.
- L'apport de consultants experts en audits techniques des SI.

Programme

1 - Méthodologie de l'audit

2 - Objectifs et types de Pen Test
- Qu'est-ce qu'un Pen Test ?
- Le cycle du Pen Test
- Différents types d'attaquants
- Types d'audits : boîte noire, boîte blanche, boîte grise
- Avantages du Pen Test
- Limites du Pen Test
- Cas particuliers : dénis de service, ingénierie sociale

3 - Aspect réglementaire
- Responsabilité de l'auditeur
- Contraintes fréquentes
- Législation : articles de loi
- Précautions
- Points importants du mandat

4 - Exemples de méthodologies et d'outils
- Préparation de l'audit
- Déroulement
- Cas particuliers
- Habilitations
- Dénis de service
- Ingénierie sociale
- Déroulement de l'audit
- Reconnaissance
- Analyse des vulnérabilités
- Exploitation
- Gain et maintien d'accès
- Comptes-rendus et fin des tests

5 - Mise en pratique sur Metasploitable
- Attaque de la machine virtuelle Metasploitable
- Recherche d'informations
- Recherche de vulnérabilités
- Exploitation des vulnérabilités
- Maintien de l'accès

6 - Éléments de rédaction d'un rapport
- Importance du rapport
- Composition
- Synthèse générale
- Synthèse technique
- Évaluation du risque
- Exemples d'impacts
- Se mettre à la place du mandataire

7 - Préparation du rapport d'audit
- Mise en forme des informations collectées lors de l'audit
- Préparation du document et application de la méthodologie vue lors du premier jour

8 - Écriture du rapport
- Analyse globale de la sécurité du système
- Description des vulnérabilités trouvées
- Définition des recommandations de sécurité
- Synthèse générale sur la sécurité du système

9 - Transmission du rapport
- Précautions nécessaires
- Méthodologie de transmission de rapport
- Que faire une fois le rapport transmis ?

Réf. SE102
5 jours
(35h présentiel)

3 380 €HT
Offerte

À DISTANCE
17/10, 05/12
PARIS
17/10, 05/12

Autres sites, nous consulter

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Tests d'intrusion pour les réseaux et terminaux mobiles

Sécuriser l'usage des terminaux mobiles

ACCESSIBLE À DISTANCE

OBJECTIFS

- Acquérir les connaissances et compétences liées aux tests de pénétration des réseaux et équipements mobiles
- Identifier les failles de sécurité des réseaux mobiles
- Être capable de sécuriser des équipements mobiles dotés d'IOS ou d'Android
- Comprendre comment sécuriser les paiements sans contact
- Savoir se prémunir contre les malwares

Public

- Techniciens et administrateurs réseaux, auditeurs, pentesteurs, RSSI

Pré-requis

Bonnes connaissances système et réseaux
Bonnes connaissances sécurité et hack éthique

Les + de cette formation

- La formation, se voulant très pragmatique, est composée de 70% de pratique pour 30% de théorie.
- Un accent particulier est mis sur la pratique des différentes formes d'attaques existantes.
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - Le risque des réseaux mobiles
- Présentation de l'écosystème
- Le modèle du risque

2 - Attaquer un réseau cellulaire
- Présentation
- Interopérabilité
- Les appels téléphoniques
- La messagerie vocale
- Les SMS
- Contre-mesures
- L'IOS
- Présentation iOS pentest toolkit
- La sécurisation de l'iOS
- Jailbreaking
- Hack d'iPhones
- Exfiltration
- Contre-mesures

3 - Androïd
- Présentation Android pentest toolkit
- Modèle de sécurité
- Stockage de données
- NFC
- Développement Android
- Décompilation et désassemblage
- Interception du trafic réseau
- Exfiltration
- Principes de sécurisation

4 - Les malwares mobiles
- Quelques chiffres
- Les Malwares sur Android
- Les Malwares sur iOS

5 - MDM
- Framework MDM
- Provisioning
- Bypass MDM

6 - Paiement par mobile
- Présentation
- Paiement sans contact
- Google Wallet

7 - Web et services mobiles
- Généralités
- Attaques XML
- OAuth 2
- SAML
- Navigateur Web mobile et sécurité WebView

Réf. SE105
5 jours
(35h présentiel)

**ORGANISÉ SUR DEMANDE,
NOUS CONSULTER**

L'aide au recrutement avec la POE (Préparation Opérationnelle à l'Emploi)

Vous rencontrez des difficultés pour recruter des collaborateurs dont les profils et les compétences sont en adéquation avec vos besoins ?

ib vous propose un dispositif complet qui répond précisément à cette problématique.
En associant pré-recrutement et formation préalable à l'embauche, ib vous propose une solution clé en main qui vous permettra d'intégrer des collaborateurs immédiatement opérationnels sur des métiers en tension.

A travers notre dispositif qui associe aux avantages liés à la POEI des services à forte valeur ajoutée, nous apportons une réponse efficace aux problèmes de pénuries de compétences et d'employabilité auxquels sont aujourd'hui confrontées les entreprises.

Pour en savoir plus, contactez-nous au 0 825 07 6000

Analyste SOC (Security Operations Center)

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

Assurer les fonctions d'analyste d'un SOC, principalement la détection et l'analyse des intrusions, l'anticipation et la mise en place des protections nécessaires

L'actualité le montre chaque jour davantage, nos organisations sont exposées à des menaces d'un nouveau genre qui peuvent fortement impacter leur fonctionnement. Clairement décidées à agir, nombreuses sont celles qui recourent aux services d'un SOC (Security Operations Center), que celui-ci soit intégré ou externalisé. L'objectif ? Pourvoir s'appuyer sur une cellule dont la mission est de prévenir, détecter et gérer les incidents de cybersécurité au plus tôt tout en menant les actions nécessaires pour qu'ils surviennent le moins possible. Au cœur du dispositif, l'analyste SOC assure la surveillance du système d'information afin de détecter les attaques dont il fait l'objet mais aussi les risques éventuels auxquels il est exposé. Véritable professionnel de la sécurité, il doit limiter la portée des attaques, interpréter les menaces et mener les actions visant à s'en préserver.

OBJECTIFS

- Connaître l'organisation d'un SOC
- Comprendre le métier d'analyste SOC
- Appréhender les outils utilisés par les analystes SOC
- Identifier les principales problématiques à travers des cas d'usage
- Apprendre à détecter des intrusions
- Savoir gérer différents incidents
- Optimiser la sécurité d'un système d'information

Public

- Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets...

Pré-requis

Connaître le guide sécurité de l'ANSSI
Avoir des connaissances en réseau
Avoir suivi le parcours introductif à la cybersécurité (MG847) ou posséder des connaissances équivalentes

Les + de cette formation

- Ce parcours d'une durée de 8 jours se découpe en 4 modules de 2 jours. Le rythme visé est un module toutes les deux semaines sur une amplitude maximale de 2 mois.
- Un programme étudié pour permettre aux participants d'intégrer un SOC en étant opérationnel sur les outils et méthodes.
- Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
- Les nombreux retours d'expériences de consultants expérimentés permettent d'illustrer les concepts et d'accroître la pertinence des réponses fournies.

Programme

1ère partie (2 jours)

1 - Principes et référentiels de gestion des incidents cybersécurité

- Introduction à la gestion des incidents cybersécurité
- NIST SP 800-61 Vs ISO / CEI 27035
- Les phases de gestion d'incident de cybersécurité
- Partage d'informations

2 - Les métiers du SOC : Incident Handling and Computer Forensics selon NIST

- Organisation d'une capacité de réponse aux incidents
- Processus de gestion des incidents
- Coordination et partage d'informations
- Exemples pratiques de réponses à des scénarios d'incidents cybersécurité : les signes d'incidents et les sources de collecte, incident relatif à un malware, incident de déni de service DoS, incident de défiguration de site web

2ème partie (2 jours)

1 - Organisation et outils du SOC : Cybersecurity monitoring et SOC Foundation

- Les enjeux de la surveillance du SI et SOC
- Introduction à « Security Monitoring »
- Security Operational Center – SOC
- Les modèles de SOC
- Les bases du SIEM
- Comment Fonctionne SIEM ?
- Évolution du SIEM
- Réponse aux incidents et automatisation avec SIEM
- Cas d'utilisation d'un NG-SIEM

2 - Vulnerability Management

- Introduction à la gestion des vulnérabilités
- Processus de gestion des vulnérabilités
- L'évolution du cycle de gestion des vulnérabilités
- Les nouveaux systèmes de gestion des vulnérabilités – VMS

3ème partie (2 jours)

1 - Cybersecurity Intelligence Incident Response Technologies

- EndPoint Detection et Response – EDR : EndPoint Protection Plateform – EPP, Enjeux et défis, l'apparition de l'EDR, évolution des EPP, mode opératoire des nouvelles solutions EPP, exemple d'une réponse par EDR à une attaque Ransomware
- Security Orchestration Automation et Response – SOAR : les nouveaux défis des SOCs, Security Orchestration Automation et Response (SOAR), OAR Vs SIEM, User and Entity Behavior Analytics – UEBA, comment mettre en œuvre une solution SOAR, avantages, pièges et conseils de mise en œuvre une solution SOAR, cas d'utilisation de l'automatisation de la sécurité pour votre entreprise (PLAYBOOK)

2 - Implémentation du SIEM : les sources de données et la collecte de logs

- Sélection des logs à analyser
- Collecte des logs avec rsyslog (Linux)
- Collecte des logs avec Sysmon (Windows)
- Surveillance des logs du réseau

4ème partie (2 jours)

1 - Implémentation du SIEM : centralisation des alertes avec la stack ELK

- La stack ELK
- Allez plus loin avec ELK

2 - Les scénarios d'attaque avec la matrice ATTetCK et analyses tactiques

- Utilisation de la matrice ATTetCK
- Identification des scénarios d'attaque
- Réflexions et analyses tactiques (SIEM)

Réf. MG842
8 jours (2+2+2+2)
(56h présentiel)

4 890 €HT
Paris 184 €HT

À DISTANCE
15/09 & 06/10 & 26/10 & 09/11
PARIS
15/09 & 06/10 & 26/10 & 09/11

Autres sites, nous consulter

Analyse forensic et réponse à incidents de sécurité

Réaliser une analyse post-mortem d'incident de sécurité informatique

ACCESSIBLE À DISTANCE

La probabilité qu'une entreprise soit victime d'une attaque augmente à mesure que les technologies évoluent. Face à ce risque croissant, les systèmes d'information peuvent subir des attaques sans que les responsables de leur sécurité ne les détectent dans l'instant et y apporte une parade. Dans le cas ou des dommages seraient constatés (vols de données par exemple), il existe une technique d'investigation post-incident : l'analyse forensic. Par l'analyse des dommages subits et des traces laissées par les attaquants, elle vise à établir la chronologie évènementielle pour reconstituer l'attaque et collecter des éléments exploitables en justice. Elle permet également d'identifier les actions d'ordre technique à mener pour neutraliser la menace.

OBJECTIFS

- Connaître les aspects juridiques de l'analyse forensic
- Savoir mener une analyse forensic
- Savoir reconstituer un incident de sécurité informatique en vue de l'expliquer
- Comprendre les sources d'un incident pour mieux se défendre
- Savoir collecter des informations utiles pour établir un dossier avec des preuves

Public

- Consultant en sécurité informatique
- Administrateurs systèmes / réseaux

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes

Les + de cette formation

- Le passage en revue des principales techniques d'analyse post-mortem.
- L'utilisation d'outils d'analyse poussés d'un système compromis.
- Une formation très pratique : l'essentiel de la formation portera sur des outils concrets que chacun peut employer dans son entreprise.
- L'apport de consultants experts en audits techniques des SI.

Programme

1 - Aspects juridiques
- Bases légales de la sécurité de l'information
- Classification des crimes informatiques
- Rôle de l'enquêteur / de l'inforensique
- Acteurs technico-juridiques : CERT, agences nationales, gendarmerie...

2 - Détecter l'incident
- Repérer les anomalies
- Revue des outils de détection d'incident
- Mise en œuvre d'un IDS / IPS

3 - Réagir suite à un incident
- Conserver les preuves
- Collecter les informations
- Revue des outils de collecte de l'information

4 - Atelier - Analyse d'un système informatique piraté
- Mise en œuvre d'un laboratoire dédié à la formation
- Analyse des anomalies
- Établir l'incident de sécurité
- Diagnostic technique et neutralisation de la menace
- Recherche de l'origine de l'attaque
- Contre-mesures

Réf. SE103
4 jours
(28h présentiel)

2 570 €HT
Offerte

À DISTANCE
07/06, 22/08, 07/11
PARIS
07/06, 22/08, 07/11

Autres sites, nous consulter

Les implantations

En mettant à votre disposition des équipes commerciales dans chacune de nos agences, nous vous apportons la garantie d'une vraie relation de proximité. Quel que soit votre besoin, vous bénéficiez de l'accompagnement d'experts géographiquement et culturellement proches de vous :

PARIS	LILLE	RENNES	STRASBOURG
AIX-EN-PROVENCE	LYON	ROUEN	TOULOUSE
BORDEAUX	NANTES	SOPHIA-ANTIPOLIS	

Collecte et analyse des Logs avec Splunk

Optimiser l'exploitation des données machines et des logs

ACCESSIBLE À DISTANCE

L'exploitation centralisée des données machines issues des logs des serveurs et postes de travail du parc de l'entreprise dépasse désormais de loin l'historique gestion des alertes. Splunk, numéro un sur son marché, propose aux administrateurs systèmes et réseaux un panel d'outils et des fonctionnalités aussi variées que performantes. La recherche d'informations et la production de rapports s'en trouve facilités par les différents modèles à disposition, ainsi les administrateurs peuvent se consacrer aux diverses taches d'exploitation. C'est précisément pour savoir tirer profit de ces différents outils que cette formation a été conçue. A l'issue de ces 2 jours, les participants disposeront des compétences et connaissances leur permettant d'optimiser et d'exploiter les données machines et logs du parc informatique de leur entreprise.

OBJECTIFS

- Être capable de comprendre les concepts Splunk Utilisateur et Splunk Administrateur
- Apprendre à installer Splunk
- Pouvoir écrire des requêtes de recherche simple dans les données
- Savoir appliquer les différentes techniques de visualisation de données en utilisant les graphes et tableaux de bord
- Être en mesure d'implémenter Splunk pour analyser et surveiller les systèmes
- Comprendre comment écrire des requêtes avancées de recherche dans les données
- Savoir configurer les alertes et les rapports

Public

- Administrateurs systèmes et réseaux

Pré-requis

Connaissances de base des réseaux et des systèmes

Les + de cette formation

- Une approche exhaustive de l'analyse des logs avec Splunk : de l'installation à la mise en œuvre de tableaux de bord et d'alertes, tous les aspects sont couverts par le programme.
- Une large place accordée à la pratique qui permet aux participants d'acquérir rapidement les compétences nécessaires à la mise en œuvre de Splunk dès leur retour en entreprise.
- Les retours d'expérience de consultants experts du sujet.

Programme

1 - Installer Splunk ; récupérer/injecter les données

- Concepts Big Data
- Installer Splunk sous Windows
- Indexer des fichiers et des répertoires via l'interface Web
- Mise en œuvre de l'Universal Forwarder
- Gestion des Indexes
- Durée de rétention des données
- Travaux pratiques : installer et configurer Splunk ; utiliser Universal Forwarder pour récupérer des logs Apaches/Linux et Active Directory/Windows

2 - Exploration de données

- Requêtes avec Search Processing Language, ou SPL, un langage développé par Splunk
- Opérateurs booléens, commandes
- Recherche à l'aide de plages de temps
- Travaux pratiques : mise en œuvre de définition d'extractions de champs, de types d'évènements et de labels ; traitement de fichiers csv ; extraire des statistiques de fichiers de journalisation Firewall

3 - Tableaux de bord (base)

- Les tableaux de bord et l'intelligence opérationnelle, faire ressortir les données
- Les types de graphes
- Travaux pratiques : créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées

4 - Tableaux de bord (avancé)

- Commandes avancées de SPLLookup
- Produire de façon régulière (programmée) des tableaux de bord au format PDF
- Travaux pratiques : créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées ; création de nombreux tableaux de bord basés sur l'analyse des événements Windows dans une optique de scénarii d'attaques

5 - Installation d'application

- Installer une application existante issue de Splunk ou d'un tiers
- Ajouter des tableaux de bord et recherches à une application
- Travaux pratiques : créer une nouvelle application Splunk ; installer une application et visualiser les statistiques de trafics réseaux

6 - Modèles de données

- Les modèles de données
- Mettre à profit des expressions régulières
- Optimiser la performance de recherche
- Pivoter des données
- Travaux pratiques : utiliser la commande pivot, des modèles pour afficher les données

7 - Enrichissement de données

- Regrouper les événements associés, notion de transaction
- Mettre à profit plusieurs sources de données
- Identifier les relations entre champs
- Prédire des valeurs futures
- Découvrir des valeurs anormales
- Travaux pratiques : mise en pratique de recherches approfondies sur des bases de données

8 - Alertes

- Conditions surveillées
- Déclenchement d'actions suite à une alerte avérée
- Devenir proactif avec les alertes
- Travaux pratiques : exécuter un script lorsqu'un attaquant parvient à se connecter sur un serveur par Brute Force SSH

Réf. SR240
2 jours
(14h présentiel)

1 485 €HT
Offerte

À DISTANCE
17/11
PARIS
17/11

Autres sites, nous consulter

Mise en place d'un SIEM

Maîtrisez votre gestion d'évènements

ACCESSIBLE À DISTANCE

OBJECTIFS

- Comprendre les limites des outils de sécurité classiques
- Découvrir les principes technologiques derrière l'acronyme SIEM
- Apprendre à détecter les menaces parmi un grand volume d'informations

Public

- Consultants en sécurité
- Ingénieurs / Techniciens
- Responsables techniques

Pré-requis

Maîtrise de l'administration Linux
Bonnes connaissances réseau / système
Notions de Scripting

Les + de cette formation

- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- Priorité à la pratique : de nombreux ateliers amènent les participants à mettre concrètement en place un SIEM.

Programme

1 - Rôle de la détection d'intrusion

2 - Terminologie
- Faux-positifs, détection, prévention, etc

3 - Architecture et types d'IDS

4 - Présentation de l'IDS Suricata

5 - Déploiement et configuration de base

6 - Langage d'écriture de règles

7 - Journalisation via Syslog

8 - Travaux pratiques
- Mise en place d'une architecture IDS virtualisée : firewall, cible, attaquant
- Jeu d'attaques et création de règles de détection (scans, bruteforce, exploitation de vulnérabilité)

9 - Présentation du HIDS OSSEC et architecture

10 - Déploiement et configuration de base

11 - Syntaxe d'écriture de règles

12 - Travaux pratiques
- Écriture de règles

13 - Limites des IDS

14 - Intégration avec les autres composants du SI

15 - Points importants dans le cadre d'un appel d'offre

16 - Défis modernes posés à la supervision classique
- Objectifs d'un SIEM
- Architecture et fonctionnalités
- Syslog et centralisation des journaux
- Synchronisation du temps (NTP)
- Présentation d'ELK
- Configuration avancée de Logstash

17 - Travaux pratiques
- Configuration d'agents Logstash
- Écritures de Groks avancés
- Environnement hétérogène : Linux, Windows

18 - Visualisation des résultats dans Kibana

19 - Conclusion
- Discussions sur les solutions alternatives
- Préparation des points-clés pour un appel d'offre

Réf. **SE010**
4 jours
(28h présentiel)

ORGANISÉ SUR DEMANDE, NOUS CONSULTER

Pour vous inscrire à une formation... il y a toujours un moyen de nous contacter

Par téléphone

Nos Conseillers Formation sont joignables de 8h30 à 18h00 au 0 825 07 6000. Ils répondront à toutes vos questions concernant les formations, les dates de sessions, les opportunités de dernière minute...

Par e-mail

Une adresse unique : espace.clients@ib.cegos.fr pour toutes vos inscriptions ou demandes de renseignements.

Par Internet

Retrouvez sur www.ib-formation.fr l'intégralité de nos programmes ainsi que toutes les informations qui vous seront utiles : dates de sessions, plans d'accès, offres de dernière minute, informations sur les évènements ib....

IBM QRadar SIEM - Les bases

Analyser les évènements du SI pour identifier les menaces

ACCESSIBLE À DISTANCE

En raison d'un nombre toujours croissant d'évènements générés par les composants d'un système d'information, un traitement à la volée est devenu impossible. C'est pourquoi les éditeurs se sont penchés sur la création d'outils permettant de gérer l'ensemble des journaux générés par les composants d'un SI (réseaux, applications, serveurs... et même utilisateurs). Ainsi, QRadar SIEM, la solution proposée par IBM se charge-t-elle de détecter des anomalies, comportements inhabituels et autres attaques en collectant puis en "analysant" (les experts parlent plus précisément d'un enchaînement de 3 actions distinctes : normalisation, agrégation et corrélation) l'ensemble des évènements en provenance du SI. Les participants à cette formation apprendront à améliorer la sécurité d'un système d'information à l'aide de QRadar SIEM.

OBJECTIFS

- Décrire comment QRadar SIEM collecte des données pour détecter les activités suspectes
- Décrire l'architecture des composants QRadar SIEM et les flux de données
- Apprendre à naviguer dans l'interface utilisateur
- Savoir utiliser QRadar pour détecter les activités suspectes et enquêter sur les attaques et les violations présumées
- Pouvoir rechercher, filtrer, regrouper et analyser les données de sécurité
- Enquêter sur les événements et les flux et sur les profils d'actifs
- Pouvoir décrire l'objectif de la hiérarchie réseau
- Déterminer comment les règles testent les données entrantes et créent des infractions
- Apprendre à utiliser l'index et la gestion des données agrégées
- Être capable de naviguer et personnaliser les tableaux de bord et les éléments de tableau de bord
- Comprendre comment créer des rapports personnalisés
- Savoir utiliser des filtres
- Être en mesure d'utiliser AQL pour les recherches avancées
- Savoir analyser un scénario du monde réel

Public

- Analystes sécurité, architectes techniques de sécurité, administrateurs réseaux et administrateurs systèmes utilisant QRadar SIEM

Pré-requis

Posséder des connaissances dans les domaines suivants : infrastructure informatique, fondamentaux de la sécurité informatique, Linux, les réseaux TCP/IP et Syslog

Certification

Cette formation prépare aux tests C1000-018 et C1000-026 (en option) qui permettent d'obtenir les certifications IBM Certified Associate Analyst - IBM QRadar SIEM V7.3.2 et IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2

Les + de cette formation

- Une formation opérationnelle : les apports théoriques sont systématiquement accompagnés de phases de mise en pratique qui favorisent un ancrage durable des acquis.
- Les conseils de professionnels ayant exploité la solution en entreprise.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Programme

1 - Introduction à IBM QRADAR
2 - Architecture des composants IBM QRADAR SIEM et flux de données
3 - Utilisation de l'interface utilisateur QRADAR SIEM
4 - Enquête sur une infraction déclenchée par des évènements
5 - Enquête sur les évènements d'une infraction
6 - Utilisation des profils d'actifs pour enquêter sur les infractions
7 - Enquête sur une infraction déclenchée par des flux
8 - Utilisation des règles
9 - Utilisation de la hiérarchie réseau
10 - Gestion des données agrégées et indexées
11 - Utilisation du tableau de bord QRADAR SIEM
12 - Création de rapports
13 - Utilisation de filtres
14 - Utilisation du langage AQL (Ariel Query Language) pour les recherches avancées
15 - Analyse d'une attaque à grande échelle dans le monde réel

Réf. SR845
3 jours
(21h présentiel)

2 270 €HT

À DISTANCE
05/09, 10/10, 14/11

IBM QRadar SIEM - Notions avancées

Identifier rapidement les menaces les plus « discrètes »

ACCESSIBLE À DISTANCE

QRadar SIEM est une plate-forme de gestion de sécurité des réseaux conçue pour détecter les anomalies, identifier les menaces et filtrer les faux positifs (des erreurs de jugement conduisant à lancer des alertes sans qu'il n'y ait lieu de le faire). Pour y parvenir, QRadar SIEM consolide les données des évènements historisés et des flux réseaux avant de les analyser pour détecter les éventuelles infractions à la sécurité nécessitant des enquêtes. Les participants à cette formation avancée apprendront à tirer parti de l'ensemble des possibilités offertes par la plate-forme pour sécuriser encore davantage leurs réseaux.

OBJECTIFS

- Comprendre comment créer des sources de journal personnalisées pour utiliser des événements provenant de sources inhabituelles
- Apprendre à créer, gérer et utiliser des collections de données de référence
- Savoir développer et gérer des règles personnalisées pour détecter une activité inhabituelle dans votre réseau
- Être en mesure de développer et gérer des scripts d'action personnalisés pour une réponse automatique aux règles
- Apprendre à développer et gérer des règles de détection d'anomalies pour détecter les situations de trafic réseau inhabituelles

Programme

1 - Création de types de source de journal
2 - Exploitation des collections de données de référence
3 - Développement de règles personnalisées
4 - Création de scripts d'action personnalisés
5 - Développement de règles de détection des anomalies

Public

- Administrateurs de sécurité
- Architectes techniques de sécurité
- Gestionnaires des infractions
- Services professionnels utilisant QRadar SIEM
- Administrateurs QRadar SIEM

Pré-requis

Connaissances de l'infrastructure informatique, des principes fondamentaux de la sécurité informatique, de Linux, Microsoft Windows, de la mise en réseau TCP/IP, des fichiers de journaux et des événements et des flux réseau

Vous devez également avoir suivi la formation "IBM QRadar SIEM - Les bases" (SR845)

Les + de cette formation

- L'apprentissage par la pratique : de nombreuses mises en situation permettent aux participants de tester en salle les pratiques et méthodes enseignées
- Le partage de bonnes pratiques pour exploiter le plus efficacement possible toute la puissance de la solution
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Réf. SR868
2 jours
(14h présentiel)

1 590 €HT

À DISTANCE
02/06, 08/09, 13/10, 17/11

Evaluations des pré-requis

Testez vos pré-requis en ligne

Parce qu'il est important de ne pas se tromper dans le choix d'une formation, nous avons développé des tests d'évaluation des pré-requis permettant aux stagiaires de s'assurer qu'ils disposent des connaissances nécessaires pour suivre les formations dans de bonnes conditions.

Généralement constitués d'une dizaine de questions à choix multiples, ces évaluations sont disponibles sur les fiches formation présentées sur notre site web (rubrique pré-requis).

Audit de sécurité de sites Web

L'audit Web par la pratique

Il est largement connu que les sites web sont des cibles privilégiées pour les hackers. Et ce n'est pas surprenant dans la mesure où il est fréquent que ceux-ci ne soient pas suffisamment sécurisés. Souvent par manque d'information, parfois par précipitation (pour limiter le retard pris sur un projet, il n'est pas rare que certaines étapes importantes soient survolées ou même totalement négligées). Et les techniques d'attaque sont nombreuses : attaques matérielles, dialogue réseau, attaques systèmes, attaques des bases de données.... C'est pourquoi il est nécessaire, pour s'assurer de la sécurité des sites web, de pratiquer des audits très complets. Et cela ne doit pas s'improviser. Il faut en effet suivre des processus précis et complets pour ne passer à côté d'aucune faille. C'est ce qu'apprendront les participants à cette formation.

OBJECTIFS

- **Connaître les différents types de vulnérabilités des sites web et comprendre comment elles peuvent être exploitées**
- **Comprendre comment augmenter le champ d'exploitation des vulnérabilités pour un test d'intrusion**
- **Disposer de l'ensemble des connaissances et compétences nécessaires à la réalisation d'un audit de sécurité**

Public

- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

Pré-requis

Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou connaissances équivalentes

Maîtrise des outils Linux

Connaissance des langages de développement Web

Les + de cette formation

- La formation permettra aux participants d'apprendre à mettre en place une véritable procédure d'audit de site Web. Ils seront confrontés aux problématiques de la sécurité des applications Web.
- Une formation très pratique : les différents aspects d'une analyse seront mis en avant à travers de nombreux exercices pratiques (70% du temps de la formation est consacré aux TP).
- Les participants bénéficient des retours d'expérience de consultants experts en cybersécurité.

Programme

1 - Introduction
- Rappel méthodologie d'audit : boite noire, boite grise
- Plan d'action : prise d'information, scan, recherche et exploitation de vulnérabilités, rédaction du rapport

2 - Reconnaissance
- Reconnaissance passive : base de données WHOIS, services en ligne (Netcraft, Robtex, Shodan, Archives), moteurs de recherche, réseaux sociaux, outils
- Reconnaissance active : visite du site comme un utilisateur, recherche de page d'administration, recherche de fichiers présents par défaut, robots.txt, sitemap, détection des technologies utilisées
- Contre-mesures : limiter l'exposition réseau, filtrer les accès aux pages d'administration et aux pages sensibles, remplacer les messages d'erreurs verbeux par des messages génériques

3 - Scan
- Les différents types de scanner : scanner de ports, scanner de vulnérabilité, scanners dédiés
- Limites des scanners

4 - Vulnérabilités
- Vulnérabilités de conception : politique de mise à jour, chiffrement des communications, politique de mot de passe (par défaut, faibles, stockage des mots de passe), isolation intercomptes (accès aux données d'autres utilisateurs, modification d'informations personnelles), gestion des sessions (prédictibles, transitant dans l'URL), contremesures (mise à jour des applications et des systèmes, chiffrement des communications, utilisation et stockage des mots de passe, vérification des droits utilisateurs, système de session non prédictible avec une entropie élevée, drapeaux des cookies)

5 - Vulnérabilités web
- Mise en place d'une solution de Proxy (Burp Suite)
- Cross-Site Scripting (XSS) : XSS réfléchie, XSS stockée, XSS Dom-Based, contournement des protections, démonstration avec l'outil d'exploitation BeEF, contre-mesures
- Cross-Site Request Forgery (CSRF) : exploitation d'un CSRF (requête HTTP GET et POST), contre-mesures
- Injection SQL : injection dans un SELECT, dans un INSERT, dans un UPDATE, dans un DELETE, technique d'exploitation
  - UNION, technique d'exploitation
  - Injections booléennes, technique d'exploitation
  - Injection dans les messages d'erreurs, technique d'exploitation
  - Injection par délais, technique d'exploitation
  - Injection dans des fichiers, exemple d'utilisation avec SQLMap, contre-mesures
- Injection de commandes : chainage de commandes, options des commandes, exploitation, exemple d'exploitation avec commix, contre-mesures
- Service Side Includes (SSI) : exemples d'attaques, contre-mesures
- Injection d'objet : exploitation, contre-mesures
- Inclusion de fichier : inclusion de fichiers locaux (LFI), inclusion de fichiers distants (RFI), contre-mesures
- Envoi de fichier (Upload) : exploitation basique, vérification de content-type, blocage des extensions dangereuses, contre-mesures
- XML External Entity (XXE) : les entités (entités générales, paramètres, caractères et externes), découverte de la vulnérabilité, exploitation de la vulnérabilité, contre-mesures
- Service Side Template Injection (SSTI) : exemple d'utilisation de Twig, exemple d'exploitation sur Twig, exemple d'exploitation sur Flask, contre-mesures

6 - Challenge final
- Mise en situation d'audit d'une application Web

Réf. SE109
3 jours
(21h présentiel)

2 250 €HT

PARIS
13/06, 21/11

Autres sites, nous consulter

+ de 3000 missions réalisées chaque année

Un projet de formation sur-mesure ?

Vous devez former plusieurs collaborateurs sur une même thématique ou une même technologie et vous souhaitez pour cela organiser une formation en intra-entreprise ?

Qu'il s'agisse de décliner les programmes présentés dans notre catalogue ou de concevoir un dispositif sur-mesure, nos équipes sont à votre entière disposition pour vous accompagner dans votre projet.

Après une analyse de vos besoins, elles apporteront à votre demande la réponse pédagogique, technique et logistique la plus pertinente.

Contactez nos Conseillers Formation au 0 825 07 6000

Sécurité des applications et des serveurs web

Sécurisez vos sites Internet et Intranet

ACCESSIBLE À DISTANCE

Avec Internet, les réseaux sont dorénavant ouverts et par conséquent, beaucoup plus exposés aux attaques virales ou autres actes de piratage. Il est donc primordial de savoir faire face à ces différents risques pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information. L'objectif de cette formation est de permettre aux participants d'identifier les risques liés à internet puis de comprendre comment sécuriser les serveurs web, les applicatifs et les données associés en recourant aux méthodes et technologies ad hoc.

OBJECTIFS

- Évaluer les risques internes et externes liés à l'utilisation d'Internet
- Identifier les différentes solutions pour mettre en œuvre la sécurité d'un serveur Web
- Comprendre comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
- Être capable de mettre en œuvre une politique de sécurité fiable sur un serveur Apache ou IIS

Public

- Responsable sécurité
- Chef de projets
- Développeur Web
- Administrateur de serveur Web

Pré-requis

Connaissance en administration Unix
Connaissance des réseaux et protocoles TCP/IP

Les + de cette formation

- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- Une formation qui accorde une large place à la mise en œuvre concrète des acquis à travers la réalisation d'une série d'ateliers amenant les participants à assurer la sécurité d'un serveur Web.

Programme

1 - Introduction au protocole HTTP
- Format des requêtes
- Mécanismes d'authentification HTTP
- Génération de requêtes HTTP
- Découverte passive d'informations
- HTTP : protocole de transport

2 - Introduction au protocole HTTPS
- Généralités
- Authentification par certificats X.509
- Méthodes d'audit HTTPS
- Historique des failles de sécurité

3 - Qualité des développements Web
- Erreurs classiques
- Classification OWASP : exemples, démonstrations
- Injections : exemple avec SQL
- XSS (Injection croisée de code)

4 - Apache
- Présentation du serveur phare du marché Web
- Sécurisation d'un serveur Apache
- Mettre en place https avec mod_ssl
- Apache en relais-inverse
- Relayage applicatif avec mod_proxy/mod_rewrite
- Filtrage applicatif avec mod_security
- Application à l'intégration Apache / Tomcat

5 - Internet Information Services (IIS)
- Architecture
- Installation
- Sécurisation
- Outils
- HTTPS

Réf. SR212
3 jours
(21h présentiel)

2 075 €HT

À DISTANCE
18/07, 02/11
PARIS
19/09

Autres sites, nous consulter

Sécurité des applications Web Java EE

Identifier les risques et savoir choisir les solutions de sécurisation

ACCESSIBLE À DISTANCE

Avec le développement de services en ligne BtoB et BtoC (consultation d'historiques de consommation par exemple), les entreprises sont de plus en plus nombreuses à exposer des données sur la toile par le biais de serveurs Web. Si certaines de ces données ne revêtent pas une dimension stratégique, il apparait néanmoins indispensable d'en assurer la sécurité, ne serait-ce qu'au regard de la loi. Aussi, sécuriser une application web ainsi que les données auxquelles elle donne accès doit-il devenir un réflexe. Les participants à cette formation de 3 jours découvriront les techniques et bonnes pratiques pour assurer la sécurité des applications développées en Java et hébergées sur des serveurs Web, mais également la sécurité liée à la JVM et proche du cœur des systèmes.

OBJECTIFS

- Connaître les risques potentiels dans l'utilisation de Java
- Identifier les parades à mettre en œuvre, les moyens de sécuriser les applications JEE
- Apprendre à sécuriser les différents aspects techniques d'une application
- Être capable de tester la sécurité des applications Java

Public

- Développeurs et analystes programmeurs "anciennes technologies"
- Chefs de projets

Pré-requis

Connaître les notions de base du langage Java est nécessaire pour suivre cette formation dans de bonnes conditions

Les + de cette formation

- Une vision objective des risques liés à Java.
- Un panorama détaillé des solutions en local (JVM) et en mode Web.
- La mise en œuvre très technique et pratique des solutions à travers une série d'ateliers.

Programme

1 - Introduction
- Les risques
- Politique de sécurité
- Évaluation des risques en fonction des différents modes d'utilisation de Java (applets, application, servlets)

2 - Sécurisation de la JVM
- Limites naturelles imposées par Java
- Gestion mémoire
- Contrôle du bytecode par la machine virtuelle

3 - Protection de l'exécution
- Exécution protégée
- Security Manager, ClassLoader
- Surcharge des méthodes d'accès
- Lecture, écriture, exécution, ouverture de socket
- Autorisation de connexions...

4 - Chiffrement
- Les mécanismes de signature
- Création de clés publiques et privées
- Les clés RSA, DSA
- Signature d'un document
- Les algorithmes SHA1withDSA, MD5withRSA
- Les MessageDigest
- Les algorithmes MD2, MD5, SHA-1, SHA-512

5 - Certificats
- Cycle de vie d'un certificat
- La fabrique de certificats Java
- Les certificats de modification X509

6 - Contrôle
- Rappel sur les ACL
- Le paquetage java.security.acl
- Ajout d'entrée, vérification d'accès

7 - Obfuscation
- Principe
- Techniques d'obfuscation
- Solutions commerciales

8 - JAAS et sécurité JEE
- Présentation
- Fonctionnement et mise en œuvre
- Le service de sécurité
- Sécurité Web et EJB
- Autorisations EJB V3
- Accès applicatifs et lien avec un annuaire LDAP

Réf. OB394
3 jours
(21h présentiel)

1 830 €HT

À DISTANCE Autres sites, nous consulter
07/11

Le learning hub ib

Vous êtes inscrit à une formation mixte ib ?
Retrouvez sur le Learning Hub l'ensemble des activités digitales intégrées à votre parcours (quiz, vidéocasts, modules e-learning,...).

Avec le Learning Hub, confortez vos pré-requis grâce à des quiz pédagogiques, des vidéos ou des modules e-learning, testez vos acquis et approfondissez les sujets de votre choix avec nos quiz post-formation et nos vidéocasts. Consultez enfin nos vidéos-tutos pour bénéficier de l'accompagnement de nos experts dans la mise en œuvre de vos nouveaux savoirs.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Sécurité des applications

Mettre en œuvre les règles et bonnes pratiques liées au développement sécurisé d'applications

ACCESSIBLE À DISTANCE

Les applications web sont de plus en plus exposées aux tentatives de piratages. La sécurisation d'une application et des données qu'elle véhicule fait dorénavant partie intégrante de tout nouveau projet de développement. Tous les acteurs IT ont pris conscience de cette nécessité et intègrent dans leurs solutions des éléments et des outils offrant un niveau de sécurisation à la hauteur des enjeux et attentes du marché. Durant cette formation de 3 jours, les participants aborderont dans le détail chaque brique de sécurisation qu'il est possible de considérer et s'approprieront les techniques à employer pour renforcer la sécurité de leurs prochaines applications.

OBJECTIFS

- Comprendre les problématiques de sécurité des applications
- Connaitre les principales menaces et vulnérabilité
- Appréhender les méthodologies / technologies de protection et de contrôle de la sécurité des applications
- Mettre en place une stratégie de veille

Public

- Architectes
- Développeurs
- Analystes
- Chefs de projets...

Pré-requis

Disposer d'une bonne connaissance de la programmation objet et de la programmation d'applications Web

Les + de cette formation

- Au-delà des apports théoriques indispensables, cette formation intègre de nombreux ateliers qui apporteront aux participants une expérience pratique de la sécurisation d'applications.
- Des conseils pratiques et méthodologiques sont proposés pour chaque thème évoqué.

Programme

1 - Sécurité dans le framework et du code
- Concepts fondamentaux
- Sécurité d'accès du code et des ressources
- Sécurité basée sur les rôles
- Le principe du W^X
- Services de chiffrement
- Validation et contrôle des entrées / sorties
- Gestion et masquage d'erreurs
- Gestion sécurisée de la mémoire
- Contrôle d'authenticité et d'intégrité d'une application/d'un code
- Offuscation du code
- Reverse engineering sur : bundle C#, application Java, binaire Windows
- Contrôle des droits avant exécution du code
- Sécuriser les données sensibles présentes dans un binaire
- Stack/Buffer/Heap overflow

2 - Les bases de la cryptographie
- Cryptographie - Les définitions
- Types de chiffrement : chiffrement à clés partagées, chiffrement à clé publique
- Symétrique vs. asymétrique, combinaisons symétrique / asymétrique
- Fonctions de hachage
- Utilisation des sels
- Signatures numériques, processus de signature, processus de vérification

3 - Chiffrement, hash et signature des données
- Cryptographie Service Providers (CSP)
- System, security, cryptographie
- Choix des algorithmes de chiffrement
- Chiffrement symétrique : algorithme (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)
- Algorithmes asymétriques
- Algorithme : RSA, DSA, GPG
- Algorithme de hachage : MD5, SHA1 / SHA2 / SH3

4 - Vue d'ensemble d'une infrastructure à clé publique (PKI)
- Certificat numérique : certificat X.509
- PKI - Les définitions
- Les fonctions PKI
- PKI - Les composants
- PKI - Le fonctionnement
- Applications de PKI : SSL, VPN, IPSec
- IPSec et SSL en entreprise
- Smart Cards (cartes intelligentes)
- Autorité de certification

5 - SSL et certificat de serveur
- Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

6 - Utilisation de SSL et des certificats clients
- Certificats clients
- Fonctionnement de SSL : phase I, II, III et IV
- Vérification de la couverture d'utilisation d'un certificat (lors du handshake)
- Vérification des dates d'utilisation d'un certificat

7 - Sécurité des services Web
- Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité
- Limitations liées à SSL
- Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP / REST

8 - Jetons de sécurité
- Jetons de sécurité : User-Name Token, Binary Token, XML Token, JWT (JSON Web Tokens), Session-based Token
- Intégrité d'un jeton (MAC / HMAC)
- Cycle de vie d'un jeton, expiration automatique (ou pas), contexte d'utilisation d'un jeton
- Habilitations suivant le contexte du jeton
- Certificats X.509
- Signature des messages SOAP / REST : création d'un jeton de sécurité, vérification des messages (MAC / HMAC), chiffrement des messages, déchiffrement du message

9 - Sécurité et développement Web
- Classification des attaques : STRIDE, OWASP
- Les erreurs classiques
- Authentification par jeton et gestion des habilitations
- Les handlers et méthodes HTTP
- Séparation des handlers par contexte de sécurité
- Attaque par injection
- Injection HTML
- Injection CSS
- Injection JS
- Injection SQL
- XSS (Injection croisée de code) : XSS réfléchi, XSS stocké
- XSS Cookie Stealer
- CSRF : Cross-Site Request Forgery

10 - Organiser la veille
- Top 10 de l'OWASP
- Le système CVE
- Le système CWE

Réf. DEV303
3 jours
(21h présentiel)

1 990 €HT
Offerte

À DISTANCE
27/06, 19/09, 05/12
Autres sites, nous consulter

PARIS
27/06, 19/09, 05/12

Recherche et exploitation de vulnérabilités sur applications Android

Techniques et méthodes de recherche de vulnérabilités sur les applications Android

Avec Android, Google détient 80% du marché des OS mobiles. Cette situation fait d'Android une cible de choix pour des acteurs malintentionnés qui n'hésitent pas à placer des codes malveillants au sein d'applications. Si Google fait son possible pour protéger au mieux les utilisateurs d'Android en éradiquant les applications potentiellement dangereuses de Play Store, il doit continuellement faire face à une ingéniosité sans limites des développeurs toujours en quête de nouvelles failles à exploiter. A travers un cas pratique proche d'une situation réelle, les participants à cette formation seront placés en situation de mener un audit de sécurité durant lequel ils découvriront l'organisation et les procédures à respecter et seront amenés à mettre en œuvre différentes techniques pour analyser la sécurité d'une application Android.

OBJECTIFS

- Être capable de maîtriser les fonctionnalités avancées du système Android
- Savoir organiser une procédure d'audit de sécurité de type test de pénétration sur une application mobile Android
- Se mettre en situation réelle d'audit

Public

- Ingénieurs / Techniciens
- Responsables techniques
- Consultants sécurité

Pré-requis

Connaissances en Web
Connaissances en sécurité

Les + de cette formation

- Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiques.
- Les participants apprendront à mettre en place une véritable procédure d'audit de type PenTest ou Test d'Intrusion sur une application mobile Android.
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - Introduction au système Android
- Modèle de sécurité d'Android
- Permissions
- Anatomie d'une application
- Manifeste d'application
- Activités et Intents
- Utilisation de Content Providers
- Stockage de fichiers sur carte SD

2 - Présentation des outils d'analyse
- Le SDK Android
- ADB (Android Debug Bridge)
- JADX
- Drozer

3 - Préparation à l'analyse
- Installation du SDK
- Déploiement d'une autorité de certification sur Burp Suite

4 - Prise d'information
- Découverte de l'activité principale
- Récupération d'informations concernant l'API utilisée
- Récupération d'informations depuis les fichiers de logs

5 - Attaque de l'API
- Cross-Site Scripting
- Injection de code SQL
- Isolation de comptes utilisateur
- Chiffrement des communications
- Gestion des sessions

6 - Reverse Engineering
- Analyse statique via JADX
- Récupération des points d'entrée de l'API
- Analyse des algorithmes de chiffrement utilisés
- Emplacement de stockage des données (local, carte SD)
- Type de données stockées
- Mots de passe présents dans le code source
- Utilisation d'intents en broadcast

Réf. SE111
3 jours
(21h présentiel)

2 600 €HT

PARIS
05/09, 28/11

Autres sites, nous consulter

L'aide au recrutement avec la POE (Préparation Opérationnelle à l'Emploi)

Vous rencontrez des difficultés pour recruter des collaborateurs dont les profils et les compétences sont en adéquation avec vos besoins ?

ib vous propose un dispositif complet qui répond précisément à cette problématique. En associant pré-recrutement et formation préalable à l'embauche, ib vous propose une solution clé en main qui vous permettra d'intégrer des collaborateurs immédiatement opérationnels sur des métiers en tension.

A travers notre dispositif qui associe aux avantages liés à la POEI des services à forte valeur ajoutée, nous apportons une réponse efficace aux problèmes de pénuries de compétences et d'employabilité auxquels sont aujourd'hui confrontées les entreprises.

Pour en savoir plus, contactez-nous au 0 825 07 6000

Sécurité des appareils et des applications mobiles

La sécurité de la mobilité informatique de bout en bout

SÉMINAIRE

ACCESSIBLE À DISTANCE

L'apparition des tablettes et des smartphones dont l'utilisation va toujours croissante, y compris en environnement professionnel, conduit les entreprises à s'adapter à de nouveaux besoins mais aussi à de nouvelles contraintes. Et effectivement, si les déploiements de solutions mobiles sont souvent relativement indolores, donc finalement assez rapides, il ne faut pas pour autant, dans la précipitation, négliger l'étape vitale de la sécurité dont dépendra le bon fonctionnement des appareils et des applications. Après avoir mis l'emphase sur les vulnérabilités des plates-formes et des applications mobiles, ce séminaire proposera un état des lieux des technologies et solutions de sécurité disponibles sur le marché.

OBJECTIFS

- **Identifier les points de vulnérabilité des solutions de mobilité, de bout en bout**
- **Disposer d'une vision d'ensemble des technologies et des solutions déployées pour protéger les plates-formes et les applications mobiles**
- **Être en mesure de comprendre la sécurité des usages privés et professionnels dans le cadre du BYOD**
- **Connaître les métriques et critères de sélection des solutions**

Public

- Responsables informatiques, consultants généralistes
- Directeurs et managers du SI souhaitant découvrir les nouvelles possibilités sur le champ de la mobilité
- Toute personne amenée à réaliser des choix techniques de solutions de sécurité des plates-formes terminales et des applications mobiles

Pré-requis

Ce séminaire nécessite une connaissance sommaire de l'informatique

Les + de ce séminaire

- Une emphase particulière est mise sur les aspects à prendre en compte pour garantir la sécurité des données de l'entreprise.
- Les retours d'expérience d'un consultant spécialiste de la sécurité et de la mobilité.
- Le discours du séminaire est illustré de nombreux exemples concrets.

Réf. SR238
2 jours
(14h présentiel)

1 730 €HT
Offerte

À DISTANCE	16/06, 24/11
PARIS	16/06, 24/11

Autres sites, nous consulter

Programme

1 - Identification de vulnérabilités des plates-formes mobiles
- Caractéristiques techniques et vulnérabilités des tablettes et Smartphones
- Risques d'escalade de privilège (Jailbreak et Rooting)
- Attaques d'Operating System (iOS, Android, Windows Phone)
- Niveaux d'attaque d'une solution de mobilité : plate-forme terminale, applications, réseaux mobiles, donnée (contenu)

2 - Panorama des fournisseurs majeurs de solutions de sécurité (MDM, MCM, MAM...)
- Airwatch, Good Technology, MobileIron
- Citrix XenMobile, IBM, Microsoft, SAP/Afiria
- Vision et capacité opérationnelle des acteurs dans un marché en développement
- Commercialisation : appliance-serveur privé et Cloud SaaS des solutions de sécurité

3 - Sécurité par la gestion des appareils mobiles (MDM)
- Description des caractéristiques communes des solutions MDM (Mobile Device Management) : prise en main à distance, géolocalisation des terminaux, vérification de conformité....
- Utilisation limitée aux zones géographiques (exemple de solution)
- Renforcement des couches logicielles (SE Android) et création de la Trust Zone (étanchéité)
- Suivi de consommation
- Accès de l'utilisateur au terminal
- Métriques et critères essentiels de sélection des solutions

4 - Sécurité par la gestion des applications (MAM)
- Description des caractéristiques communes des solutions MAM (Mobile Application Management) : mise à jour automatique des applications, installation interdite des Apps....
- Isolation par les containers
- Apps Stores privés et autorisés : intégration des applications de l'écosystème par des API et connecteurs
- Séparation des interactions entre les applications du terminal et du serveur
- Métriques de qualité et critères principaux de choix

5 - Sécurité par la gestion des contenus et données (MCM)
- Définition du MCM (Mobile Content Management)
- Sécurité contre les fuites des données (DLP)
- Sécurité par la surveillance des activités (SIEM)
- Encryptions gérées des données (On Device Encryption FIPS 140-2 (AES))
- Cloud de stockage sécurisé et partagé pour les mobiles

6 - Sécurité des terminaux mobiles personnels utilisés dans le cadre professionnel (BYOD)
- Définition du concept BYOD (Bring Your Own Device)
- Isolation par la virtualisation du terminal associée aux MDM et MAM
- Sécurité par la responsabilisation : fixation d'un cadre légal d'utilisation (chartre d'utilisation, confidentialité CNIL...)

7 - Sécurité de la connectivité des terminaux aux serveurs d'applications
- Solutions existantes : VPN SSL, Firewall
- Authentification d'accès aux réseaux : NAC et RBAC
- Sécurité selon les types de réseaux GSM/4G et WiFi et les lieux de connexion

8 - Impacts et grandes tendances
- Banalisation et abstraction des plates-formes terminales mobiles
- Convergence des solutions mobiles et traditionnelles "fixes"
- Refonte des dispositifs de sécurité actuels

Toutes nos formations en détail sur...

www.ib-formation.fr

Avis de l'expert, parcours pédagogiques, publics, dates, ...
tout ce qu'il faut savoir sur nos formations est sur notre site.
Découvrez également nos tests de pré-requis en ligne et nos conseils pour aller plus loin dans l'expertise.

Durcissement des systèmes

Améliorer la sécurité des systèmes

ACCESSIBLE À DISTANCE

Avec des environnements de plus en plus connectés, le risque d'attaques s'accentue... Comment dès lors minimiser ces risques sur les équipements informatiques de l'entreprise ? L'application de diverses techniques de durcissement de systèmes (ou Hardening en anglais), plus ou moins complexes à mettre en œuvre, comme par exemple restreindre l'accès aux réseaux Wifi ou encore cloisonner les machines, permet de répondre à ce besoin. A l'issue de cette formation de 3 jours, les participants auront acquis les connaissances et compétences nécessaires au durcissement des systèmes Linux et Windows.

OBJECTIFS

- **Comprendre l'intérêt des techniques de durcissement systèmes et réseau**
- **Maîtriser les différentes techniques de durcissement des systèmes Linux et Windows**
- **Être capable de protéger les systèmes de l'entreprise contre des vulnérabilités non publiées**

Public

- Administrateurs systèmes et réseaux

Pré-requis

Disposer de connaissances en administration système Windows et Linux

Les + de cette formation

- Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiques.
- Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).
- Les retours d'expériences de professionnels de la sécurité.

Programme

1 - Introduction générale sur la sécurité informatique

- Mise en place d'un atelier de machines Linux/Windows vulnérables et à durcir
- Cartographie d'un système d'information : identification de la topologie réseau
- Cartographie d'un système d'information : identifier les machines accessibles avec NMap
- Cartographie d'un système d'information : identifier les machines affectées par des vulnérabilités connues
- Faire une veille sur les vulnérabilités connues
- Durcissement réseau : restreindre l'accès à un réseau filaire ou sans-fil
- Durcissement réseau : cloisonner les machines
- Durcissement réseau : masquer une machine et ses services avec un pare-feu

2 - Durcissement de machines Windows

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles sur Windows
- Définir une politique de mises à jour sur les produits Microsoft
- Surveiller les mises à jour de sécurité des produits non-Microsoft
- Restreindre l'accès distant au parc Windows
- Mise en place d'alertes de sécurité sur le parc Windows
- Utilisation du pare-feu Windows
- Utilisation d'un anti-virus sur Windows
- Restreindre l'exécution des applications
- Utiliser les politiques de groupes (GPO)
- Auditer les politiques de groupes (GPO) avec Microsoft Security Compliance Manager
- Protection physique (clés USB, BIOS...)

3 - Durcissement de machines Linux

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles sur Linux
- Définir une politique de mises du noyau Linux
- Définir une politique de mises à jour des applicatifs tiers sur Linux
- Restreindre l'accès distant au parc Linux
- Mise en place d'alertes de sécurité sur le parc Linux avec OSSEC
- Utilisation du pare-feu Linux
- Utilisation d'un anti-virus sur Linux
- Restreindre l'exécution des applications et des commandes sur Linux
- Auditer les configurations avec Lynis

Réf. **SE011**
3 jours
(21h présentiel)

**ORGANISÉ SUR DEMANDE,
NOUS CONSULTER**

Pour vous inscrire à une formation... il y a toujours un moyen de nous contacter

Par téléphone

Nos Conseillers Formation sont joignables de 8h30 à 18h00 au 0 825 07 6000. Ils répondront à toutes vos questions concernant les formations, les dates de sessions, les opportunités de dernière minute...

Par e-mail

Une adresse unique : espace.clients@ib.cegos.fr pour toutes vos inscriptions ou demandes de renseignements.

Par Internet

Retrouvez sur www.ib-formation.fr l'intégralité de nos programmes ainsi que toutes les informations qui vous seront utiles : dates de sessions, plans d'accès, offres de dernière minute, informations sur les évènements ib....

Détection, identification et éradication de Malwares

Les bases de l'analyse de malwares sous Windows

Conçus dans un but bien précis, comme par exemple utiliser les ressources de l'ordinateur pour miner des crypto-monnaies ou encore rançonner l'entreprise en rendant inaccessibles ses données, les logiciels malveillants (ou malwares) font peser une lourde menace sur les organisations. Les participants à cette formation de 3 jours apprendront à distinguer les grandes familles de malwares et leurs techniques d'infection, de propagation et de persistance. Ils apprendront à réaliser des analyses avancées pour les détecter puis à s'en protéger et à les éradiquer.

OBJECTIFS

- Connaître les différents types de malwares
- Être capable d'identifier un malware
- Comprendre comment mettre en œuvre des contre-mesures adéquates
- Apprendre à manier les outils d'inspection du système

Public

- Responsables gestion incident
- Techniciens réponse incident
- Auditeurs techniques
- Analystes de sécurité

Pré-requis

Connaissances du système Microsoft Windows

Les + de cette formation

- Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation, et mis en pratique lors des travaux dirigés.
- Les nombreux travaux pratiques (50% du temps de la formation) favorisent une mise en œuvre rapide et simplifiée des nouveaux acquis.
- Les conseils et partages de bonnes pratiques de consultants expérimentés.

Programme

1 - Introduction aux malwares
- Virus
- Vers
- Botnet
- Rançongiciels
- Rootkits (userland – kernel-land)
- Bootkit

2 - Eradication réponse à incident
- Processus inforensique et analyste de logiciels malveillants
- Réponse à incident automatisée sur un parc

3 - Détection
- Les anti-virus et leurs limites
- Chercher des informations sur un malware
- NIDS / HIDS
- EDR
- Concept d'IOC dans le cadre d'un SOC / CERT (hash, motifs, etc..)

4 - Identification
- Analyse dynamique manuelle
- Analyse dynamique automatisée (sandboxes)
- Analyse statique basique
- Introduction à l'analyse mémoire avec Volatility
- Introduction à la rétro-conception

Réf. SE110
3 jours
(21h présentiel)

2 290 €HT

PARIS	Autres sites, nous consulter
22/08	

CURSUS MÉTIER C

30 Cursus Métier à découvrir

Pour vous permettre de disposer d'équipes toujours plus polyvalentes et rapidement opérationnelles, ib vous propose des cursus adaptés à leur évolution vers de nouveaux domaines de compétences. Étudiés pour favoriser une acquisition rapide de nouveaux savoirs, nos cursus métier couvrent les thématiques actuellement au cœur des préoccupations des entreprises.

Retrouvez tous nos Cursus Métier sur www.ib-formation.fr

Gestion des identités avec Windows Server 2016

Annuaire, infrastructure à clé publique et fédération d'identité

ACCESSIBLE À DISTANCE

FORMATION MIXTE

Depuis Windows 2000, l'identification et l'authentification des utilisateurs et des ordinateurs reposent sur un annuaire LDAP connu sous le nom d'Active Directory. Avec l'émergence des technologies cloud, tout spécialement en mode hybride, la gestion des identités prend une dimension nouvelle qui dépasse souvent les limites de l'entreprise. Cette formation rassemble toutes les informations nécessaires aussi bien pour la gestion des identités internes que pour leur intégration à un environnement plus vaste incluant clients et/ou fournisseurs.

OBJECTIFS

- Savoir installer et configurer des contrôleurs de domaine
- Être capable de mettre en œuvre et de sécuriser AD DS dans des environnements complexes et de le synchroniser avec Azure AD
- Savoir créer les GPO et les utiliser pour définir les paramètres utilisateur
- Comprendre comment créer et gérer les GPO et savoir les utiliser pour définir les paramètres utilisateur
- Pouvoir mettre en place et administrer une hiérarchie d'autorités de certification avec AD CS (Active Directory Domain Services)
- Disposer des connaissances nécessaires à la mise en œuvre et à l'administration d'AD FS et d'AD RMS
- Pouvoir assurer la surveillance, le dépannage et la disponibilité des services AD DS

Public

- Professionnels ayant une certaine expérience de AD DS souhaitant découvrir les fonctionnalités de gestion d'identités et de contrôle des accès disponibles sous Windows Server 2016
- Administrateurs système ou infrastructure souhaitant étendre leur domaine de compétence

Pré-requis

Posséder une expérience pratique des concepts et technologies AD DS, de Windows Server 2012 ou 2016 et de Windows 7, 8 ou 10

Connaissances des technologies réseaux telles que l'adressage IP, la résolution de noms et DHCP

Connaissances de Microsoft Hyper-V et des concepts de base des serveurs de virtualisation

Connaissance des meilleures pratiques de sécurité

Expérience de base avec l'interface de ligne de commande Windows PowerShell

Les + de cette formation

- Une formation rythmée durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- La richesse des ateliers favorise l'assimilation des points abordés au cours des 5 journées de formation.
- Les contenus digitaux mis à disposition des participants avant et après la formation renforcent l'efficacité pédagogique du programme et garantissent un bénéfice durable de l'action de formation.

Programme

1 Avant le présentiel

Pour aborder la formation dans les meilleures conditions, retrouvez sur le Learning Hub ib :

- Un quiz de consolidation des pré-requis

2 En présentiel

1 - Installation et configuration des contrôleurs de domaine

- Généralités sur AD DS
- Le rôle de contrôleur de domaine
- Déploiement des contrôleurs de domaine

2 - Gestion des objets AD DS

- Comptes d'utilisateur
- Comptes de groupe
- Comptes d'ordinateur
- Utilisation de PowerShell pour l'administration d'AD DS
- Structure et gestion des unités d'organisation

3 - Infrastructure AD DS avancée

- Introduction
- Déploiement en environnement complexe
- Relations d'approbation

4 - Sites et réplication

- Description de la réplication AD DS
- Configuration des sites
- Configuration et surveillance de la réplication AD DS

5 - Stratégie de groupe

- Introduction
- Création et administration des objets de stratégie de groupe (GPO – Group Policy Objects)
- Périmètre d'applicabilité et modalités de traitement des GPO
- Dépannage

6 - Paramétrage de l'environnement utilisateur par GPO

- Modèles d'administration
- Redirection de dossiers et scripts
- Préférences

7 - Sécurisation d'AD DS

- Sécurisation des contrôleurs de domaine
- Mise en place d'une politique de sécurisation des comptes
- Audit de l'authentification
- Configuration de comptes de services gérés (MSA – Managed Service Accounts)

8 - Déploiement et administration d'AD CS (Active Directory Certificate Services)

- Déploiement des autorités de certification
- Administration des autorités de certification
- Dépannage et maintenance des autorités de certifications

9 - Déploiement et administration des certificats

- Modèles de certificat
- Déploiement, révocation et récupération de certificats
- Utilisation de certificats en environnement commercial
- Mise en œuvre et administration de cartes à puce

10 - Mise en œuvre et administration d'AD FS (Active Directory Federation Services)

- Présentation d'AD FS
- Prérequis et planification
- Déploiement et configuration
- Web Application Proxy

11 - Mise en œuvre et administration d'AD RMS (Active Directory Rights Management Services)

- Introduction
- Déploiement et gestion de l'infrastructure
- Protection des documents

12 - Synchronisation AD DS – Azure AD

- Préparation
- Mise en place de la synchronisation avec Azure AD Connect
- Gestion des identités

13 - Surveillance, maintenance et dépannaged'AD DS

- Surveillance d'AD DS
- Maintenance de la base de données AD DS
- Récupération d'objets AD DS

3 Après le présentiel

Retrouvez sur le Learning Hub ib :

- Un quiz pédagogique pour évaluer vos acquis et approfondir les sujets de votre choix
- Des vidéocasts pour revenir sur les points clés de la formation
- Des vidéos-tutos pour vous accompagner dans la mise en œuvre de vos acquis

Réf. **M20742**

5 jours

(35h présentiel)

2 920 €HT

Offerte

À DISTANCE	BORDEAUX	NANTES	SOPHIA ANTIPOLIS
18/07, 19/09, 12/12	14/11	27/06, 14/11	26/09
PARIS	**LILLE**	**RENNES**	**STRASBOURG**
18/07, 19/09, 12/12	04/07, 21/11	27/06, 14/11	14/11
AIX-EN-PROVENCE	**LYON**	**ROUEN**	**TOULOUSE**
26/09	13/06, 24/10	19/09	21/11

Windows Server 2016 - Assurer la sécurité de l'infrastructure

ACCESSIBLE À DISTANCE

Construire une infrastructure sécurisée à tous les niveaux

Cette formation propose un tour d'horizon complet de l'arsenal des outils disponibles pour assurer la sécurité des environnements Windows. Pour une efficacité maximale des contre-mesures, l'approche adoptée est la suivante : on considère que des intrusions ont déjà eu lieu et qu'il importe de limiter les dégâts d'une part en protégeant les identifiants utilisés pour l'administration et d'autre part en s'assurant que les administrateurs ne peuvent effectuer que les tâches qui leur sont assignées, et ce uniquement lorsque nécessaire.

OBJECTIFS

- Être en mesure d'assurer la sécurité des systèmes Windows Server
- Comprendre comment assurer la sécurité des infrastructures de développement et de production
- Apprendre à configurer et mettre en œuvre l'administration "Just In Time"
- Disposer des connaissances nécessaires pour assurer la sécurité des données
- Savoir configurer le pare-feu Windows et les pare-feux distribués
- Être capable de sécuriser le trafic réseau et de parer les attaques
- Apprendre à sécuriser l'infrastructure de virtualisation
- Prendre en compte les menaces liées aux logiciels malfaisants

Public

- Ingénieurs système et réseau opérant dans des environnements Windows complexes, comportant notamment des accès Cloud et Internet

Pré-requis

Avoir suivi les formations "Installation de Windows Server 2016, gestion du stockage et de la virtualisation" (M20740), "Les services réseaux Windows Server 2016 (M20741) et "Gestion des identités avec Windows Server 2016" (M20742) ou connaissances équivalentes
Posséder une solide expérience sur les réseaux (TCP/IP, UDP, DNS...), les principes AD DS, la virtualisation Hyper-V et la sécurité Windows Server

Les + de cette formation

- Les nombreux travaux pratiques qui ponctuent la formation permettent aux participants de mettre immédiatement en application leurs acquis.
- Les conseils et bonnes pratiques pour assurer la sécurité du nouveau système d'exploitation serveur de Microsoft.
- Les retours d'expérience de formateurs spécialistes de la sécurité des systèmes Windows.

Programme

1 - Détection des intrusions avec les outils Sysinternals
- Généralités
- Les outils Sysinternals

2 - Protection des identifiants et des accès privilégiés
- Droits utilisateur
- Comptes d'ordinateur et comptes de service
- Protection des identifiants
- Stations dédiées et serveurs intermédiaires
- Déploiement d'une solution de gestion des mots de passe d'administrateur local

3 - Limitation des droits d'administration et principe du privilège minimal
- Description
- Implémentation et déploiement

4 - Gestion des accès privilégiés et forêts administrative
- Le concept de forêt administrative
- Introduction à Microsoft Identity Manager
- Administration "Just In Time" et gestion des accès privilégiés avec Microsoft Identity Manager

5 - Atténuation des risques liés aux logiciels malfaisants
- Configuration et gestion de Microsoft Defender
- Stratégies de restrictions logicielles et AppLocker
- Configuration et utilisation de Device Guard
- Utilisation et déploiement de Enhanced Mitigation Experience Toolkit

6 - Méthodes d'analyse et d'audit avancées pour la surveillance de l'activité
- Introduction : l'audit système
- Stratégies d'audit avancées
- Audit et enregistrement des sessions PowerShell

7 - Analyse de l'activité avec Microsoft Advanced Threat Analytics et Operations Management Suite
- Advanced Threat Analytics
- Présentation de OMS

8 - Sécurisation de l'infrastructure de virtualisation
- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

9 - Sécurisation de l'infrastructure de développement applicatif et de production
- Security Compliance Manager
- Nano Server
- Containers

10 - Protection des données par chiffrement
- Planification et implémentation du chiffrement EFS (Encrypting File System)
- Planification et implémentation de BitLocker

11 - Limitation des accès aux fichiers
- File Server Resource Manager (FSRM)
- Automatisation de la gestion et de la classification des fichiers
- Contrôle d'accès dynamique (Dynamic Access Control)

12 - Limitation des flux réseaux au moyen de pare-feu
- Le pare-feu Windows
- Pare-feu distribués

13 - Sécurisation du trafic réseau
- Menaces liées au réseau et règles de sécurisation des connexions
- Paramétrage avancé de DNS
- Analyse du trafic réseau avec Microsoft Message Analyzer
- Sécurisation et analyse du trafic SMB

14 - Mise à jour de Windows Server
- Présentation de WSUS
- Déploiement des mises à jour avec WSUS

Réf. M20744
5 jours
(35h présentiel)

2 920 €HT
Offerte

À DISTANCE
10/10, 12/12
PARIS
10/10, 12/12

Autres sites, nous consulter

Le learning hub ib

Vous êtes inscrit à une formation mixte ib ?
Retrouvez sur le Learning Hub l'ensemble des activités digitales intégrées à votre parcours (quiz, vidéocasts, modules e-learning,...).

Avec le Learning Hub, confortez vos pré-requis grâce à des quiz pédagogiques, des vidéos ou des modules e-learning, testez vos acquis et approfondissez les sujets de votre choix avec nos quiz post-formation et nos vidéocasts. Consultez enfin nos vidéos-tutos pour bénéficier de l'accompagnement de nos experts dans la mise en œuvre de vos nouveaux savoirs.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Installer, configurer et protéger des postes de travail Windows 10

Mettre en œuvre la nouvelle génération de postes de travail

ACCESSIBLE À DISTANCE

FORMATION MIXTE

Devant l'accueil mitigé réservé aux différentes versions de Windows 8, le successeur de l'inusable Windows 7, Microsoft semble avoir très largement rectifié le tir avec son nouvel OS client. Rapidement encensé par la presse spécialisée puis par les professionnels de l'informatique, Windows 10 semble ainsi promis à un bel avenir. D'autant plus que cette dernière mouture combine la simplicité d'utilisation des interfaces tactiles avec l'ergonomie éprouvée du PC traditionnel. Cette formation constitue un point d'entrée idéal pour les personnes en charge de la mise en œuvre de Windows 10. A l'issue de ces 5 journées, elles disposeront des compétences nécessaires à la mise en production de postes Windows 10 en environnement professionnel.

OBJECTIFS

- Apprendre à installer et personnaliser des clients Windows
- Être capable de configurer les mises à jour pour Windows
- Comprendre commet configurer les périphériques et les pilotes, le stockage et les paramètres de gestion réseau et à distance dans Windows
- Savoir configurer et gérer les navigateurs et les applications dans Windows
- Pouvoir configurer l'accès au compte et l'authentification, les autorisations de fichiers et de dossiers
- Être capable de décrire les méthodes de sécurisation de l'interface Windows, les menaces courantes et les méthodes permettant de les atténuer
- Apprendre à dépanner les installations de Windows et d'applications
- Pouvoir résoudre les problèmes de matériel et de pilote, les problèmes de fichiers et effectuer des restaurations

Public

- Professionnels IT qui effectuent l'installation, la configuration, la gestion locale générale et la maintenance des services de base windows 10 et ultérieur

Pré-requis

Compréhension de base des réseaux informatiques et des concepts matériels

Compréhension de base des concepts de système d'exploitation et d'application

Expérience de l'utilisation du système d'exploitation Windows

Certification

Cette formation prépare au test MD-100 - Windows Client (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft 365 Certified Modern Desktop Administrator Associate

Les + de cette formation

- Les nombreux travaux pratiques proposés lors de cette formation apportent aux participants une première expérience pratique de l'implémentation et de la gestion de Windows 10.
- Les retours d'expérience de consultants-formateurs experts des systèmes d'exploitation Microsoft.
- Les contenus digitaux mis à disposition des participants avant et après la formation renforcent l'efficacité pédagogique du programme et garantissent un bénéfice durable de l'action de formation.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 Avant le présentiel

Pour aborder la formation dans les meilleures conditions, retrouvez sur le Learning Hub ib :

- Un quiz de consolidation des pré-requis

2 En présentiel

1 - Installation de Windows
- Présentation du client Windows
- Éditions du client Windows et configuration requise
- Méthodes d'installation
- Mise à niveau et migration des clients Windows
- Méthodes de déploiement

2 - Configuration de l'autorisation et de l'authentification
- Authentification
- Gestion des utilisateurs et des groupes
- Configuration du contrôle de compte d'utilisateur
- Mise en œuvre de l'enregistrement des appareils

3 - Configuration et personnalisation post-installation
- Configurer et personnaliser le menu Démarrer de Windows
- Options de configuration courantes
- Méthodes de configuration avancées
- Gestion des pilotes et des périphériques

4 - Mise à jour de Windows
- Modèle de maintenance Windows
- Mise à jour de Windows

5 - Configuration de la mise en réseau
- Configurer la connectivité réseau IP
- Implémenter la résolution de noms
- Mettre en œuvre la connectivité réseau sans-fil
- Vue d'ensemble de l'accès à distance
- Gestion à distance

6 - Configuration du stockage
- Gestion du stockage
- Gestion des disques et des volumes
- Gestion des espaces de stockage

7 - Configuration de l'accès et de l'utilisation des données
- Vue d'ensemble des systèmes de fichiers
- Configuration et gestion de l'accès aux fichiers
- Configuration et gestion des dossiers partagés
- Gestion des fichiers utilisateur

8 - Gestion des applications dans le client Windows
- Fournir des applications aux utilisateurs
- Gestion des applications Windows universelles
- Gestion du navigateur Microsoft Edge

9 - Configuration de la protection contre les menaces et de la sécurité avancée
- Protection contre les logiciels malveillants et les menaces
- Microsoft Defender
- Règles de sécurité de connexion
- Méthodes de protection avancées

10 - Prise en charge de l'environnement Client Windows
- Windows Architecture
- Outils de support et de diagnostic
- Surveillance et dépannage des performances de l'ordinateur

11 - Dépannage des fichiers et des applications
- Récupération de fichiers dans Windows
- Dépannage des applications

12 - Dépannage du système d'exploitation
- Dépannage du démarrage de Windows
- Résolution des problèmes de service du système d'exploitation

13 - Dépannage du matériel et des pilotes
- Dépannage des défaillances du pilote de périphérique
- Vue d'ensemble du dépannage matériel
- Dépannage des défaillances physiques

3 Après le présentiel

Retrouvez sur le Learning Hub ib :

- Un quiz pédagogique pour évaluer vos acquis et approfondir les sujets de votre choix
- Des vidéocasts pour revenir sur les points clés de la formation
- Des vidéos-tutos pour vous accompagner dans la mise en œuvre de Windows 10

Réf. MSMD100

5 jours

(35h présentiel)

2 960 €HT

Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
12/09, 14/11	05/09	
PARIS	**LYON**	
12/09, 14/11	05/09	

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Sécuriser un système Linux

Les techniques de sécurisation d'un système Linux

ACCESSIBLE À DISTANCE

La sécurité informatique est devenue une préoccupation essentielle des entreprises et donc des responsables informatiques. La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique et d'un autre côté, il est souvent très vulnérable compte tenu des nombreuses possibilités de configuration offertes. Cette formation permettra aux participants de découvrir l'ensemble des techniques de sécurisation d'un système Linux.

OBJECTIFS

- Comprendre comment bâtir une sécurité forte autour de Linux
- Savoir mettre en place la sécurité d'une application Linux
- Comprendre les fondamentaux de la sécurité informatique et notamment de la sécurité réseau
- Être capable de sécuriser les échanges réseaux en environnement hétérogène grâce à Linux

Public

- Administrateurs systèmes et réseaux expérimentés

Pré-requis

Avoir suivi les formations "Linux administration niveau 1 - Installation et mise en œuvre" (XW302) et "Linux administration niveau 2 - Gestion et maintenance" (XW303) ou connaissances équivalentes

Certification

Cette formation prépare au test ENI-LINUX (en option au tarif de 180 €) qui permet d'obtenir la certification Certification IT – Administration d'un système Linux

Les + de cette formation

- Le passage en revue des différents aspects de la sécurisation de systèmes Linux.
- En accordant une large place à la pratique, ce programme favorise un ancrage durable et efficace des acquis.
- Le partage des techniques et bonnes pratiques garantissant une mise en œuvre efficace d'une sécurité sur-mesure.

Programme

1 - Les enjeux de la sécurité
- Les attaques, les techniques des hackers
- Panorama des solutions
- La politique de sécurité

2 - La cryptologie ou la science de base de la sécurité
- Les concepts de protocoles et d'algorithmes cryptographiques
- Les algorithmes symétriques et asymétriques (à clé publique), les fonctions de hachage
- La signature numérique, les certificats X-509, la notion de PKI

3 - Les utilisateurs et les droits
- Rappels sur la gestion des utilisateurs et des droits, les ACLs
- La dangerosité des droits d'endossement
- La sécurité de connexion, le paquetage SHADOW

4 - Les bibliothèques PAM
- L'architecture du système PAM, les fichiers de configuration
- L'étude des principaux modules

5 - Le système SELinux ou la sécurité dans le noyau
- L'architecture du système SELinux
- Modifier les règles de comportement des exécutables

6 - Les principaux protocoles cryptographiques en client/serveur
- SSH, le protocole et les commandes ssh
- SSL, l'utilisation de SSL et des certificats X-509 dans Apache et stunnel
- Kerberos et les applications kerbérorérisées

7 - Les pares-feux
- Panorama des techniques pares-feux
- L'architecture Netfilter/Iptables, la notion de chaine, la syntaxe d'iptables
- La bibliothèque tcpd ou l'enveloppe de sécurité, la sécurisation via xinetd
- Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables
- Le proxy SQUID

8 - Les VPN
- Panorama des techniques tunnels et VPN
- Le logiciel OpenVPN

9 - La sécurisation des applications
- Principes généraux
- Sécurisation du Web, d'email, du DNS, du FTP

10 - Les techniques d'audit
- L'audit des systèmes de fichiers avec AIDE et Tripwire
- Les outils d'attaque réseau
- La détection des attaques avec snort

Réf. XW305
4 jours
(28h présentiel)

2 495 €HT

À DISTANCE
17/10

Autres sites, nous consulter

Les implantations

En mettant à votre disposition des équipes commerciales dans chacune de nos agences, nous vous apportons la garantie d'une vraie relation de proximité. Quel que soit votre besoin, vous bénéficiez de l'accompagnement d'experts géographiquement et culturellement proches de vous :

PARIS	LILLE	RENNES	STRASBOURG
AIX-EN-PROVENCE	LYON	ROUEN	TOULOUSE
BORDEAUX	NANTES	SOPHIA-ANTIPOLIS	

IBM AIX - Mise en œuvre des dispositifs de sécurité

Installer et gérer les outils de sécurité AIX

ACCESSIBLE À DISTANCE

OBJECTIFS

- Savoir identifier les risques auxquels sont exposés les systèmes AIX
- Connaître les commandes et les composants AIX permettant de contrer les menaces de sécurité système et réseau
- Savoir configurer IPSEC et LDAP
- Savoir configurer la fonction de sécurité Role Based Access Control (RBAC)
- Être capable de mettre en œuvre les systèmes de fichiers cryptés, le mode Trusted Execution d'AIX, les services sécurisés en utilisant PowerSC et les options d'installation d'AIX

Programme

1 - Caractéristiques de sécurité Aix
2 - Sécurité de base du système Aix
3 - Contrôle d'accès basé sur les rôles
4 - Systèmes de fichiers cryptés
5 - Exécution de confiance
6 - LDAP
7 - Mise en œuvre des fonctionnalités de sécurité lors de l'installation d'Aix

Public

- Administrateurs AIX, administrateurs réseau et responsables sécurité

Pré-requis

Posséder des compétences d'administration réseau et AIX ou avoir suivi la formation "IBM Power Systems pour AIX II - Implémentation et administration d'AIX" (IXU92)

Les + de cette formation

- Une formation pratique : de nombreux exercices pratiques réalisés sur AIX 7 ponctuent chaque module de la formation.
- Les trucs et astuces de formateurs consultants spécialistes de la technologie.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Réf. **IXU97**
3 jours
(21h présentiel)

2 390 €HT

À DISTANCE
28/11

Autres sites, nous consulter

Des équipes à votre écoute

Vous accompagner au quotidien et construire avec vous la solution la plus pertinente implique une organisation flexible, capable de réagir rapidement et efficacement. C'est pourquoi nous avons organisé nos équipes pour apporter des réponses adaptées à chacune de vos problématiques.

- À votre disposition du lundi au vendredi de 8h30 à 18h00, nos Conseillers Formation vous guident dans le choix de vos formations, vous orientent dans vos démarches administratives et répondent à toutes vos sollicitations.
- Nos Ingénieurs Conseil, présents dans chacun de nos centres, apportent des réponses à vos demandes spécifiques et construisent avec vous des solutions adaptées à vos problématiques.
- Notre équipe Grands Projets vous accompagne dans la définition et la mise en œuvre de vos projets stratégiques (grands déploiements, accompagnement du changement...).

Un numéro unique : 0 825 07 6000

IBM z/OS - Sécurité avancée : crypto, réseaux, RACF et votre entreprise

ACCESSIBLE À DISTANCE

Implémenter la sécurité z/OS pour les applications web

IBM a, avec les serveurs System z, implémenté des technologies de pointe, telles que la cryptographie haute-performance, la sécurité sur plusieurs niveaux ou encore une autorité de certification digitale à grande échelle. Cette formation de sécurité avancée z/OS présente l'évolution de l'architecture actuelle de sécurité de z/OS. Elle explore en détail les diverses techniques qui sont mises en place dans les services de cryptographie z/OS, dans Resource Access Control Facility (RACF) z/OS et dans les services intégrés de sécurité z/OS.

OBJECTIFS

- Connaître les composants de la sécurité relatifs au réseau, à la plate-forme et aux transactions sur z/OS
- Savoir expliquer comment RACF supporte les utilisateurs et les groupes Unix
- Comprendre les différences entre les techniques de cryptographie asymétriques et symétriques
- Être capable d'expliquer les bases de WebSphere Application Server ainsi que la sécurité des services Web
- Apprendre à utiliser la commande RACDCERT
- Savoir utiliser le système SSL
- Être en mesure d'expliquer le fonctionnement de l'authentification Kerberos
- Comprendre comment installer, paramétrer et utiliser les z/OS PKI Services

Public

- Programmeurs système z/OS et spécialistes de la sécurité en charge de la conception et de l'implémentation de la sécurité z/OS pour les applications web

Pré-requis

Connaissance générale de z/OS, y compris des connaissances de base sur les services Unix

Posséder une expérience de la configuration des serveurs web sur z/OS

Connaissance de base de TCP/IP et RACF

Les + de cette formation

- Les nombreux ateliers qui accompagnent les différents modules de cette formation garantissent l'acquisition d'un savoir-faire pratique dans la mise en œuvre de la sécurité en environnement z/OS.
- L'expertise de consultants spécialistes de la sécurité.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Programme

1 - Introduction de la sécurité z/OS pour le "On Demand Business"
2 - Plate-forme de sécurité z/OS
3 - Introduction aux certificats digitaux et aux PKI
4 - Le protocole SSL
5 - Serveurs HTTP et Apache, authentification client SSL et sécurité de WebSphere Application Server
6 - RACF et les certificats digitaux
7 - Open Cryptographic Services Facility
8 - Introduction aux fonctionnalités de sécurité de z/OS Communications Server
9 - Vue d'ensemble du système SSL
10 - Connexion sécurisée TN3270
11 - Connexion sécurisée FTP Serveur et client
12 - Vue d'ensemble de la cryptographie : Cryptographiée intégrée System z
13 - Services d'authentification réseau et Enterprise Identity Mapping
14 - LDAP Directory Services dans z/OS et Tivoli Director Server pour z/OS
15 - Introduction à OpenSSH pour z/OS

Réf. SR782
4 jours
(28h présentiel)

3 185 €HT

À DISTANCE
21/06, 25/10

Autres sites, nous consulter

Sécurité du Cloud Computing

Synthèse de la sécurité du Cloud et des nouveaux usages des technologies

SÉMINAIRE

ACCESSIBLE À DISTANCE

Présenté comme un moyen de réduire les coûts et de simplifier la gestion des moyens, le Cloud redessine les usages de l'informatique. Le positionner dans un contexte opérationnel comme la mobilité des employés et l'accès aux ressources informatiques en tout lieu, à tout moment et avec tout type de terminaux, nous permet de mesurer la complexité de son déploiement. Quelle que soit sa nature, privée ou publique, l'adoption du cloud doit s'accompagner de réflexions approfondies sur la sécurité. Ce séminaire s'appuie sur les travaux d'organismes de standardisation et sur un panorama des solutions du marché pour présenter la sécurité du Cloud dans un contexte opérationnel.

OBJECTIFS

- **Comprendre comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud**
- **Connaître les moyens génériques de la sécurité du Cloud**
- **Être en mesure de s'inspirer des solutions et des démarches des opérateurs de Cloud pour sécuriser son approche**
- **Comprendre comment éviter la mise en place d'une sécurité coûteuse et laborieuse pouvant dégrader la performance du réseau global**

Public

- Directeurs du système d'information ou responsables du service informatique souhaitant analyser les risques liés à l'utilisation d'une solution Cloud
- Responsables et chefs de projet en charge de la mise en place d'une politique de sécurité lié à un projet Cloud
- Chefs de projet et toute personne en charge de la sécurité du Cloud Computing

Pré-requis

Ce séminaire nécessite une connaissance sommaire de l'informatique

Les + de ce séminaire

- Ce séminaire offre une synthèse claire des différents moyens pour assurer la sécurité du Cloud.
- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.

Réf. **SR236**
2 jours
(14h présentiel)

1 890 €HT
Offerte

À DISTANCE	13/10
PARIS	13/10

Autres sites, nous consulter

Programme

1 - Introduction
- Rappel des éléments matériels et logiciels de l'architecture Cloud selon les organismes de standardisation NIST (National Institute of Standards and Technology)
- Complexité du contexte de l'utilisation en tout lieu avec tout type de terminaux de connexion

2 - Déceler les points de vulnérabilité du Cloud
- Solutions et architectures du Cloud proposées par des grands acteurs du secteur (OS Cloud, virtualisation, stockage, Datacenter, réseaux…)
- Points de vulnérabilité du terminal d'accès au Datacenter du Cloud
- Problèmes de sécurité spécifique aux Clouds ouverts et interconnectés
- Quatre niveaux de sécurité (technologique, organisationnel, contractuel et de conception d'architectures techniques)

3 - S'inspirer des recommandations d'organismes officiels CSA (Cloud Security Alliance) et ENISA (European Network and Information Security Agency) pour sécuriser le Cloud et gérer les risques
- Protection d'accès à distance au Cloud et Datacenter (firewall multifonctions)
- Sécurité des transactions en ligne par la cryptologie (PKI)
- Authentification des accès : NAC, RBAC, portail captif, authentification forte
- IAM (Identity and Access Management)
- Surveillance des activités anormales (IDS/IPS, NIDS/NIPS)
- SIEM (Security Information and Event Management)
- Lutte contre le vol de données (DLP : Data Lost Prevention)
- 35 types de risques selon ENISA
- Traitement des 5 risques majeurs et fréquents en s'appuyant sur les recommandations d''ENISA

4 - S'appuyer sur les solutions techniques de sécurité du Cloud, proposées par les constructeurs et opérateurs Cloud
- Synthèse des approches, matériels et logiciels de sécurité adoptés par des fournisseurs de Cloud
- Solutions de sécurité offertes par les opérateurs de Cloud public
- Internalisation des dispositifs privés dans le Datacenter du Cloud
- Cloud intermédiaire de sécurité (SecaaS : Security as a Service)
- Avantages et inconvénients de chaque solution

5 - Sécuriser le Cloud par l'organisation des processus et le contrat de SLA
- Classification des applications éligibles pour le Cloud
- Évaluation des risques et mise en place de leur gestion
- Plan de reprise d'activité
- Choix entre les Clouds souverains et ouverts
- Définir les critères de SLA de sécurité
- Responsabilité de l'entreprise : terminaux d'accès et réseaux locaux et distants
- Responsabilités partagées des parties prenantes (entreprise cliente et son fournisseur des services du Cloud) en cas de problèmes liés à la sécurité

6 - Sécuriser le Cloud par la conception des architectures
- Isolement et étanchéité des solutions impliquées (Virtualisation, Stockage, orchestration, API, connecteurs…) et des applications
- Association des moyens de protection, en fonction du niveau de sécurité nécessaire des éléments du Cloud
- Cloud hybride
- Cryptage de la transmission au niveau des réseaux locaux du Datacenter
- Firewall local au sein du Cloud
- Sécuriser les accès locaux et distants au Cloud en tout lieu pour des terminaux mobiles : VPN SSL, VPN IPSec et IEEE802.11i
- Dispositifs out-band de sécurité et de Firewall d'identité pour les accès mobiles en local
- Impact des solutions incohérentes de sécurité et métriques de qualité indispensable
- Ingénierie du trafic IP et des flux de données pour le bon fonctionnement des applications

7 - Sécuriser l'utilisation des périphériques personnels des employés pour accéder au Cloud (BYOD : Bring Your Own Device)
- Choix des solutions sécurisées d'accueil des terminaux (VDI, TS-WEB, RDP, PCoIP…)
- Sélection des périphériques : tablettes, Smartphone, OS, navigateurs…. et leurs contraintes
- Étude des vulnérabilités pour fixer les règles d'utilisation d'accès au Cloud
- Affectation des droits selon des critères techniques et organisationnels

Amazon Web Services (AWS) - Fondamentaux de la sécurité

NOUVEAUTÉ N · SÉMINAIRE S · ACCESSIBLE À DISTANCE

Découvrir les concepts fondamentaux de sécurité du Cloud AWS

OBJECTIFS

- Savoir identifier les avantages et les responsabilités en matière de sécurité lors de l'utilisation du cloud AWS
- Être capable de décrire les fonctionnalités de contrôle d'accès et de gestion d'AWS
- Pouvoir comprendre les différentes méthodes de cryptage des données pour sécuriser les données sensibles
- Comprendre comment sécuriser l'accès réseau aux ressources AWS
- Pouvoir déterminer quels services AWS peuvent être utilisés pour la journalisation et la surveillance de la sécurité

Public

- Professionnels IT intéressés par les pratiques de sécurité du cloud
- Professionnels de la sécurité avec une connaissance minimale d'AWS

Pré-requis

Connaissance des pratiques de sécurité informatique et des concepts d'infrastructure

Connaissances des concepts de cloud computing

Les + de ce séminaire

- Cette formation permet aux participants d'approfondir, de poser des questions, de trouver des solutions et d'obtenir les commentaires d'instructeurs accrédités par AWS possédant des connaissances techniques approfondies.
- Il s'agit d'une formation de niveau fondamental qui fait partie du cursus de certification AWS Security.
- La qualité d'une formation officielle AWS (support de cours numérique en anglais).

Programme

1 - Sécurité sur AWS
- Principes de conception de sécurité dans le cloud AWS
- Modèle de responsabilité partagée AWS

2 - Sécurité du Cloud
- Infrastructure mondiale AWS
- Sécurité du centre de données
- Conformité et gouvernance

3 - Sécurité dans le Cloud (partie 1)
- Gestion des identités et des accès
- Protection des données
- Lab : introduction aux politiques de sécurité

4 - Sécurité dans le Cloud (partie 2)
- Sécurisation de votre infrastructure
- Surveillance et contrôles de détection
- Lab : sécurisation des ressources VPC avec des groupes de sécurité

5 - Sécurité dans le Cloud (partie 3)
- Atténuation DDoS
- Éléments essentiels de la réponse aux incidents
- Lab : automatisation de la réponse aux incidents avec AWS Config et AWS Lambda

6 - Conclusion
- Présentation de l'outil AWS Well-Architected

Réf. **CC324**
1 jour
(7h présentiel)

775 €HT
Offerte

À DISTANCE	21/06, 26/09, 28/11
PARIS	21/06, 26/09, 28/11

Autres sites, nous consulter

CURSUS MÉTIER C

30 Cursus Métier à découvrir

Pour vous permettre de disposer d'équipes toujours plus polyvalentes et rapidement opérationnelles, ib vous propose des cursus adaptés à leur évolution vers de nouveaux domaines de compétences. Étudiés pour favoriser une acquisition rapide de nouveaux savoirs, nos cursus métier couvrent les thématiques actuellement au cœur des préoccupations des entreprises.

Retrouvez tous nos Cursus Métier sur www.ib-formation.fr

Amazon Web Services (AWS) - Ingénierie Sécurité

Opérations de sécurité sur AWS

ACCESSIBLE À DISTANCE

Cette formation montre comment utiliser efficacement les services de sécurité AWS pour rester sécurisé dans le cloud AWS. Elle porte sur les pratiques de sécurité recommandées par AWS pour améliorer la sécurité de vos données et de vos systèmes dans le cloud. Le cours met en évidence les fonctionnalités de sécurité des services clés AWS, notamment les services de calcul, de stockage, de mise en réseau et de base de données. Les participants apprendront également à tirer parti des services et des outils AWS pour l'automatisation, la surveillance continue, la journalisation et la réponse aux incidents de sécurité.

OBJECTIFS

- Être capable d'identifier les avantages et les responsabilités en matière de sécurité liés à l'utilisation du cloud AWS
- Comprendre comment construire des infrastructures applicatives sécurisées
- Pouvoir protéger les applications et les données contre les menaces de sécurité courantes
- Apprendre à effectuer et automatiser les contrôles de sécurité
- Savoir configurer l'authentification et les autorisations pour les applications et les ressources
- Être capable de surveiller les ressources AWS et répondre aux incidents
- Pouvoir capturer et traiter les journaux
- Comprendre comment créer et configurer des déploiements automatisés et reproductibles avec des outils tels que les AMI et AWS CloudFormation

Public

- Ingénieurs sécurité, architectes sécurité et professionnels de la sécurité de l'information

Pré-requis

Connaissance des pratiques de sécurité informatique et des concepts d'infrastructure

Familiarité avec les concepts de cloud computing

Avoir suivi les formations "Amazon Web Services (AWS) - Fondamentaux de la sécurité" (CC324)" et "Amazon Web Services (AWS) - Architecture" (CC312)

Certification

Cette formation prépare au test SCS-C01(en option au tarif de 315 €) qui permet d'obtenir la certification AWS Certified Security - Specialty

Les + de cette formation

- Cette formation explique comment utiliser efficacement les services de sécurité AWS pour travailler en toute sécurité dans le Cloud AWS.
- Une pédagogie basée sur l'alternance de phases théoriques et d'ateliers de mise en pratique. Elle permet aux participants de tester de nouvelles compétences et de les appliquer à leur environnement de travail grâce à différents exercices pratiques.
- Des consultants formateurs experts : les instructeurs sont certifiés pédagogiquement par Amazon Web Services, et disposent de la certification requise du niveau concerné par la formation.
- La qualité d'une formation officielle AWS (support de cours numérique en anglais).

Programme

1 - Sécurité sur AWS
- Sécurité dans le cloud AWS
- Modèle de responsabilité partagée AWS
- Présentation de la réponse aux incidents
- DevOps avec ingénierie de sécurité

2 - Identification des points d'entrée sur AWS
- Identifier les différentes manières d'accéder à la plate-forme AWS
- Comprendre les stratégies IAM
- Limite des autorisations IAM
- Analyseur d'accès IAM
- Authentification multi-facteur
- AWS CloudTrail
- Lab : accès entre comptes

3 - Considérations relatives à la sécurité : environnements d'applications Web
- Menaces dans une architecture à trois niveaux
- Menaces courantes : accès utilisateur
- Menaces courantes : accès aux données
- Conseiller de confiance AWS

4 - Sécurité des applications
- Images de machines Amazon
- Inspecteur Amazon
- Gestionnaire de systèmes AWS
- Lab : utilisation d'AWS Systems Manager et d'Amazon Inspector

5 - Sécurité des données
- Stratégies de protection des données
- Chiffrement sur AWS
- Protection des données au repos avec Amazon S3, Amazon RDS, Amazon DynamoDB
- Protection des données archivées avec Amazon S3 Glacier
- Analyseur d'accès Amazon S3
- Points d'accès Amazon S3

6 - Sécurisation des communications réseau
- Considérations de sécurité Amazon VPC
- Mise en miroir du trafic Amazon VPC
- Réponse aux instances compromises
- Équilibrage de charge Elastic
- Gestionnaire de certificats AWS

7 - Surveillance et collecte de journaux sur AWS
- Amazon CloudWatch et CloudWatch Logs
- Configuration AWS
- Amazon Macie
- Journaux de flux Amazon VPC
- Journaux d'accès au serveur Amazon S3
- Journaux d'accès ELB
- Lab : surveiller et répondre avec AWS Config

8 - Traitement des journaux sur AWS
- Amazon Kinésis
- Amazon Athéna
- Lab : analyse des journaux du serveur Web

9 - Considérations relatives à la sécurité : environnements hybrides
- Connexions AWS Site-to-Site et Client VPN
- Connexion directe AWS
- Passerelle de transit AWS

10 - Protection hors région
- Amazone Route 53
- AWS WAF
- Amazon CloudFront
- Bouclier AWS
- Gestionnaire de pare-feu AWS
- Atténuation DDoS sur AWS

11 - Considérations relatives à la sécurité : environnements sans serveur
- Amazon Cognito
- Passerelle d'API Amazon
- AWS Lambda

12 - Détection et enquête sur les menaces
- Amazon GuardDuty
- Centre de sécurité AWS
- Détective Amazon

13 - Gestion des secrets sur AWS
- AWS KMS
- AWS CloudHSM
- Gestionnaire de secrets AWS
- Lab : utilisation d'AWS KMS

14 - Automatisation et sécurité dès la conception
- AWS CloudFormation
- Catalogue de services AWS
- Lab : automatisation de la sécurité sur AWS avec AWS Service Catalog

15 - Gestion de compte et provisionnement sur AWS
- Organisations AWS
- Tour de contrôle AWS - AWS SSO
- Service d'annuaire AWS
- Lab : accès fédéré avec ADFS

Réf. CC319
3 jours
(21h présentiel)

2 395 €HT
Offerte

À DISTANCE
19/07, 27/09, 29/11
PARIS
19/07, 29/11

Autres sites, nous consulter

Google Cloud Platform - Sécurité

Contrôles et techniques de sécurité sur Google Cloud Platform

ACCESSIBLE À DISTANCE

Cette formation donne aux participants un aperçu approfondi des contrôles et techniques de sécurité sur Google Cloud Platform. À travers des présentations, des démonstrations et des ateliers pratiques, les participants découvrent et déploient les composants d'une solution GCP sécurisée. Ils apprennent également des techniques d'atténuation des risques d'attaques pouvant survenir en de nombreux points d'une infrastructure basée sur GCP, telles que des attaques par déni de service distribué (DDoS) ou par hameçonnage, ou des menaces impliquant une classification et une utilisation de contenu.

OBJECTIFS

- Comprendre l'approche Google en matière de sécurité
- Gérer des identités d'administration à l'aide de Cloud Identity
- Implémenter un accès administrateur avec un principe de moindre privilège à l'aide de Google Cloud Resource Manager et Cloud IAM
- Implémenter des contrôles de trafic IP à l'aide de pare-feu VPC et de Cloud Armor
- Implémenter la fonctionnalité Identity-Aware Proxy
- Analyser les modifications apportées à la configuration ou aux métadonnées des ressources à l'aide des journaux d'audit GCP
- Être capable de sécuriser un environnement Kubernetes
- Détecter des données sensibles et les masquer à l'aide de l'API Data Loss Prevention
- Analyser un déploiement GCP à l'aide de Forseti
- Résoudre les problèmes liés aux principaux types de faille, et plus particulièrement dans le cas d'un accès public aux données et aux machines virtuelles

Public

- Analystes, architectes et ingénieurs en sécurité de l'information
- Spécialistes en sécurité de l'information / cybersécurité
- Architectes d'infrastructure cloud, développeurs d'applications cloud

Pré-requis

Avoir suivi la formation "Google Cloud Platform - Les fondamentaux de l'infrastructure" (CC380) et "Google Cloud Platform - Réseau " (CC404) ou connaissances équivalentes

Connaissances des concepts fondamentaux de la sécurité de l'information

Compétences de base avec les outils de ligne de commande et les environnements de système d'exploitation Linux

Posséder une expérience des opérations de systèmes, y compris le déploiement et la gestion d'applications, sur site ou dans un environnement de cloud public

Compréhension du code en Python ou JavaScript

Certification

Cette formation prépare au test CSE (en option) qui permet d'obtenir la certification Google Professional Cloud Security Engineer

Les + de cette formation

- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, de démonstrations et de travaux pratiques.
- Les consultants spécialistes de la technologie apportent leurs conseils et leur expérience.
- Une formation animée par un formateur certifié Google Cloud Platform.
- La qualité d'une formation officielle Google (support de cours en anglais).

Programme

1 - Fondements de la sécurité GCP

2 - Cloud Identity
- Cloud Identity
- Synchronisation avec Microsoft Active Directory à l'aide de Google Cloud Directory Sync
- Utilisation du service géré pour Microsoft Active Directory (version bêta)
- Choix entre l'authentification Google et l'authentification unique basée sur SAML
- Meilleures pratiques, y compris la configuration DNS, les comptes de super administrateur

3 - Gestion des identités, des accès et clés
- GCP Resource Manager : projets, dossiers et organisations
- Rôles GCP IAM, y compris les rôles personnalisés
- Stratégies GCP IAM, y compris les stratégies d'organisation
- Labels GCP IAM - GCP IAM Recommender
- Outil de dépannage et journaux d'audit GCP IAM
- Les meilleures pratiques, y compris la séparation des fonctions et le moindre privilège, l'utilisation de groupes Google dans les politiques et éviter l'utilisation des rôles primitifs

4 - Configurer un Google Virtual Private Cloud pour l'isolement et sécurité
- Configuration des pare-feu VPC
- Équilibrage de charge et politiques SSL
- Accès privé à l'API Google
- Utilisation du proxy SSL
- Meilleures pratiques pour les réseaux VPC, y compris l'homologation et le VPC partagé utilisation, utilisation correcte des sous-réseaux
- Meilleures pratiques de sécurité pour les VPN
- Considérations de sécurité pour les options d'interconnexion et d'appairage
- Produits de sécurité disponibles auprès des partenaires
- Définir un périmètre de service, y compris des ponts de périmètre
- Configuration de la connectivité privée aux API et services Google

5 - Sécurisation de Compute Engine : techniques et meilleures pratiques
- Comptes de service Compute Engine, par défaut et définis par le client
- Rôles IAM pour les machines virtuelles
- Scope d'APIs pour les machines virtuelles
- Gestion des clés SSH pour les machines virtuelles Linux
- Gestion des connexions RDP pour les machines virtuelles Windows
- Contrôles de stratégie de l'organisation
- Chiffrement des images de machine virtuelle avec des clés de chiffrement gérées par le client et fournies par le client
- Recherche et correction de l'accès public aux machines virtuelles
- Meilleures pratiques, notamment l'utilisation d'images personnalisées renforcées, comptes de service personnalisés, scope d'APIs personnalisés et l'utilisation des informations d'identification par défaut de l'application au lieu de clés gérées par l'utilisateur
- Chiffrement des disques VM avec des clés de chiffrement fournies par le client
- Utilisation de machines virtuelles blindées pour maintenir l'intégrité des machines virtuelles

6 - Sécurisation des données Cloud : techniques et meilleures pratiques
- Cloud Storage et autorisations IAM
- Cloud Storage et ACLs
- Audit des données cloud, y compris la recherche et la correction données accessibles publiquement
- URL signées de Cloud Storage
- Signed policy documents
- Chiffrement des objets Cloud Storage avec des clés de chiffrement gérées par le client et fournies par le client
- Meilleures pratiques, y compris la suppression de versions archivées d'objets après rotation des clés
- Vues autorisées par BigQuery
- Rôles BigQuery IAM
- Meilleures pratiques, notamment préférer les autorisations IAM aux ACL

7 - Sécurisation des applications : techniques et meilleures pratiques
- Types de vulnérabilités de sécurité des applications
- Protections DoS dans App Engine et les Cloud Functions
- Cloud Security Scanner - Identity Aware Proxy

8 - Sécuriser Kubernetes : techniques et meilleures pratiques
- Autorisation
- Sécurisation des charges de travail et des clusters
- Journalisation et surveillance

9 - Protéger contre les attaques Distributed Denail of Service
- Fonctionnement des attaques DDoS
- Mitigations : GCLB, Cloud CDN, autoscaling, pare-feu VPC ingress et egress, Cloud Armor
- Types de produits partenaires complémentaires

10 - Protéger contre les vulnérabilités liées au contenu
- Menace : Ransomware
- Atténuations : sauvegardes, IAM, Data Loss Prevention API
- Menaces : utilisation abusive des données, violations de la vie privée, contenu sensible / restreint / inacceptable
- Menace : phishing d'identité et Oauth
- Atténuation : classification du contenu à l'aide des API Cloud ML ; numérisation et rédaction de données à l'aide de l'API Data Loss Prevention

11 - Surveillance, journalisation, audit et numérisation
- Security Command Center
- Surveillance et journalisation Stackdriver
- Journaux de flux VPC
- Journalisation d'audit cloud
- Déployer et utiliser Forseti

Réf. CC408
3 jours
(21h présentiel)

2 350 €HT
Paris 90 €HT

À DISTANCE
15/06, 21/09, 16/11
PARIS
15/06, 21/09, 16/11

Autres sites, nous consulter

Microsoft Azure - Technologies de sécurité

Implémenter et contrôler la sécurité dans le Cloud Azure

ACCESSIBLE À DISTANCE

OBJECTIFS

- Comprendre comment gérer l'identité et l'accès sur Azure
- Apprendre à mettre en œuvre la protection de la plate-forme
- Être capable de sécuriser les données et les applications
- Comprendre comment gérer les opérations de sécurité

Public

- Ingénieurs en sécurité Azure
- Professionnels IT de la sécurité informatique

Pré-requis

Avoir suivi la formation "Microsoft Azure – Administration" (MSAZ104) ou disposer d'une bonne connaissance des sujets couverts par cette formation

Certification

Cette formation prépare au test AZ-500 (en option au tarif de190 €) qui permet d'obtenir la certification Microsoft Certified Azure Security Engineer Associate

CPF Cette formation est éligible au CPF. Utilisez sa référence (MSAZ500) pour la retrouver dans l'application Mon compte formation ou sur le site moncompteformation.gouv.fr

Les + de cette formation

- Une pédagogie active et variée : les phases de cours magistral sont complétées par des moments d'échanges et des séances de mise en pratique des acquis.
- Les travaux pratiques permettent aux participants de développer une expérience concrète de la mise en place de la sécurité sur Azure.
- L'expertise technique et l'expérience de consultants de haut niveau.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Gérer l'identité et l'accès
- Azure Active Directory
- Identité hybride
- Azure Identity Protection
- Gestion des identités privilégiées Azure AD
- Gouvernance d'entreprise

2 - Mettre en œuvre la protection de la plate-forme
- Sécurité du périmètre
- Sécurité du réseau
- Sécurité de l'hôte
- Sécurité des conteneurs

3 - Données et applications sécurisées
- Azure Key Vault
- Sécurité des applications
- Sécurité du stockage
- Sécurité de la base de données SQL

4 - Gérer les opérations de sécurité
- Azure Monitor
- Azure Security Center
- Azure Sentinel

Réf. MSAZ500
5 jours
(35h présentiel)

3 175 €HT
Offerte

À DISTANCE	BORDEAUX	NANTES	SOPHIA ANTIPOLIS
13/06, 29/08, 03/10, 21/11, 12/12	03/10	14/11	28/11
PARIS	**LILLE**	**RENNES**	**STRASBOURG**
13/06, 29/08, 03/10, 21/11, 12/12	10/10	14/11	13/06, 21/11
AIX-EN-PROVENCE	**LYON**	**ROUEN**	**TOULOUSE**
28/11	04/07, 05/12	26/09	19/09

CPF

Découvrez nos formations éligibles au CPF

Nous proposons de nombreuses formations éligibles sous certaines conditions au Compte Personnel de Formation. Retrouvez-en la liste régulièrement actualisée sur notre site web.

Pour en savoir plus sur le CPF, rendez-vous sur www.ib-formation.fr

Microsoft 365 - Gestion des identités et des services

Mettre à disposition des utilisateurs les services Office 365

ACCESSIBLE À DISTANCE

Lorsqu'on évoque Office 365, il est souvent fait référence aux améliorations d'usages et aux gains de productivité qui découlent de l'utilisation de la suite d'outils collaboratifs. Mais avant d'envisager de profiter de ces bénéfices, il est indispensable d'implémenter l'annuaire et les services réseaux en adéquation avec les besoins et le système d'information existant de l'entreprise (architecture full cloud ou hybride, migration de la totalité des boites aux lettres ou progressive...). Cette formation de 5 jours a été conçue pour fournir aux participants toutes les connaissances sur les avantages et les écueils de chaque scénario d'implémentation et de migration.

OBJECTIFS

- Comprendre comment concevoir, configurer et gérer Microsoft 365
- Connaître les fonctionnalités du produit Microsoft 365
- Savoir configurer Microsoft 365
- Acquérir les compétences nécessaires au déploiement de Microsoft 365 Apps for enterprise
- Planifier et mettre en œuvre la synchronisation des identités
- Comprendre comment mettre en œuvre l'application et l'accès externe

Public

- Toute personne souhaitant déployer et administrer les services Microsoft 365

Pré-requis

Une bonne compréhension du DNS et une expérience fonctionnelle de base avec les services Microsoft 365

Une bonne compréhension des pratiques informatiques générales

Posséder une expérience autour de la messagerie, le travail d'équipe, la sécurité et la conformité ou la collaboration

Certification

Cette formation prépare au test MS-100 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft 365 Certified Enterprise Administrator Expert

Les + de cette formation

- Cette formation couvre trois éléments centraux de l'administration d'entreprise Microsoft 365 : la gestion des locataires et des services Microsoft 365, la gestion Microsoft 365 et la gestion des identités Microsoft 365.
- Une pédagogie basée sur l'alternance de phases théoriques, d'ateliers de mise en pratique, de retours d'expérience et d'échanges.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Conception d'un tenant Microsoft 365
- Planification d'un tenant dans Microsoft 365
- Planification de l'infrastructure locale pour Microsoft 365
- Planification de la solution d'identité et d'authentification pour Microsoft 365
- Planification de l'infrastructure de support pour Microsoft 365
- Planification des exigences hybrides pour le déploiement Microsoft 365
- Planification de la migration vers Microsoft 365

2 - Configuration d'un tenant Microsoft 365
- Configuration de l'expérience Microsoft 365
- Gestion des comptes d'utilisateurs et des licences dans Microsoft 365
- Gestion des groupes dans Microsoft 365
- Ajout d'un domaine personnalisé dans Microsoft 365
- Configuration de la connectivité client à Microsoft 365
- Utilisation de FastTrack et des services partenaires pour prendre en charge Microsoft 365

3 - Gestion d'un tenant Microsoft 365
- Configuration des rôles d'administration dans Microsoft 365
- Gestion de l'intégrité et des services des tenant dans Microsoft 365
- Gestion des déploiements Microsoft 365 Apps for Enterprise pilotées par l'utilisateur
- Implémentation de la télémétrie Office
- Mise en œuvre de Workplace Analytics

4 - Exploration des services de la plate-forme Microsoft 365
- Exploration d'Exchange Online en tant qu'administrateur d'entreprise Microsoft 365
- Exploration de SharePoint Online en tant qu'administrateur d'entreprise Microsoft 365
- Exploration de Microsoft Teams en tant qu'administrateur d'entreprise Microsoft 365
- Exploration de Microsoft Power Platform en tant qu'administrateur d'entreprise Microsoft 365
- Création des applications en tant qu'administrateur d'entreprise Microsoft 365 avec Power Apps
- Création de flux en tant qu'administrateur d'entreprise Microsoft 365 avec Power Automate
- Création des rapports et des tableaux de bord en tant qu'administrateur d'entreprise Microsoft 365 avec Power BI
- Création de chatbots en tant qu'administrateur d'entreprise Microsoft 365 avec Power Virtual Agents

5 - Planification et mise en œuvre de la synchronisation des identités
- Exploration de la synchronisation des identités
- Planification de la mise en œuvre d'Azure AD Connect
- Mise en œuvre d'Azure AD Connect
- Gestion des identités synchronisées
- Exploration de la gestion des mots de passe dans Microsoft 365

6 - Implémentation des applications et des accès externes dans Azure AD
- Implémentation des applications dans Azure AD
- Configuration du proxy d'application Azure AD
- Exploration des solutions d'accès externe

Réf. MSMS100
5 jours
(35h présentiel)

3 095 €HT
Offerte

À DISTANCE	BORDEAUX	NANTES	SOPHIA ANTIPOLIS
18/07, 12/09, 24/10, 28/11	21/11	05/12	10/10
PARIS	**LILLE**	**RENNES**	**STRASBOURG**
18/07, 12/09, 24/10, 28/11	20/06, 21/11	05/12	17/10
AIX-EN-PROVENCE	**LYON**	**ROUEN**	**TOULOUSE**
10/10	13/06, 24/10	21/11	12/12

+ de 3000 missions réalisées chaque année

Un projet de formation sur-mesure ?

Vous devez former plusieurs collaborateurs sur une même thématique ou une même technologie et vous souhaitez pour cela organiser une formation en intra-entreprise ?

Qu'il s'agisse de décliner les programmes présentés sur notre site web ou de concevoir un dispositif sur-mesure, nos équipes sont à votre entière disposition pour vous accompagner dans votre projet.

Après une analyse de vos besoins, elles apporteront à votre demande la réponse pédagogique, technique et logistique la plus pertinente.

Contactez nos Conseillers Formation au 0 825 07 6000

Microsoft 365 - Gestion de la sécurité et de la mobilité

Garantir de la souplesse aux utilisateurs et sécuriser les échanges

ACCESSIBLE À DISTANCE

Il fut une époque (encore assez récente) où dans l'esprit des professionnels, cloud et sécurité ne faisaient pas forcément bon ménage. Et le doute augmentait encore dès lors qu'était évoqué le recours à des applications ou des équipements mobiles. Conscients de cette réticence, les grands acteurs du marché ont développé de nombreux outils visant à mettre en place une sécurité performante à tous les étages. Microsoft a ainsi intégré à son offre 365 une gamme complète d'outils particulièrement performants pour protéger chaque élément du SI (annuaire, authentification, dialogue clients/serveurs, applications mobiles...). L'objet de cette formation est précisément de présenter par le détail l'ensemble de ces outils et de permettre aux professionnels concernés par le sujet de la sécurité d'apprendre à les mettre en œuvre.

OBJECTIFS

- Découvrir les métriques et les services de sécurité Microsoft 365
- Connaître Microsoft 365 Threat Intelligence
- Comprendre la gouvernance des données dans Microsoft 365 et Microsoft 365 Intelligence
- Apprendre à effectuer des recherches et enquêtes
- Comprendre comment gérer les périphériques
- Apprendre à effectuer les stratégies de déploiement de Windows 10
- Être capable de gérer les périphériques mobiles

Public

- Toute personne souhaitant déployer et administrer les services Microsoft 365

Pré-requis

Avoir suivi la formation "Microsoft 365 - Gestion des identités et des services" (MSMS100) ou disposer d'une bonne connaissance des sujets couverts par cette formation

Certification

Cette formation prépare au test MS-101 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft 365 Certified Enterprise Administrator Expert

Les + de cette formation

- Une pédagogie complète basée sur l'alternance de phases théoriques, de séquences d'échanges, d'ateliers de mise en pratique et de retours d'expériences.
- Les travaux pratiques qui ponctuent la formation permettent aux participants de mettre immédiatement en application leurs acquis.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Explorer les mesures de sécurité dans Microsoft 365
- Examiner les vecteurs de menace et les violations de données
- Explorer le modèle de sécurité Zero Trust
- Découvrir les solutions de sécurité dans Microsoft 365
- Examiner Microsoft Secure Score
- Examiner la gestion des identités privilégiées
- Examiner Azure Identity Protection

2 - Gestion des services de sécurité Microsoft 365
- Examiner Exchange Online Protection
- Examiner Microsoft Defender pour Office 365
- Gérer les pièces jointes sécurisées
- Gérer les liens sécurisés
- Explorer les rapports dans les services de sécurité Microsoft 365

3 - Implémenter Threat Intelligence dans Microsoft 365
- Aperçu de Microsoft 365 Threat Intelligence
- Explorer le tableau de bord de sécurité
- Implémenter Microsoft Defender pour l'identité
- Mettre en œuvre Microsoft Cloud Application Security

4 - Introduction à la gouvernance des données dans Microsoft 365
- Découvrir l'archivage dans Microsoft 365
- Explorer la rétention dans Microsoft 365
- Explorer la gestion des droits relatifs à l'information
- Découvrir le cryptage des messages Office 365
- Explorer la gestion des enregistrements sur place dans SharePoint
- Explorer la prévention des pertes de données dans Microsoft 365

5 - Implémenter la gouvernance des données dans Microsoft 365
- Évaluer la préparation à la conformité
- Mettre en œuvre des solutions de conformité
- Créer des barrières d'information dans Microsoft 365
- Créer une stratégie DLP à partir d'un modèle intégré
- Créer une stratégie DLP personnalisée
- Créer une stratégie DLP pour protéger les documents
- Mettre en œuvre des conseils de stratégie pour les stratégies DLP

6 - Gérer la gouvernance des données dans Microsoft 365
- Gérer la rétention dans les e-mails
- Résoudre les problèmes de gouvernance des données
- Explorer les étiquettes de sensibilité
- Implémenter des étiquettes de sensibilité
- Mettre en œuvre la gouvernance des données

7 - Gérer la recherche de contenu et les enquêtes dans Microsoft 365
- Rechercher du contenu dans le centre de conformité Microsoft 365
- Mener des enquêtes sur les journaux d'audit
- Gérer la découverte électronique avancée

8 - Préparer la gestion des périphériques dans Microsoft 365
- Explorer la cogestion de l'appareil Windows 10
- Préparer les périphériques Windows 10 pour la cogestion
- Transition de Configuration Manager vers Intune
- Examiner le Microsoft Store for Business
- Planifier la gestion des applications

9 - Planification de la stratégie de déploiement Windows 10
- Examiner les scénarios de déploiement de Windows 10
- Explorer les modèles de déploiement de Windows Autopilot
- Planifier la stratégie d'activation d'abonnement Windows 10
- Résoudre les erreurs de mise à niveau de Windows 10
- Analyser les données de diagnostic de Windows 10 à l'aide de Desktop Analytics

10 - Mise en œuvre de la gestion des périphériques mobiles dans Microsoft 365
- Explorer la gestion des périphériques mobiles
- Déployer la gestion des périphériques mobiles
- Enregistrer des périphériques à MDM
- Gérer la conformité des périphériques

Réf. MSMS101
5 jours
(35h présentiel)

3 095 €HT
Offerte

À DISTANCE	LILLE	Autres sites, nous consulter
29/08, 10/10, 21/11	03/10	
PARIS	**LYON**	
29/08, 10/10, 21/11	12/09	

PEARSON VUE AUTHORISED TEST CENTRE

Certifications éditeurs

Nos centres de formation certifiés Pearson Vue disposent de salles dédiées à des sessions de tests menant aux certifications éditeurs : Microsoft, VMware, Citrix, Cisco...

Retrouvez toutes les certifications éditeurs sur www.ib-formation.fr

Microsoft 365 - Techniques de sécurité pour les administrateurs

Garantir la sécurité des données et des échanges

ACCESSIBLE À DISTANCE

Conséquence immédiate du développement des usages de solutions cloud, les besoins des entreprises en termes de sécurité informatique s'accroissent inévitablement. La mission des professionnels de ce sujet sensible est d'adapter les règles et stratégies de sécurisation aux fonctionnements et échanges (internes et externes) des entreprises. En réponse à ces attentes légitimes de ses clients, Microsoft fournit dans ses offres Azure et Microsoft 365 les possibilités d'optimiser ces paramètres de sécurisation à tous les niveaux (Annuaire, données serveurs et utilisateurs, matériels, flux d'échanges d'informations internes et externes, applications mobiles...). A l'issue de cette formation de 5 jours, les participants disposeront des connaissances l eur permettant de définir et mettre en place les stratégies de sécurité les plus adaptées à leur entreprise.

OBJECTIFS

- Savoir administrer la sécurité des utilisateurs et des groupes dans Microsoft 365
- Être capable de planifier et d'implémenter Azure AD Connect et gérer les identités synchronisées
- Pouvoir planifier la mise en œuvre des identités fédérées
- Savoir utiliser Microsoft Secure Score pour évaluer la sécurité
- Comprendre comment utiliser les divers services avancés de protection pour Microsoft 365
- Savoir implémenter la protection des informations Azure pour Microsoft 365 et la protection des informations Windows pour les périphériques
- Être en mesure de planifier et déployer un système d'archivage et de conservation des données dans le respect des obligations liées au RGPD

Public

- Administrateur sécurité

Pré-requis

Compréhension conceptuelle de base de Microsoft Azure

Expérience sur Windows 10 et Office 365

Compréhension de base des réseaux informatiques, des autorisations et de l'authentification

Connaissance pratique de la gestion des périphériques mobiles

Certification

Cette formation prépare au test MS-500 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft 365 Certified Security Administrator Associate

CPF Cette formation est éligible au CPF. Utilisez sa référence (MS500) pour la retrouver dans l'application Mon compte formation ou sur le site moncompteformation.gouv.fr

Les + de cette formation

- Les nombreux travaux pratiques proposés lors de cette formation fournissent aux participants une première expérience pratique de l'administration de la sécurité sur Microsoft 365.
- Les retours d'expérience de consultants-formateurs experts de la solution.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Gestion des utilisaterus et des groupes
- Concepts de gestion de l'identité et des accès
- Le modèle Zero Trust
- Planifier une solution d'identité et d'authentification
- Comptes et rôlels d'utilisateurs
- Gestion des mots de passe

2 - Synchronisation et protection des identités
- Planifier la synchronisation d'annuaires
- Configurer et gérer les identités synchronisées
- Protection de l'identité Azure AD

3 - Gestion des identités et des accès
- Gestion des applications
- Gouvernance des identités
- Gérer l'accès aux appareils
- Contrôle d'accès basé sur les rôles (RBAC)
- Solutions pour l'accès externe
- Gestion des identités privilégiées

4 - Sécurité dans microsoft 365
- Vecteurs de menaces et violations des données
- Stratégie et principes de sécurité
- Solutions de sécurité Microsoft
- Score sécurisé

5 - Protection contre les menaces
- Exchange Online Protection (EOP)
- Microsoft Defender pour Office 365
- Gestion des pièces jointes sécurisées
- Gestion des liens sécurisés
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

6 - Gestion des menaces
- Utiliser le tableau de bord de sécurité
- Enquête sur les menaces et réponses
- Azure Sentinel
- Analyse avancée des menaces

7 - Sécurité des applications Cloud Microsoft
- Déployer Cloud Application Security
- Utiliser les informations de sécurité des applications cloud

8 - Mobilité
- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Déployer des services de périphériques mobiles
- Enregistrer des périphériques dans la gestion des périphériques mobiles

9 - Protection et gouvernance de l'information
- Concepts de protection des informations
- Gouvernance et gestion des documents
- Étiquettes de sensibilité
- Archivage dans Microsoft 365
- Rétention dans Microsoft 365
- Stratégies de rétention dans le Centre de conformité Microsoft 365
- Archivage et rétention dans Exchange
- Gestion des enregistrements sur place dans SharePoint

10 - Gestion des droits et cryptage
- Gestion des droits relatifs à l'information (IRM)
- Extension de messagerie Internet polyvalente sécurisée (S-MIME)
- Chiffrement de messages Office 365

11 - Prévention de la perte de données
- Principes fondamentaux de la prévention des pertes de données
- Créer une stratégie DLP
- Personnaliser une stratégie DLP
- Créer une stratégie DLP pour protéger les documents
- Conseils sur les stratégies

12 - Gestion de la conformité
- Centre de conformité

13 - Gestion des risques d'initiés
- Risque d'initié
- Accès privilégié
- Obstacles à l'information
- Construire des murs éthiques dans Exchange Online

14 - Rechercher du contenu et enquêter
- Recherche de contenu
- Enquêtes sur les journaux d'audit
- eDiscovery avancé

Réf. MSMS500
4 jours
(28h présentiel)

2 640 €HT
Offerte

À DISTANCE	**LILLE**	Autres sites, nous consulter
04/07, 29/08, 17/10, 05/12	12/12	
PARIS	**LYON**	
04/07, 29/08, 17/10, 05/12	28/11	

Les fondamentaux de la sécurité, de la conformité et de l'identité Microsoft

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

Se familiariser avec les principes fondamentaux de la sécurité, de la conformité et de l'identité

OBJECTIFS

- Être capable de décrire les concepts de base de la sécurité, de la conformité et de l'identité
- Pouvoir comprendre les concepts et les fonctionnalités des solutions Microsoft de gestion des identités et des accès
- Décrire les capacités des solutions de sécurité Microsoft
- Comprendre les fonctionnalités de gestion de la conformité de Microsoft

Public

- Toute personne intéressée par les solutions de sécurité, de conformité et d'identité Microsoft

Pré-requis

Compréhension générale des concepts de réseau et de cloud computing

Connaissances informatiques générales ou toute expérience pratique dans un environnement informatique

Compréhension générale de Microsoft Azure et Microsoft 365

Certification

Cette formation prépare au test SC-900 (en option au tarif de 120 €) qui permet d'obtenir la certification Microsoft Certified Security, Compliance, and Identity Fundamentals

Les + de cette formation

- Un tour d'horizon des concepts de base de sécurité, de conformité et d'identité et des solutions Microsoft basées sur le cloud.
- Les retours d'expérience de consultants-formateurs experts de la solution.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Décrire les concepts de base de la sécurité, de la conformité et de l'identité

- Décrire les concepts et méthodologies de sécurité et de conformité
- Décrire les concepts d'identité

2 - Décrire les concepts et les fonctionnalités des solutions de gestion des identités et des accès Microsoft

- Décrire les services de base et les types d'identité d'Azure AD
- Décrire les fonctionnalités d'authentification d'Azure AD
- Décrire les fonctionnalités de gestion des accès d'Azure AD
- Décrire les fonctionnalités de protection des identités et de gouvernance d'Azure AD

3 - Décrire les fonctionnalités des solutions de sécurité Microsoft

- Décrire les fonctionnalités de sécurité de base dans Azure
- Décrire les fonctionnalités de gestion de la sécurité d'Azure
- Décrire les fonctionnalités de sécurité de Microsoft Sentinel
- Décrire les fonctionnalités de protection contre les menaces de Microsoft 365
- Décrire les fonctionnalités de gestion de la sécurité de Microsoft 365
- Décrire la sécurité des terminaux avec Microsoft Intune

4 - Décrire les fonctionnalités des solutions de conformité Microsoft

- Décrire les fonctionnalités de gestion de la conformité dans Microsoft
- Décrire les fonctionnalités de protection et de gouvernance des informations de Microsoft 365
- Décrire les fonctionnalités de risque d'initié dans Microsoft 365
- Décrire les fonctionnalités de découverte électronique et d'audit de Microsoft 365
- Décrire les fonctionnalités de gouvernance des ressources dans Azure

Réf. MSSC900
1 jour
(7h présentiel)

730 €HT
Offerte

À DISTANCE Autres sites, nous consulter
20/06, 03/10, 28/11
PARIS
20/06, 03/10, 28/11

Analyste des opérations de sécurité Microsoft

Maîtriser les outils de sécurité Microsoft pour parer les risques

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

Découvrez comment enquêter, répondre et rechercher les menaces à l'aide de Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender. Dans ce cours, vous apprendrez comment atténuer les cybermenaces à l'aide de ces technologies. Plus précisément, vous allez configurer et utiliser Azure Sentinel et utiliser Kusto Query Language (KQL) pour effectuer la détection, l'analyse et la création de rapports. Le cours a été conçu pour les personnes qui occupent un poste dans le domaine des opérations de sécurité et aide les apprenants à se préparer à l'examen SC-200: Analyste des opérations de sécurité Microsoft.

OBJECTIFS

- **Être capable d'expliquer comment Microsoft Defender pour Endpoint peut remédier aux risques dans votre environnement**
- **Savoir administrer un environnement Microsoft Defender pour Endpoint**
- **Apprendre à configurer les règles de réduction de la surface d'attaque sur les périphériques Windows 10**
- **Pouvoir examiner les domaines et les adresses IP dans Microsoft Defender pour Endpoint**
- **Être en mesure d'examiner les comptes d'utilisateurs et configurer les paramètres d'alerte dans Microsoft Defender**

Public

- Analystes sécurité
- Ingénieurs sécurité

Pré-requis

Compréhension de base de Microsoft 365

Compréhension fondamentale des produits de sécurité, de conformité et d'identité Microsoft

Compréhension intermédiaire de Windows 10

Familiarité avec les services Azure, en particulier les bases de données Azure SQL et le stockage Azure

Connaissance des machines virtuelles Azure et des réseaux virtuels

Compréhension de base des concepts de script

Certification

Cette formation prépare au test SC-200 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft Certified Security Operations Analyst Associate

Les + de cette formation

- Une formation complète qui permet aux participants d'acquérir les connaissances nécessaires pour détecter et contrer les menaces de sécurité avec Microsoft Azure Sentinel, Azure Defender et Microsoft 365 Defender.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Atténuer les menaces à l'aide de Microsoft 365 Defender

- Introduction à la protection contre les menaces avec Microsoft 365
- Atténuer les incidents à l'aide de Microsoft 365 Defender
- Corriger les risques avec Microsoft Defender pour Office 365
- Microsoft Defender pour l'identité
- Protéger les identités avec Azure AD Identity Protection
- Microsoft Defender pour les applications cloud
- Répondre aux alertes de prévention de la perte de données à l'aide de Microsoft 365
- Gérer les risques internes dans Microsoft 365

2 - Atténuer les menaces à l'aide de Microsoft Defender for Endpoint

- Se protéger contre les menaces avec Microsoft Defender for Endpoint
- Déployer l'environnement Microsoft Defender for Endpoint
- Implémenter des améliorations de sécurité Windows
- Effectuer des enquêtes sur l'appareil
- Effectuer des actions sur un appareil
- Effectuer des enquêtes sur les preuves et les entités
- Configurer et gérer l'automatisation
- Configurer pour les alertes et les détections
- Utiliser la gestion des menaces et des vulnérabilités

3 - Atténuer les menaces à l'aide de Microsoft Defender pour le Cloud

- Planifier des protections de charges de travail cloud à l'aide de Microsoft Defender pour cloud
- Protections des charges de travail dans Microsoft Defender pour le cloud
- Connecter des ressources Azure à Microsoft Defender pour le cloud
- Connecter des ressources non Azure à Microsoft Defender pour le cloud
- Corriger les alertes de sécurité à l'aide de Microsoft Defender pour le cloud

4 - Créer des requêtes pour Microsoft Sentinel à l'aide du langage de requête Kusto (KQL)

- Construire des instructions KQL pour Microsoft Sentinel
- Analyser les résultats de requête à l'aide de KQL
- Créer des instructions multi-tables à l'aide de KQL
- Utilisation de données de chaîne à l'aide d'instructions KQL

5 - Configurer votre environnement Microsoft Sentinel

- Présentation de Microsoft Sentinel
- Créer et gérer des espaces de travail Microsoft Sentinel
- Journaux de requêtes dans Microsoft Sentinel
- Utiliser des listes de surveillance dans Microsoft Sentinel
- Utiliser les renseignements sur les menaces dans Microsoft Sentinel

6 - Connecter les journaux à Microsoft Sentinel

- Connecter des données à Microsoft Sentinel à l'aide de connecteurs de données
- Connecter les services Microsoft à Microsoft Sentinel
- Connecter Microsoft 365 Defender à Microsoft Sentinel
- Connecter des hôtes Windows à Microsoft Sentinel
- Connecter les journaux Common Event Format à Microsoft Sentinel
- Connecter des sources de données syslog à Microsoft Sentinel
- Connecter des indicateurs de menace à Microsoft Sentinel

7 - Créer des détections et effectuer des enquêtes à l'aide de Microsoft Sentinel

- Détection des menaces avec l'analyse Microsoft Sentinel
- Gestion des incidents de sécurité dans Microsoft Sentinel
- Réponse aux menaces avec les playbooks Microsoft Sentinel
- Analyse du comportement des utilisateurs et des entités dans Microsoft Sentinel
- Interroger, visualiser et surveiller les données dans Microsoft Sentinel

8 - Effectuer une recherche de menaces dans Microsoft Sentinel

- Concepts de chasse aux menaces dans Microsoft Sentinel
- Chasse aux menaces avec Microsoft Sentinel
- Rechercher des menaces à l'aide de blocs-notes dans Microsoft Sentinel

Réf. **MSSC200**
4 jours
(28h présentiel)

2 620 €HT
Offerte

À DISTANCE
26/09, 05/12
PARIS
26/09, 05/12

Autres sites, nous consulter

Administrateur d'identité et d'accès Microsoft

Mise en œuvre d'une gouvernance des identités pour gérer les accès aux applications

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

OBJECTIFS

- Apprendre à mettre en œuvre une solution de gestion des identités
- Comprendre comment mettre en place des solutions d'authentification et de gestion des accès
- Savoir mettre en œuvre la gestion des accès pour les applications
- Être capable de planifier et mettre en œuvre une stratégie de gouvernance des identités

Public

- Administrateurs d'identité et d'accès qui envisagent de passer l'examen de certification associé ou qui effectuent des tâches d'administration d'identité et d'accès dans leur travail quotidien
- Administrateur ou à un ingénieur qui souhaite se spécialiser dans la fourniture de solutions d'identité et de systèmes de gestion d'accès pour les solutions basées sur Azure ou jouer un rôle essentiel dans la protection d'une organisation

Pré-requis

Avoir suivi les formations "Les fondamentaux de la sécurité, de la conformité et de l'identité Microsoft" (MSSC900) et "Microsoft Azure - Administration" (MSAZ104) et ou connaissances équivalentes

Certification

Cette formation prépare au test SC-300 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft Certified Identity and Access Administrator Associate

Les + de cette formation

- Cette formation pratique fournit aux participants les connaissances et les compétences nécessaires pour mettre en œuvre des solutions de gestion d'identité basées sur Microsoft Azure AD et les technologies d'identité connectées.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Mettre en œuvre une solution de gestion des identités
- Implémenter la configuration initiale d'Azure AD
- Créer, configurer et gérer des identités
- Mettre en œuvre et gérer des identités externes
- Mettre en œuvre et gérer l'identité hybride

2 - Mettre en œuvre une solution d'authentification et de gestion des accès
- Sécuriser l'utilisateur Azure AD avec MFA
- Gérer l'authentification des utilisateurs
- Planifier, mettre en œuvre et administrer l'accès conditionnel
- Gérer la protection des identités Azure AD

3 - Implémenter la gestion des accès pour les applications
- Planifier et concevoir l'intégration de l'entreprise pour l'authentification unique
- Mettre en œuvre et surveiller l'intégration des applications d'entreprise pour l'authentification unique
- Implémenter l'enregistrement de l'application

4 - Planifier et mettre en œuvre une stratégie de gouvernance des identités
- Planifier et mettre en œuvre la gestion des droits
- Planifier, mettre en œuvre et gérer les révisions d'accès
- Planifier et mettre en œuvre l'accès privilégié
- Surveiller et maintenir Azure AD

Réf. MSSC300
4 jours
(28h présentiel)

2 620 €HT
Offerte

À DISTANCE
21/06, 04/10, 29/11
PARIS
21/06, 04/10, 29/11

Autres sites, nous consulter

Pour vous inscrire à une formation... il y a toujours un moyen de nous contacter

Par téléphone

Nos Conseillers Formation sont joignables de 8h30 à 18h00 au 0 825 07 6000. Ils répondront à toutes vos questions concernant les formations, les dates de sessions, les opportunités de dernière minute...

Par e-mail

Une adresse unique : espace.clients@ib.cegos.fr pour toutes vos inscriptions ou demandes de renseignements.

Par Internet

Retrouvez sur www.ib-formation.fr l'intégralité de nos programmes ainsi que toutes les informations qui vous seront utiles : dates de sessions, plans d'accès, offres de dernière minute, informations sur les évènements ib....

Administrateur de la protection des informations Microsoft

Protégez les informations dans votre déploiement Microsoft 365

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

OBJECTIFS

- Apprendre à configurer les stratégies de prévention de la perte de données
- Être capable de sécuriser les messages dans Office 365
- Pouvoir décrire le processus de configuration de la gouvernance de l'information
- Savoir définir les termes clés associés aux solutions de protection et de gouvernance des informations de Microsoft
- Comprendre comment utiliser les types d'informations sensibles et les classificateurs
- Passer en revue et analyser les rapports DLP
- Pouvoir identifier et atténuer les violations de la stratégie DLP

Public

- Administrateur de la protection des informations
- Administrateur, praticien des risques, ingénieur en sécurité

Pré-requis

Connaissance de base des technologies de sécurité et de conformité Microsoft

Connaissance de base des concepts de protection de l'information

Compréhension des concepts du cloud computing

Compréhension des produits et services Microsoft 365

Certification

Cette formation prépare au test SC-400 (en option au tarif de 190 €) qui permet d'obtenir la certification Microsoft Certified Information Protection Administrator Associate

Les + de cette formation

- Un focus sur la gouvernance des données et la protection des informations au sein de votre organisation.
- Une formation rythmée durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.
- La richesse des ateliers qui favorise l'assimilation des points abordés.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Programme

1 - Implémenter la protection des informations dans Microsoft 365

- Introduction à la protection et à la gouvernance des informations dans Microsoft 365
- Classer les données pour la protection et la gouvernance
- Créer et gérer des types d'informations sensibles
- Décrire le cryptage Microsoft 365
- Déployer le chiffrement des messages dans Office 365
- Configurer les étiquettes de sensibilité
- Appliquer et gérer les étiquettes de sensibilité

2 - Implémenter la prévention de la perte de données dans Microsoft 365

- Empêcher la perte de données dans Microsoft 365
- Mettre en œuvre la prévention de la perte de données Endpoint
- Configurer les stratégies DLP pour Microsoft Cloud App Security et Power Platform
- Gérer les stratégies et rapports DLP dans Microsoft 365

3 - Implémenter la gouvernance de l'information dans Microsoft 365

- Informations de gouvernance dans Microsoft 365
- Gérer la rétention des données dans les charges de travail Microsoft 365
- Gérer les enregistrements dans Microsoft 365

Réf. MSSC400
2 jours
(14h présentiel)

1 470 €HT
Offerte

À DISTANCE
01/09, 21/11
PARIS
01/09, 21/11

Autres sites, nous consulter

L'aide au recrutement avec la POE (Préparation Opérationnelle à l'Emploi)

Vous rencontrez des difficultés pour recruter des collaborateurs dont les profils et les compétences sont en adéquation avec vos besoins ?

ib vous propose un dispositif complet qui répond précisément à cette problématique. En associant pré-recrutement et formation préalable à l'embauche, ib vous propose une solution clé en main qui vous permettra d'intégrer des collaborateurs immédiatement opérationnels sur des métiers en tension.

A travers notre dispositif qui associe aux avantages liés à la POEI des services à forte valeur ajoutée, nous apportons une réponse efficace aux problèmes de pénuries de compétences et d'employabilité auxquels sont aujourd'hui confrontées les entreprises.

Pour en savoir plus, contactez-nous au 0 825 07 6000

Check Point Security Administration (CCSA) R80

L'essentiel pour assurer la gestion au quotidien

ACCESSIBLE À DISTANCE

Les produits de Check Point Software sont parmi les plus utilisés dans le monde de la sécurité. Cette introduction constitue une formation complète sur le Firewall Check Point, incluant la gestion de la politique de sécurité, la translation d'adresses (NAT), la mise à jour des systèmes, la mise en place des tunnels VPNs ou encore la sécurité de messagerie et de contenu.

OBJECTIFS

- Découvrir les technologies Check Point
- Être à même de déployer une politique de sécurité et de surveiller le trafic
- Comprendre comment gérer les utilisateurs et fournir un accès aux ressources protégées
- Être capable de mettre en œuvre la translation d'adresse (NAT) et des VPNs
- Apprendre à installer la passerelle de sécurité dans un environnement distribué
- Pouvoir configurer les règles sur les serveurs Web et passerelle
- Être capable de créer une base de règle de base dans SmartDashboard et affecter des autorisations
- Savoir planifier des sauvegardes et des mises à niveau transparentes avec un minimum de temps
- Comprendre comment surveiller et de dépanner IPS et le trafic de réseau commun
- Se préparer au passage de l'examen de certification Check Point CCSA (Check Point Certified Security Administrator)

Public

- Administrateurs réseaux, ingénieurs sécurité et réseaux
- Responsables de la sécurité des systèmes d'informations
- Toutes personnes visant la certification CCSA

Pré-requis

Connaissance de base des réseaux et/ou des compétences Windows Server Unix

Certification

Cette formation prépare au test 156-215.80 (en option) qui permet d'obtenir la certification Check Point Certified Security Administrator (CCSA) R80

Les + de cette formation

- Les participants sont amenés à réaliser de nombreux ateliers et développent ainsi un premier savoir-faire pratique.
- Les retours terrain de consultants impliqués dans des projets de mise en œuvre de la solution.
- Une formation qui constitue une excellente préparation à la certification CCSA R80.
- La qualité d'une formation officielle Check Point (support de cours en anglais).

Programme

1 - Introduction aux technologies Check Point
2 - Installation de la «Security Gateway» dans un environnement distribué
3 - Configuration des règles sur le web et serveurs de passerelle
4 - Création d'une politique de sécurité dans Smartdashboard et attribution des autorisations
5 - Planification des sauvegardes
6 - Gestion des mises à niveau en minimisant leur impact sur les passerelles
7 - Surveillance et diagnostic des IPS et du trafic réseau
8 - Être prêt à se défendre contre les menaces réseau
9 - Évaluer les politiques de sécurité existantes et optimiser la base de règles
10 - Gérer l'accès des utilisateurs aux réseaux locaux d'entreprise
11 - Surveiller les activités de réseau suspectes et analyser les attaques
12 - Résoudre les connexions réseau
13 - Protéger les courriels et la messagerie contenu
14 - Check Point - Présentation de la technologie
15 - Plates-formes de déploiement et les politiques de sécurité
16 - Circulation et surveillance des connexions
17 - Traductions d'adresses réseau
18 - Gestion et authentification des utilisateurs
19 - Utilisation SmartUpdate
20 - Sensibilisation identité d'exécution
21 - Configuration de tunnels VPN
22 - Résoudre les problèmes de l'administration de la sécurité

Réf. SE87
3 jours
(21h présentiel)

2 235 €HT

À DISTANCE
13/06, 18/07, 12/09, 10/10, 14/11, 05/12

Autres sites, nous consulter

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Check Point Security Expert (CCSE) R80

Mise en œuvre des fonctionnalités avancées

ACCESSIBLE À DISTANCE

Cette formation de niveau 2, destinée aux experts sécurité, constitue un cours complet sur Firewall-1 incluant de nombreuses options de configuration avancées (Routage Avancé, QoS, Redondance et Haute Disponibilité des liens, VPN SSL...). Elle apporte également un descriptif complet de toutes les nouvelles applications et solutions apparues avec la version R8x du produit et ses fameuses lames logicielles ("software blades") qui permettent de construire une solution de sécurité à la carte.

OBJECTIFS

- Comprendre comment sauvegarder votre passerelle de sécurité et votre serveur de gestion
- Pouvoir construire, tester et dépanner une passerelle de sécurité en cluster
- Apprendre à mettre à niveau et dépanner un serveur de gestion
- Savoir configurer et maintenir des solutions d'accélération de la sécurité
- Être capable de gérer, tester et optimiser les tunnels VPN d'entreprise
- Apprendre à se prémunir des menaces
- Se préparer au passage de l'examen de certification Check Point CCSE (Check Point Certified Security Expert)

Public

- Administrateurs réseaux, ingénieurs sécurité et réseaux, responsables de la sécurité des systèmes d'informations
- Toutes personnes visant la certification CCSE

Pré-requis

Être certifié CCSA R80 ou avoir suivi la formation "Check Point Security Administration (CCSA) R80" (SE87)

Il est fortement recommandé d'avoir des compétences sur TCP/IP, internet et la gestion des systèmes Unix et Windows

Certification

Cette formation prépare au test 156-315.80 (en option) qui permet d'obtenir la certification Check Point Certified Security Expert (CCSE) R80

Les + de cette formation

- Les nombreux travaux pratiques qui ponctuent la formation permettent aux participants de mettre immédiatement en application leurs acquis.
- Les consultants spécialistes de la technologie apportent leurs conseils et leur expérience.
- Une formation qui constitue une excellente préparation à la certification Check Point Certified Expert (CCSE) R80.40.
- La qualité d'une formation officielle Check Point (support de cours en anglais).

Programme

1 - Sauvegarde des passerelles
2 - Sauvegarde du serveur de gestion
3 - Construction, test et diagnostic d'un cluster de passerelles
4 - Mettre à jour et dépanner le serveur de gestion
5 - Configurer et maintenir des modules d'accélération SecureXL
6 - Gérer, tester et optimiser les tunnels VPN Check Point
7 - Présentation de la technologie
8 - Plates-formes de déploiement et les politiques de sécurité
9 - Circulation et surveillance des connexions
10 - Traductions d'adresses réseau
11 - Gestion et authentification des utilisateurs
12 - Utilisation SmartUpdate
13 - Sensibilisation identité d'exécution
14 - Configuration de tunnels VPN
15 - Résoudre les problèmes de l'administration de la sécurité
16 - Construire, tester et dépanner de nombreux scénarios de déploiement
17 - Appliquer les conseils d'initiés du dépannage
18 - Vérifier Security Systems Point
19 - Pratiquer les techniques de valorisation avancées
20 - Migrer vers une solution de sécurité de clustering
21 - Créer des évènements pour le reporting de conformité
22 - Gérer l'accès interne et externe aux ressources d'entreprise

Réf. SE88
3 jours
(21h présentiel)

2 235 €HT

À DISTANCE
12/12

Autres sites, nous consulter

F5 - Configuration d'Advanced WAF : Web Application Firewall

Sécuriser les applications Web

ACCESSIBLE À DISTANCE

Avec des réseaux informatiques inter connectés, les menaces visant les applications et les données sont omniprésentes. Avec Advanced WAF, F5 Networks propose une solution de protection des applications Web contre les attaques par force brute, par extraction de contenu de sites Web (le "web scraping") ou encore par déni de service ("DDoS" au niveau de la couche 7). Cette formation très pratique d'une durée de 4 jours permettra aux participants d'acquérir l'expertise nécessaire pour détecter, atténuer et prévenir les attaques basées sur le protocole HTTP qui ciblent les applications Web.

OBJECTIFS

- **Décrire le rôle du système BIG-IP en tant que périphérique proxy complet dans un réseau de distribution d'applications**
- **Être capable de provisionner le pare-feu d'application Web avancé F5**
- **Pouvoir définir un pare-feu d'application Web**
- **Décrire comment F5 Advanced Web Application Firewall protège une application Web en sécurisant les types de fichiers, les URL et les paramètres**
- **Comprendre comment déployer F5 Advanced Web Application Firewall à l'aide du modèle Rapid Deployment (et d'autres modèles) et définir les contrôles de sécurité inclus dans chaque**
- **Définir les paramètres d'apprentissage, d'alarme et de blocage en fonction de la configuration du pare-feu d'application Web avancé F5**
- **Définir les signatures d'attaque et expliquer pourquoi leur mise en scène est importante**
- **Apprendre à déployer des campagnes contre les menaces pour vous protéger contre les menaces CVE**
- **Savoir comparer la mise en œuvre des stratégies de sécurité positives et négatives et expliquer les avantages de chaque**

Public

- Personnel SecOps responsable du déploiement, du réglage et de la maintenance quotidienne de F5 Advanced WAF

Pré-requis

Aucun, il est toutefois conseillé d'avoir suivi la formation "F5 - Administration BIG-IP" (SE70) ou être certifié Administrateur BIG-IP F5

Il est conseillé d'avoir suivi les formations en ligne gratuites suivantes : "Premiers pas avec BIG-IP" et "Premiers pas avec BIG-IP Application Security Manager)" pour les participants ayant une expérience limitée en matière d'administration et de configuration BIG-IP

Les + de cette formation

- L'alternance de cours théorique, de travaux pratiques et de d'échanges permettra aux participants d'acquérir les compétences nécessaires à la détection et à la prévention des attaques sur les applications Web.
- La qualité d'une formation officielle (support de cours en anglais).

Programme

1 - Configuration du système BIG-IP
- Présentation du système BIG-IP
- Configuration initiale du système BIG-IP
- Archivage de la configuration du système BIG-IP
- Exploitation des ressources et outils de support

2 - Traitement du trafic avec BIG-IP
- Identification des objets de traitement de trafic BIG-IP
- Comprendre les profils
- Aperçu des stratégies de trafic local
- Visualiser le flux de requêtes HTTP

3 - Concepts liés aux applications Web
- Présentation du traitement des demandes d'application Web
- Pare-feu d'application Web
- Contrôles de sécurité de la couche 7
- Vue d'ensemble des éléments de communication Web et de la structure de requêtes HTTP

4 - Vulnérabiltiés des applications Web
- Une taxonomie des attaques
- Exploits communs contre les applications Web

5 - Déploiement des stratégies de sécurité
- Définir l'apprentissage
- Comparaison des modèles de sécurité positifs et négatifs
- Le workflow de déploiement
- Attribution d'une stratégie au serveur virtuel
- Workflow de déploiement
- Configurer les technologies de serveur

6 - Réglage des stratégies et infractions
- Traitement du trafic post-déploiement
- Comment les infractions sont catégorisées
- Taux d'infraction : échelle de menace
- Définir la mise en scène et l'application, le mode d'application
- Définir la période de préparation à l'application
- Revoir la définition de l'apprentissage

7 - Signatures d'attaque et campagnes contre les menaces
- Définition des signatures d'attaque
- Les bases de la signature d'attaque
- Création de signatures d'attaque définies par l'utilisateur
- Définition des modes d'édition simples, avancés
- Définition des ensembles de signature d'attaque

8 - Élaboration d'une stratégie de sécurité positive
- Définition et apprentissage des composants de stratégie de sécurité
- Définition du joker (Wildcard)
- Définir le cycle de vie de l'entité
- Choisir le programme d'apprentissage
- Affichage des suggestions d'apprentissage et de l'état d'avancement

9 - Sécurisation des cookies et autres en-têtes
- Le but des cookies WAF avancés F5
- Définition des cookies autorisés et appliqués
- Sécuriser les en-têtes HTTP

10 - Rapports visuels et journalisation
- Affichage des données récapitulatives de sécurité des applications
- Rapports
- Statistiques sur la force brute et le Web Scraping
- Affichage des rapports de ressources
- Conformité PCI : PCI-DSS 3.0
- Analyse des demandes

11 - Projet de lab 1

12 - Gestion avancée des paramètres
- Définition des types de paramètres
- Définir des paramètres statiques, dynamiques
- Définition des niveaux de paramètres
- Autres considérations relatives aux paramètres

13 - Élaboration automatique de stratégies
- Vue d'ensemble de l'élaboration automatique de stratégies
- Définition de modèles qui automatisent l'apprentissage
- Définition du relâchement et du resserrement des stratégies
- Définition de la vitesse d'apprentissage
- Définition des modifications du site de suivi

14 - Intégration du scanner de vulnérabilité d'applications Web
- Intégration de la sortie du scanner
- Importer des vulnérabilités
- Résolution des vulnérabilités
- Utilisation du fichier XSD du scanner XML générique

15 - Déploiement de stratégies en couches
- Définir une stratégie parent et l'héritage
- Cas d'utilisation du déploiement de la stratégie parent

16 - Application de la connexion et atténuation de la force brute
- Définition des pages de connexion pour le contrôle de flux
- Configuration de la détection automatique des pages de connexion
- Définition des attaques par force brute

17 - Reconnaissance avec suivi de session
- Définition du suivi de session
- Configuration des actions en cas de détection de violation

18 - Atténuation DOS de la couche 7
- Définition des attaques par déni de service
- Définition du profil de protection DoS
- Présentation de la protection DoS basée sur TPS
- Création d'un profil de journalisation DoS

19 - Bots Défense avancés
- Classification des clients avec le profil Bot Defense
- Définition des signatures de bot
- Définition de l'empreinte digitale F5

20 - Chiffrement de formulaire à l'aide de Datasafe
- Ciblage des éléments de la livraison d'applications
- Exploiter le modèle d'objet de document

Protection des applications à l'aide de DataSafe

21 - Révisions et laboratoires finaux

Réf. SE72
4 jours
(28h présentiel)

3 450 €HT

À DISTANCE
20/06, 25/07, 12/09, 26/09, 24/10, 21/11, 19/12

Autres sites, nous consulter

Palo Alto Networks Firewall 10.1 - Configuration et Management

Mettre en œuvre les firewalls de nouvelle génération

CERTIFIANT

ACCESSIBLE À DISTANCE

Palo Alto Networks, le spécialiste américain de la sécurité informatique et des firewalls, a lancé mi 2020 une nouvelle version de son système d'exploitation PAN OS. Avec PAN OS 10.1, le constructeur propose le tout premier pare-feu de dernière génération basé sur le Machine Learning. Avec cette avancée technologique majeure Palo Alto bouscule le monde de la prévention en fournissant une solution capable de se prémunir des attaques inconnues tout en améliorant ses fonctionnalités précédentes. Bien au-delà de la seule prise en main des dernières fonctionnalités les participants à cette formation apprendront à installer, configurer et manager les firewalls de nouvelle génération de Palo Alto.

OBJECTIFS

- Être capable de configurer et manager les fonctionnalités essentielles des firewalls Palo Alto Networks de nouvelles générations
- Comprendre comment configurer et gérer les stratégies de sécurité et NAT pour activer le trafic approuvé vers et depuis les zones
- Savoir configurer et gérer les stratégies de prévention des menaces pour bloquer le trafic provenant d'adresses IP, de domaines et d'URL connus et inconnus
- Pouvoir monitorer le trafic réseau en utilisant les interfaces web interactives et les rapports intégrés

Public

- Ingénieurs sécurité, administrateurs sécurité, spécialistes des opérations de sécurité, analystes de la sécurité et équipe de support

Pré-requis

Connaissance de base des concepts de réseau, y compris le routage, la commutation et l'adressage IP

Être familiarisé avec les concepts de base de la sécurité

Une expérience avec d'autres technologies de sécurité (IPS, proxy et filtrage de contenu) est un plus

Certification

Cette formation prépare au test PCNSA qui permet d'obtenir la certification Palo Alto Networks Certified Network Security Administrator (PCNSA).

Un voucher permettant le passage du test de certification associé à cette formation est inclus dans le prix de la formation.

Le passage de l'examen est compris dans le prix de la formation.

Les + de cette formation

- Cette formation allie théorie, démonstrations, discussions interactives mais aussi des exercices pratiques.
- Une formation "concrète" : les travaux pratiques proposés permettent aux participants d'acquérir une première expérience pratique de la configuration, du management et de l'exploitation des firewalls de nouvelle génération Palo Alto Networks.
- Les exercices sont effectués via des labs en ligne hébergés sur du matériel Palo Alto.
- La qualité d'une formation officielle Palo Alto (support de cours en anglais).

Programme

1 - Portfolio et architecture de Palo Alto Networks
2 - Configuration initiale des paramètres du pare-feu
3 - Gestion des configurations du pare-feu
4 - Gérer les comptes d'administrateur du pare-feu
5 - Connexion du pare-feu aux réseaux de production avec des zones de sécurité
6 - Créer et gérer des règles de stratégie de sécurité
7 - Créer et gérer des règles de stratégie NAT
8 - Contrôler l'utilisation des applications avec APP-ID
9 - Blocage des menaces connues à l'aide de profils de sécurité
10 - Blocage du trafic Web inapproprié avec le filtrage d'URL
11 - Blocage des menaces inconnues avec Wildfire
12 - Contrôle de l'accès aux ressources réseau avec l'ID utilisateur
13 - Utilisation du déchiffrement pour bloquer les menaces dans le trafic chiffré
14 - Localisation des informations importantes à l'aide de journaux et de rapports

Réf. SE52
5 jours
(35h présentiel)

3 750 €HT
Paris 115 €HT

À DISTANCE	PARIS	Autres sites, nous consulter
13/06, 04/07, 22/08, 19/09, 10/10, 28/11, 12/12	13/06, 04/07, 22/08, 19/09, 10/10, 28/11, 12/12	

Les programmes certifiants

CERTIFIANT

Les programmes certifiants ib sont destinés aux personnes souhaitant acquérir de nouveaux savoirs et les valoriser par l'obtention d'une certification reconnue sur le marché de l'informatique.

Des cursus de plusieurs semaines permettant d'évoluer vers un nouveau métier aux formations courtes visant à acquérir une expertise sur un domaine précis, notre offre de formations certifiantes est à la fois complète et variée

Le passage des examens de certification, généralement proposés en fin de session, est systématiquement inclus dans le prix de nos formations certifiantes.

Palo Alto Networks : Firewall 10.1 - Troubleshooting

Exploitation courante et dépannage de la solution

ACCESSIBLE À DISTANCE

OBJECTIFS

- Apprendre à utiliser des outils de pare-feu, y compris l'interface de ligne de commande, pour enquêter sur les problèmes de mise en réseau
- Pouvoir suivre des méthodologies de dépannage éprouvées qui sont spécifiques aux fonctionnalités individuelles
- Comprendre comment analyser les journaux avancés pour résoudre divers scénarios du quotidien
- Être capable de résoudre des défis avancés basés sur des scénarios

Public

- Ingénieurs sécurité, administrateurs sécurité, spécialistes des opérations de sécurité, analystes sécurité, ingénieurs réseau et équipe de support

Pré-requis

Avoir suivi la formation "Palo Alto Networks Firewall 10.1 - Configuration et Management" (SE52) ou avoir expérience pratique équivalente

Avoir une solide connaissance pratique du routage et de la commutation, de l'adressage IP et des concepts de sécurité réseau, et au moins six mois d'expérience avec les pare-feu Palo Alto Networks

Certification

Cette formation prépare au test PCNSE (en option) qui permet d'obtenir la certification Palo Alto Networks Certified Network Security Engineer (PCNSE)

Les + de cette formation

- Cette formation allie théorie, démonstrations, discussions interactives et aussi exercices pratiques.
- Les exercices sont effectués via des labs en ligne hébergés sur du matériel Palo Alto Networks.
- La qualité d'une formation officielle Palo Alto (support de cours numérique en anglais).

Programme

1 - Outils et ressources
2 - Logique de flux
3 - Capture de paquets
4 - Journaux de diagnostic des paquets
5 - Trafic entrant hôte
6 - Trafic de transit
7 - Services systèmes
8 - Gestion des certificats et decryptage SSL
9 - ID Utilisateur
10 - GlobalProtect
11 - Escalades et RMAS
12 - Prochaines étapes

Réf. SE54
3 jours
(21h présentiel)

2 690 €HT

À DISTANCE
07/09, 07/12

Autres sites, nous consulter

290 formations au format mixte en 2022

Des solutions multi-modales et digitales pour une nouvelle expérience d'apprentissage

Notre offre intègre de nombreuses formations mixtes (blended) qui associent à la formation en salle des activités digitales de différentes natures : modules e-learning, vidéocasts, rich média, classes virtuelles, Rapid Learning, quiz,...

Nous proposons ainsi des **dispositifs d'apprentissage entièrement tournés vers l'apprenant** qui reposent sur une combinaison optimisée de différentes modalités et qui renforcent ainsi l'efficacité et la rapidité de l'apprentissage.

Conçus par nos experts, les contenus digitaux qui enrichissent nos formations tout en permettant dans de nombreux cas d'en optimiser la durée sont accessibles à distance sur le Learning Hub ib avant, pendant ou après les phases de présentiel.

Pour en savoir plus, rendez-vous sur www.ib-formation.fr

Palo Alto Networks Cortex XDR 2 - Prevention, Analysis, and Response

ACCESSIBLE À DISTANCE

Prévenir les menaces et protéger les terminaux

OBJECTIFS

- Être capable de différencier l'architecture et les composants de Cortex XDR
- Savoir décrire les concepts de prévention des menaces pour la protection des terminaux
- Apprendre à travailler avec la console de gestion Cortex XDR
- Pouvoir différencier les attaques par exploitation et les attaques de logiciels malveillants et décrire comment Cortex XDR les bloque
- Comprendre comment effectuer les actions de réponse appropriées
- Savoir décrire l'analyse de causalité et les concepts d'analyse de Cortex XDR
- Être en mesure de trier et enquêter sur les alertes et gestion des incidents
- Pouvoir gérer les règles Cortex XDR et étudier les menaces via le centre de requêtes

Programme

1 - Présentation de la famille Cortex XDR2
2 - Travailler avec les applications Cortex
3 - Premiers pas avec EndPoint Protection
4 - Protection contre les logiciels malveillants
5 - Protection contre les exploits
6 - Exceptions et actions de réponse
7 - Analyse des menaces comportementales
8 - Règles Cortex XDR
9 - Gestion des incidents
10 - Rechercher et enquêter
11 - Dépannage de base

Public

- Analystes en cyber-sécurité et spécialistes des opérations de sécurité

Pré-requis

Être familier avec les concepts de sécurité d'entreprise

Les + de cette formation

- Cette formation pratique permet aux participants d'apprendre à configurer et à gérer Cortex XDR à partir de la console de gestion pour protéger les endpoints contre les attaques de logiciels malveillants.
- La qualité d'une formation officielle Palo Alto (support de cours en anglais).

Réf. SE55
3 jours
(21h présentiel)

2 690 €HT

À DISTANCE
12/09, 07/12

Autres sites, nous consulter

Les implantations

En mettant à votre disposition des équipes commerciales dans chacune de nos agences, nous vous apportons la garantie d'une vraie relation de proximité. Quel que soit votre besoin, vous bénéficiez de l'accompagnement d'experts géographiquement et culturellement proches de vous :

PARIS	LILLE	RENNES	STRASBOURG
AIX-EN-PROVENCE	LYON	ROUEN	TOULOUSE
BORDEAUX	NANTES	SOPHIA-ANTIPOLIS	

Symantec ProxySG V6.7 : Administration - Les bases

Déployer ProxySG pour sécuriser les échanges

NOUVEAUTÉ

ACCESSIBLE À DISTANCE

OBJECTIFS

- Être capable de décrire les principales fonctions de Secure Web Gateway du ProxySG
- Apprendre à configurer et appliquer les licences sur un ProxySG
- Comprendre comment déployer un ProxySG en mode explicite ou transparent
- Savoir utiliser le gestionnaire de stratégie visuelle afin d'établir des stratégies de gestion du filtrage Web, d'authentification et de gestion du trafic SSL
- Apprendre à utiliser les journaux d'accès ProxySG pour générer des rapports

Public

- Professionnels qui souhaitent maîtriser les fondamentaux de Symantec BlueCoat ProxySG

Pré-requis

Avoir une compréhension de base des concepts de réseau, tels que les réseaux locaux (LAN), Internet, la sécurité et les protocoles IP

Les + de cette formation

- La formation est un cours d'introduction qui permet aux participants d'apprendre les options de déploiement et la gestion des différentes fonctionnalités clés de Proxy SG.
- Cette formation comprend de nombreux exercices de mise en pratique dans un environnement de travail.
- La qualité d'une formation officielle Symantec.

Programme

1 - Introduction à la passerelle Web sécurisée Symantec ProxySG
- Décrire les fonctions d'un serveur proxy
- Différencier les serveurs proxy des pare-feu
- Décrire les principales fonctionnalités et avantages de Symantec ProxySG
- Les différents modèles ProxySG
- Ressources communautaires en ligne de Symantec
- Accéder à l'aide intégrée et à la documentation du produit Symantec

2 - Options de déploiement de sécurité ProxySG
- 3 méthodes de déploiement du réseau
- 3 rôles possibles du ProxySG

3 - Console de gestion ProxySG
- Relation entre la console de gestion et la CLI ProxySG
- Fonction principale des principaux domaines de la console de gestion

4 - Interception de trafic utilisant des services Proxy
- Comprendre les fonctions des services proxy, des auditeurs et des types de proxy
- Décrire les trois services proxy les plus courants
- Expliquer comment les paramètres d'interception et de contournement affectent ce qui arrive au trafic réseau passant par le ProxySG
- Expliquer la fonction des paramètres du service proxy global commun

5 - Protocole de transfert Hypertexte (HTTP)
- Comprendre comment une connexion est lancée sur la couche de transport
- Identifier les composants d'une URL HTTP
- Expliquer les deux types de messages HTTP : requête et réponse
- Identifier les codes de réponse communs

6 - Introduction au gestionnaire de politique visuelle
- La relation entre le VPM, le CPL et la console de gestion
- L'ordre de traitement par défaut pour les couches et les règles de la politique
- Les déclencheurs et les actions qui peuvent être utilisés dans la politique d'écriture
- Identifier les types d'objets que le VPM prend en charge
- Quelques recommandations à suivre lors de l'utilisation du VPM pour créer une stratégie

7 - Filtrage du contenu Web
- Les principaux concepts de filtrage Web
- Les bases de données de la catégorie primaire
- Les types de catégories disponibles pour la politique
- Comment BlueCoat WebFilter et WebPulse fonctionnent ensemble

8 - Utilisation de l'intelligence de menace pour défendre le réseau
- Le Global Intelligence Network
- Les niveaux de géolocalisation et de risque de menace et leur utilisation dans une politique

9 - Assurer des téléchargements sécurisés
- Comment le malware peut être transmis via HTTP
- Les méthodes, avantages et inconvénients de la détection du type de fichier
- Considérations pour décider quel contenu bloquer les sources possibles de logiciels malveillants

10 - Notification de l'utilisateur des politiques d'utilisation d'Internet
- Expliquer la fonction et les différents composants des pages d'exception intégrées et personnalisées
- Décrire les objets "Notify User"
- Identifier les types de pages pouvant être envoyées aux utilisateurs en utilisant les objets Notify User
- Décrire les pages splash et les pages de coaching en utilisant les objets Notify User dans le VPM

11 - Accès à l'ouverture de session sur ProxySG
- Décrire, à haut niveau, comment le ProxySG effectue l'enregistrement d'accès
- Décrire les composants d'une installation de journal d'accès ProxySG
- Identifier les installations de journal et les formats de journal par défaut
- Décrire les cas d'utilisation courante pour le téléchargement périodique et continu des journaux d'accès

Réf. SE98
2 jours
(14h présentiel)

ORGANISÉ SUR DEMANDE, NOUS CONSULTER

Certified Stormshield Network Administrator (NT-CSNA)

NOUVEAUTÉ · CERTIFIANT · ACCESSIBLE À DISTANCE

L'essentiel pour assurer la gestion au quotidien

OBJECTIFS

- Être capable de prendre en main un firewall SNS et connaître son fonctionnement
- Comprendre comment configurer un firewall dans un réseau
- Pouvoir définir et mettre en œuvre des politiques de filtrage et de routage
- Apprendre à configurer un contrôle d'accès aux sites web en http et https (proxy)
- Savoir configurer des politiques d'authentification
- Comprendre comment mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL)

Public

- Responsables informatique, administrateurs réseaux et tous techniciens informatique

Pré-requis

Avoir de bonnes connaissances TCP/IP, une formation réseau préalable est un plus

Certification

Cette formation prépare au test CNSA qui permet d'obtenir la certification Certified Stormshield Network Administrator (CSNA)
Deux passages de l'examen de certification en ligne sont compris dans le prix de la formation.

Les + de cette formation

- Cette formation a pour but de présenter la gamme et les fonctionnalités de base du produit Stormshield Network Security.
- La formation alterne cours théorique et travaux pratiques.
- Les participants reçoivent un support de cours composé du cours, des travaux pratiques (Labs) et de leurs corrections. Afin de pouvoir mettre en pratique les éléments du cours, ils disposent d'un environnement technique complet.
- Afin de maintenir l'expertise des participants, toutes les mises à jour du support de cours sont accessibles au format PDF durant 3 ans sur la plate-forme https://institute.stormshield.eu. Ils y trouveront également un environnement virtuel pédagogique leur permettant de manipuler le produit et de rejouer les Labs en toute autonomie.
- La qualité d'une formation officielle Stormshield.

Programme

1 - Prise en main du firewall
- Enregistrement sur l'espace client et accès aux ressources techniques
- Initialisation du boitier et présentation de l'interface d'administration
- Configuration système et droits d'administration
- Installation de la licence et mise à jour de la version du système
- Sauvegarde et restauration d'une configuration

2 - Traces et supervisions
- Présentation des catégories de traces
- Supervision et graphiques d'historiques

3 - Les objets
- Notion d'objet et types d'objets utilisables
- Objets réseau et routeur

4 - Configuration réseau
- Modes de configuration d'un boitier dans un réseau
- Types d'interfaces (Ethernet, modem, bridge, VLAN, GRETAP)
- Types de routage et priorités

5 - Translation d'adresses (NAT)
- Translation sur flux sortant (déguisement)
- Translation sur flux entrant (redirection)
- Translation bidirectionnelle (translation un pour un)

6 - Filtrage
- Généralités sur le filtrage et notion de suivi de connexion (stateful)
- Présentation détaillée des paramètres d'une règle de filtrage
- Ordonnancement des règles de filtrage et de translation

7 - Protection applicative
- Mise en place du filtrage URL en http et https
- Configuration de l'analyse antivirale et de l'analyse par détonation Breach Fighter
- Module de prévention d'intrusion et profils d'inspection de sécurité

8 - Utilisateurs et authentification
- Configuration des annuaires
- Présentation des différentes méthodes d'authentification (LDAP, Kerberos, Radius, Certificat SSL, SPNEGO, SSO)
- Enrôlement d'utilisateurs
- Mise en place d'une authentification explicite via portail captif

9 - Les réseaux privés virtuels
- Concepts et généralités VPN IPSec (IKEv1 et IKEv2)
- Site à site avec clé pré-partagée
- Virtual Tunneling Interface

10 - VPN SSL
- Principe de fonctionnement
- Configuration

11 - Passage de l'examen de certification "Certified Stormshield Network Administrator (CSNA)"
- La certification consiste en un examen effectué en ligne (1h30, 70 questions).
- Le score minimum de certification est de 70%.
- L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de trois semaines sur la plateforme https://institute.stormshield.eu.
- En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine supplémentaire.

Réf. SE92
3 jours
(21h présentiel)

2 250 €HT

À DISTANCE Autres sites, nous consulter
20/06

Certifications éditeurs

PEARSON VUE AUTHORISED TEST CENTRE

Nos centres de formation certifiés Pearson Vue disposent de salles dédiées à des sessions de tests menant aux certifications éditeurs : Microsoft, VMware, Citrix, Cisco...

Retrouvez toutes les certifications éditeurs sur www.ib-formation.fr

Certified Stormshield Network Expert (NT-CSNE)

Mise en œuvre des fonctionnalités avancées

NOUVEAUTÉ · CERTIFIANT · ACCESSIBLE À DISTANCE

OBJECTIFS

- Être capable d'utiliser de manière avancée l'IHM
- Apprendre à configurer avec précision le moteur de prévention d'intrusions
- Savoir mettre en place une PKI et une authentification transparente
- Comprendre comment mettre en place un VPN IPsec par certificat
- Pouvoir configurer un cluster haute disponibilité

Public

- Responsables informatique, administrateurs réseaux et tous techniciens informatique ayant obtenu la certification CSNA

Pré-requis

Toutes personnes ayant réussi l'examen CSNA dans les 3 ans précédant la formation CSNE

Certification

Cette formation prépare au test CNSE qui permet d'obtenir la certification Certified Stormshield Network Expert (NT-CSNE)

Deux passages de l'examen de certification en ligne sont compris dans le prix de la formation.

Les + de cette formation

- Cette formation a pour but de présenter les fonctionnalités avancées du produit Stormshield Network Security.
- La formation alterne cours théorique et travaux pratiques.
- Les participants reçoivent un support de cours composé du cours, des travaux pratiques (Labs) et de leurs corrections. Afin de pouvoir mettre en pratique les éléments du cours, ils disposent d'un environnement technique complet.
- Afin de maintenir l'expertise des participants, toutes les mises à jour du support de cours sont accessibles au format PDF durant 3 ans sur la plate-forme https://institute.stormshield.eu. Ils y trouveront également un environnement virtuel pédagogique leur permettant de manipuler le produit et de rejouer les Labs en toute autonomie.
- La qualité d'une formation officielle Stormshield.

Programme

1 - Présentation détaillée du moteur de prévention d'intrusion Stormshield Network
- Différences entre la prévention et la détection d'intrusion
- Le moteur de prévention d'intrusion
- Les différents types d'analyses
- Les profils protocolaires et applicatifs

2 - Infrastructure à clés publiques
- Bases de cryptographie symétrique et asymétrique
- Les types de chiffrement
- PKI Stormshield Network
- Création d'une autorité de certification, d'une identité serveur et d'une identité utilisateur

3 - Proxy SSL
- Principe de fonctionnement
- Paramétrages du proxy SSL
- VPN IPSec avancé
- Fonctionnement détaillé et mécanisme de NAT traversal
- Support du Dead Peer Detection (DPD)
- Architecture VPN en étoile et chainage
- NAT dans IPSec
- Architecture VPN IPsec avec tunnel de secours
- Configuration d'un VPN site à site avec utilisation de certificats
- Configuration d'un VPN nomade

4 - GRE et GRETAP
- Principe de fonctionnement
- Configuration et mise en place

5 - Authentification transparente
- Principe de fonctionnement
- Méthode d'authentification SPNEGO
- Méthode d'authentification par certificat SSL

6 - Haute disponibilité
- Principe de fonctionnement
- Assistant de création et de configuration d'un cluster HA
- Configuration des interfaces réseaux
- Configuration avancée

7 - Passage de l'examen de certification "Certified Stormshield Network Expert (NT-CSNE)"
- La certification consiste en un examen effectué en ligne (2h, 90 questions).
- Le score minimum de certification est de 70%.
- L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de trois semaines sur la plate-forme https://institute.stormshield.eu.
- En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine supplémentaire.

Réf. SE93
3 jours
(21h présentiel)

2 250 €HT

PARIS	Autres sites, nous consulter
21/06	

IBM Security Identity Manager - Les bases de l'administration

Renforcer la sécurité des accès

ACCESSIBLE À DISTANCE

Cette formation de 4 jours est une introduction à l'administration d'IBM Security Identity Manager. Les participants apprendront comment planifier, installer, configurer et utiliser le système IBM Security Identity Manager.

OBJECTIFS

- Découvrir IBM Security Identity Manager
- Pouvoir discuter de l'architecture et du processus de déploiement
- Comprendre comment gérer la structure organisationnelle, les utilisateurs et les rôles
- Apprendre à télécharger des utilisateurs vers Identity Manager à l'aide du processus de flux d'identité
- Être capable de configurer les services et les stratégies pour les nœuds finaux Identity Manager
- Savoir configurer et automatiser le provisioning des ressources
- Pouvoir personnaliser les flux de travail et les opérations du cycle de vie
- Apprendre à implémenter des rapports à l'aide de rapports par défaut et personnalisés
- Comprendre comment gérer l'accès aux consoles Identity Manager
- Savoir configurer la synchronisation sélective du mot de passe
- Être en mesure de gérer les propriétés de journalisation

Programme

1 - Introduction à IBM Security Identity Manager
2 - Architecture et installation
3 - Gestion de l'organisation, des utilisateurs et des rôles
4 - Chargement des données utilisateur
5 - Configuration des ressources gérées dans IBM Identity Manager
6 - Ressources d'approvisionnement
7 - Gestion des flux de travail et des opérations du cycle de vie
8 - Utiliser la fonctionnalité de rapport
9 - Gestion de l'accès aux consoles IBM Security Identity Manager
10 - Configuration de la synchronisation sélective du mot de passe
11 - Gestion des propriétés de journalisation

Public

- Administrateurs système et développeurs qui déploient et gèrent IBM Security Identity Manager

Pré-requis

Connaître les annuaires LDAP
Connaissances des fondamentaux TCP/IP, JavaScript et Linux

Les + de cette formation

- Une formation qui accorde une large place à la pratique : 50% du temps est consacré à des ateliers de mise en situation.
- Une formation très complète : les participants acquerront les connaissances nécessaires sur le produit (depuis l'installation complète jusqu'au déploiement de la solution).
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Réf. SR836
4 jours
(28h présentiel)

2 800 €HT

À DISTANCE
27/06, 07/11

Des équipes à votre écoute

Vous accompagner au quotidien et construire avec vous la solution la plus pertinente implique une organisation flexible, capable de réagir rapidement et efficacement. C'est pourquoi nous avons organisé nos équipes pour apporter des réponses adaptées à chacune de vos problématiques.

- À votre disposition du lundi au vendredi de 8h30 à 18h00, nos Conseillers Formation vous guident dans le choix de vos formations, vous orientent dans vos démarches administratives et répondent à toutes vos sollicitations.
- Nos Ingénieurs Conseil, présents dans chacun de nos centres, apportent des réponses à vos demandes spécifiques et construisent avec vous des solutions adaptées à vos problématiques.
- Notre équipe Grands Projets vous accompagne dans la définition et la mise en œuvre de vos projets stratégiques (grands déploiements, accompagnement du changement...).

Un numéro unique : 0 825 07 6000

IBM Access Manager Platform - Les fondamentaux

Mettre en œuvre la solution de sécurité des accès

ACCESSIBLE À DISTANCE

OBJECTIFS

- Être capable de décrire le produit IBM Access Manager et ses principales fonctionnalités
- Discuter de l'architecture et du processus de déploiement
- Comprendre comment configurer les utilisateurs, groupes et domaines d'Access Manager
- Savoir présenter les concepts d'un proxy inverse et son intégration dans votre infrastructure Web
- Décrire l'espace objet protégé et le modèle de contrôle d'accès aux règles
- Pouvoir expliquer comment configurer des jonctions de proxy inverse pour gérer les requêtes Web
- Apprendre à configurer les mécanismes d'authentification pris en charge par Access Manager
- Comprendre comment configurer la journalisation, l'audit et le traçage pour les composants Access Manager

Programme

1 - Introduction à IBM Access Manager
2 - Architecture et installation
3 - Gestion des utilisateurs, des groupes et des domaines
4 - Concepts de Proxy Inverse
5 - Contrôle d'accès basé sur des règles
6 - Configuration des jonctions pour les ressources back-end
7 - Cadre et méthodes d'authentification
8 - Journalisation, audit et traçage

Public

- Administrateurs système et développeurs

Pré-requis

Familiarité avec LDAP, TCP / IP et HTTP
Familiarité avec la ligne de commande Linux
Connaissance de base de JavaScript
Connaissance pratique des concepts de sécurité, y compris SSL, l'authentification et l'autorisation

Les + de cette formation

- Une formation opérationnelle : les apports théoriques sont accompagnés de phases de mise en pratique qui favorisent un ancrage durable des acquis.
- Les conseils de professionnels ayant exploité la solution en entreprise.
- La qualité d'une formation officielle IBM (support de cours numérique en anglais).

Réf. SR745
3 jours
(21h présentiel)

2 390 €HT

À DISTANCE
18/10

Les labels Qualité

Fruit d'une volonté historique de l'entreprise et d'un engagement quotidien de nos équipes, notre système qualité apporte à nos clients la garantie d'une satisfaction optimale.

Reposant sur une remise en question permanente de notre organisation et de nos méthodes et s'enrichissant chaque jour des retours de nos clients, il favorise l'atteinte d'un objectif unique : l'excellence de nos prestations.

Chez ib, la qualité est une réalité attestée par l'obtention de la certification ISO 9001 et le référencement au Datadock.

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Sécuriser les emails avec Cisco Email Security Appliance (SESA)

ACCESSIBLE À DISTANCE

Assurer la sécurité des échanges par mail avec une appliance

Destiné à protéger l'entreprise de menaces pouvant être véhiculées par les emails, l'Appliance Cisco Email Security scrute l'intégralité des contenus qui transitent par la messagerie. Qu'il s'agisse de messages expédiés ou reçus, le dispositif réagit dès lors qu'il identifie du contenu assimilé à du spam, du phishing ou contenant un malware ou un virus en le plaçant automatiquement en quarantaine. Disposant de tout un arsenal technologique dédié à la sécurité des échanges par email, la solution peut être paramétrée très finement. Les administrateurs de la solution participants à cette formation de 4 jours apprendront à configurer les différents outils proposés avec l'Appliance.

OBJECTIFS

- Apprendre à configurer et à mettre en œuvre l'application Cisco de sécurité des mails
- Pouvoir intégrer un service d'annuaire via LDAP
- Être capable d'analyser et de réaliser le dépannage des problèmes d'intégration de LDAP
- Savoir utiliser les différents filtres afin de modifier et de réorienter les emails
- Comprendre comment déployer en toute sécurité et réaliser le dépannage des filtres
- Apprendre à configurer TLS et le GSD (Guaranteed Secure Delivery)
- Pouvoir authentifier les emails à l'aide de DKIM et SPF
- Se préparer à passer l'examen Securing Email with Cisco Email Security Appliance (300-720 SESA)

Public

- Administrateurs systèmes
- Toute personne s'occupant de la messagerie (designers, architectes, gestionnaires réseaux...)

Pré-requis

Posséder des compétences et connaissances sur les fondamentaux TCP/IP (l'adressage IP et le sous-réseau, le routage statique IP et DNS)
Posséder des compétences sur la messagerie internet (SNMTP, les formats de messages Internet et les formats de messages MIME)
Connaitre et savoir manipuler l'interface en ligne de commandes (CLI) ainsi que l'interface graphique utilisateur (GU)
Posséder des connaissances sur la sécurité des emails

Certification

Cette formation prépare au test 300-720 SESA (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- La formation intègre de nombreux travaux pratiques qui favorisent une assimilation rapide et durable des thématiques abordées en cours.
- Les retours d'expérience de consultants-formateurs spécialistes de la technologie.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

Programme

1 - Présentation de IronPort
- Présentation de la technologie et du produit
- Mettre en œuvre et configurer IronPort

2 - Organisation des mises en œuvre
- Mettre en œuvre et configurer le système
- Déterminer les expéditeurs ainsi que les groupes de destinataires

3 - Paramétrer le public cocnerné
- Élaborer la stratégie de flux des messages
- Table d'accès des hôtes et des groupes de destinataires
- Routes SMTP
- Anti-Spam

4 - Stopper les Spams à l'aide d'IronPort
- Paramétrer et appliquer les "sender base reputation scores" ainsi que "content adpative scanning engine"
- Paramétrer et installer les Anti-Virus et Filtres
- Paramétrer l'activation d'un ou plusieurs Anti-Virus
- Appliquer les filtres contre les virus pour une protection "Zerohour"
- Utilisation des stratégies

5 - Concevoir des stratégies pour les mails des utilisateurs
- Déterminer les messages fractionnés
- Détailler la localisation centralisée (rapports)
- Réaliser la localisation de messages

6 - Élaborer et guider en quarantaine
- Consacrer des utilisateurs en quarantaine
- Attribuer des "bounce profiles"
- Élaborer des passerelles virtuelles
- Réaliser le filtrage de contenus

7 - Détailler le sacan des contenus
- Paramétrer la détection d'objet intégré
- Identifier les pièces jointes non protégées ou protégées par mot de passe
- Analyser des identifiants "intelligents"
- Crypter les messages

8 - Le paramétrage d'une demande chiffrée
- Répondre avec le "Cisco Registered Envelope Service"
- Répondre avec un Serveur local de clés
- Dans une action de chiffrement lier une action de filtrage
- Paramétrer des demandes LDAP

9 - Présentation de LDAP
- Jetons et opérateurs de demandes
- Paramétrer un profil LDAP ainsi que des "Call-Ahead" SMTP
- Appliquer les demandes groupées LDAP
- Routage LDAP et "masquerading"

10 - Appliquer LDAP pour des demandes de routage des messages
- LDAP et"pipe-line"
- Paramétrer les demandes de routage
- Contrôler le routage LDAP
- Appliquer LDAP pour les requêtes déguisées
- Paramétrage du filtrage des messages

11 - Présentation du filtrage des emails
- Overview
- Administrer le filtrage des messages
- Paramétrer TLS

12 - Présentation de TLS
- Paramétrer TLS
- Identification des emails

13 - Résoudre les problèmes d'authentification
- Overview, signature et vérification DKIM
- Présentation de la technologie SPF et SIDF
- Vérification SPF

14 - Analyser et séparer les problèmes
- Identification des outils de dépannage
- Administrer le système

15 - Instruments pour le support
- Sauvegarder et restaurer le système
- Mettre à jour le logiciel

Réf. **CS86**
4 jours
(28h présentiel)

3 580 €HT

À DISTANCE
25/07, 03/10, 12/12
PARIS
25/07, 03/10, 12/12

Autres sites, nous consulter

Sécuriser les accès Web avec Cisco Web Security Appliance (SWSA)

ACCESSIBLE À DISTANCE

Mettre en place une solution matérielle pour garantir la sécurité des accès Web

En dépit du fait que les entreprises aient massivement déployé des anti-virus et des anti-spyware sur les postes de travail, les infections par des logiciels malveillants en provenance du web ne cessent de croître. Les proxies Web traditionnels (utilisés pour la fonction de cache et de filtrage URL par catégorie gérant les accès Internet des utilisateurs) étant désormais insuffisants lorsqu'il s'agit de se protéger contre les nouvelles menaces Internet, Cisco propose avec ses boitiers IronPort S-Series, une solution très aboutie pour garantir la sécurité du réseau. Les participants à cette formation sauront mettre en œuvre et configurer IronPort S-Series pour garantir une sécurité optimale des réseaux.

OBJECTIFS

- Apprendre à installer et à vérifier Cisco WSA
- Savoir déployer des services de proxy
- Comprendre comment utiliser l'authentification
- Être en mesure de configurer des stratégies
- Pouvoir mettre en place une défense contre les logiciels malveillants
- Savoir configurer des stratégies de sécurité des données
- Comprendre comment mettre en œuvre l'administration et le dépannage
- Se préparer à l'examen Securing the Web with Cisco Web Security Appliance (300-725 SWSA)

Public

- Architectes de sécurité
- Concepteurs de systèmes
- Administrateurs réseau
- Ingénieurs d'exploitation
- Les gestionnaires de réseau, les techniciens de réseau ou de sécurité, et les ingénieurs et gestionnaires de sécurité responsables de la sécurité Web
- Intégrateurs et partenaires Cisco

Pré-requis

Avoir des connaissances sur TCP/IP, les services DNS, SSH, FTP, SNMP, HTTP et HTTPS
Avoir de l'expérience sur le routage IP
Être certifié CCNA
Connaissances de Windows

Certification

Cette formation prépare au test 300-725 SWSA (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- La formation intègre de nombreux travaux pratiques qui favorisent une assimilation rapide et durable des thématiques abordées en cours.
- Les retours d'expérience de consultants-formateurs spécialistes de la technologie.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

Programme

1 - Description de Cisco WSA
2 - Déploiement des services de Proxy
3 - Utilisation de l'authentification
4 - Création de stratégies de décryptage pour contrôler le trafic HTTPS
5 - Défense contre les logiciels malveillants
6 - Application des paramètres de contrôle d'utilisation acceptable
7 - Sécurité des données et prévention des pertes de données
8 - Exécution de l'administration et du dépannage
9 - Références

Réf. CS87
2 jours
(14h présentiel)

2 060 €HT

À DISTANCE Autres sites, nous consulter
10/10
PARIS
10/10

Tél : 0 825 07 6000 • espace.clients@ib.cegos.fr • www.ib-formation.fr

Implémenter et configurer Cisco Identity Services Engine (SISE)

ACCESSIBLE À DISTANCE

Contrôler l'accès et maîtriser les menaces

En raison du nombre croissant d'équipements interconnectés (PC, tablettes, smartphones, téléphones IP,...) et de la variété des modes d'accès aux réseaux des entreprises (Internet, VPN,...), garantir la sécurité des accès aux données de l'entreprise s'avère aujourd'hui plus complexe qu'auparavant... Leader des équipements réseaux, Cisco propose, à travers son offre ISE, une solution éprouvée qui permet de centraliser et unifier la gestion de la stratégie d'accès au réseau pour fournir un accès cohérent et sécurisé à chaque utilisateur et appareil, et ainsi réduire les risques. A l'issue de cette formation de 5 jours, les participants auront acquis les connaissances et compétences nécessaires à la mise en œuvre d'Identity Services Engine au sein de leur organisation.

OBJECTIFS

- **Décrire les déploiements Cisco ISE, y compris les composants de base du déploiement et comment ils interagissent pour créer une architecture de sécurité cohésive**
- **Décrire les avantages d'un tel déploiement et comment chaque capacité Cisco ISE contribue à ces avantages**
- **Comprendre comment les stratégies Cisco ISE sont utilisés pour mettre en œuvre l'authentification et l'autorisation, et comment exploiter cette capacité pour répondre aux besoins de votre organisation**
- **Décrire les dispositifs d'accès au réseau (NAD) tiers, Cisco TrustSec et Easy Connect**
- **Être capable de configurer l'authentification Web, les processus, le fonctionnement et les services invités, y compris les composants d'accès invités et divers scénarios d'accès invités**
- **Pouvoir configurer une solution BYOD et décrire la relation entre les processus BYOD et leurs composantes de configuration connexes**
- **Décrire et configurer les différents certificats liés à une solution BYOD**
- **Se préparer à l'examen Implementing and Configuring Cisco Identity Services Engine (300-715 SISE)**

Public

- Ingénieurs en sécurité des réseaux
- Administrateurs ISE
- Ingénieurs en sécurité des réseaux sans-fil
- Intégrateurs et partenaires Cisco

Pré-requis

Familiarité avec l'interface de ligne de commande (CLI) du logiciel Cisco IOS

Familiarité avec le client de mobilité sécurisé Cisco AnyConnect

Familiarité avec les systèmes d'exploitation Microsoft Windows et la norme 802.1X

Certification

Cette formation prépare au test 300-715 SISE (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- L'alternance de phases théoriques et d'exercices pratiques, les participants apprendront à utiliser Cisco ISE pour gagner en visibilité sur ce qui se passe dans leur réseau, à rationaliser la gestion des politiques de sécurité et à contribuer à l'efficacité opérationnelle.
- Les retours d'expérience de consultants-formateurs spécialistes de la technologie.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

Programme

1 - Présentation de l'architecture et du déploiement de Cisco ISE
- Utilisation de Cisco ISE comme moteur de stratégie d'accès au réseau
- Cas d'utilisation Cisco ISE
- Description des fonctions de Cisco ISE
- Modèles de déploiement Cisco ISE
- Visibilité du contexte

2 - Application de la politique ISE de Cisco
- Utilisation de 802.1X pour l'accès câblé et sans-fil
- Utilisation du contournement de l'authentification MAC pour l'accès câblé et sans-fil
- Introduction à la gestion des identités
- Configuration des services de certificats
- Présentation de la stratégie ISE de Cisco
- Mise en œuvre de la prise en charge des périphériques d'accès réseau tiers
- Présentation de Cisco TrustSec
- Configuration Cisco TrustSec
- Easy Connect

3 - Authentification Web et service aux invités
- Introduction de l'accès Web avec Cisco ISE
- Présentation des composants de l'accès invité
- Configuration des paramètres d'accès invité
- Configuration des portails de sponsors et d'invités

4 - Cisco ISE Profiler
- Présentation de Cisco ISE Profiler
- Déploiement du profilage et pratiques exemplaires

5 - Cisco ISE BYOD
- Présentation du processus Cisco ISE BYOD
- Description du flux de BYOD
- Configuration du portail Mes appareils
- Configuration des certificats dans les scénarios BYOD

6 - Services de conformité des points d'accès Cisco ISE
- Présentation des services de conformité des points d'accès
- Configuration des services de posture client et de provisionnement dans Cisco ISE

7 - Travailler avec des dispositifs d'accès au réseau
- La TACACS+
- Administration des dispositifs Cisco ISE TACACS
- Configurer l'administration des dispositifs TACACS
- Lignes directrices et best practices de la TACACS+ en matière d'administration des dispositifs
- Migration de Cisco ACS vers Cisco ISE

Réf. **CS98**
5 jours
(35h présentiel)

4 080 €HT

À DISTANCE
12/09, 05/12
PARIS
12/09, 05/12

Autres sites, nous consulter

Implémenter des solutions sécurisées avec les Virtual Private Networks Cisco (SVPN)

Sécuriser les réseaux

ACCESSIBLE À DISTANCE

OBJECTIFS

- Être capable de présenter les options VPN de site à site ou d'accès à distance disponibles sur les routeurs et pare-feux Cisco
- Pouvoir examiner les options de conception de VPN de site à site et d'accès à distance
- Passer en revue les processus de dépannage pour les différentes options VPN disponibles sur le routeur et les pare-feu Cisco

Public

- Ingénieur sécurité réseaux
- Candidat à la CCNP Security

Pré-requis

Avoir suivi les formations "Implémentation et administration des solutions Cisco (CCNA)" (CS100) et "Implémenter et exploiter les technologies Cisco Security Core (SCOR)" (CS130) ou connaissances équivalentes

Certification

Cette formation prépare au test 300-730 SVPN (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- Cette formation permet aux participants d'acquérir les connaissances nécessaires à l'implémentation, la configuration, la surveillance et la prise en charge des solutions de réseau privé virtuel (VPN) d'entreprise.
- La formation intègre de nombreux travaux pratiques qui favorisent une assimilation rapide et durable des thématiques abordées en cours.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

Programme

1 - Introduction aux principes fondamentaux de la technologie VPN
2 - Mise en œuvre de solutions VPN de site à site
3 - Mise en œuvre du système d'exploitation Cisco Internetwork (Cisco IOS) Solutions FlexVPN site à site
4 - Mise en œuvre des solutions VPN de transport crypté du groupe Cisco IOS (GET)
5 - Implantation des VPN Anyconnect de Cisco
6 - Mise en œuvre des VPN sans client

Réf. CS133
5 jours
(35h présentiel)

4 080 €HT

À DISTANCE
13/06, 17/10
PARIS
13/06, 17/10

Autres sites, nous consulter

Pour vous inscrire à une formation... il y a toujours un moyen de nous contacter

Par téléphone

Nos Conseillers Formation sont joignables de 8h30 à 18h00 au 0 825 07 6000. Ils répondront à toutes vos questions concernant les formations, les dates de sessions, les opportunités de dernière minute...

Par e-mail

Une adresse unique : espace.clients@ib.cegos.fr pour toutes vos inscriptions ou demandes de renseignements.

Par Internet

Retrouvez sur www.ib-formation.fr l'intégralité de nos programmes ainsi que toutes les informations qui vous seront utiles : dates de sessions, plans d'accès, offres de dernière minute, informations sur les évènements ib....

Sécuriser les réseaux avec les firewalls de dernière génération Cisco Firepower (SSNGFW)

ACCESSIBLE À DISTANCE

Protéger les réseaux avec un pare-feu de dernière génération Cisco Firepower

OBJECTIFS

- Décrire les concepts clés des technologies NGIPS et NGFW et du système de défense contre les menaces Cisco Firepower, et identifier les scénarios de déploiement
- Effectuer les tâches initiales de configuration et d'installation des dispositifs de défense contre les menaces de Cisco Firepower
- Décrire comment gérer le trafic et mettre en œuvre la qualité de service (QoS) en utilisant Cisco Firepower Threat Defense
- Décrire comment mettre en œuvre la NAT en utilisant Cisco Firepower Threat Defense
- Effectuer une découverte initiale du réseau, en utilisant Cisco Firepower pour identifier les hôtes, les applications et les services
- Décrire le comportement, l'utilisation et la procédure de mise en œuvre des politiques de contrôle d'accès
- Décrire les concepts et les procédures de mise en œuvre des caractéristiques du renseignement de sécurité
- Se préparer à l'examen Securing Networks with Cisco Firepower (300-710 SNCF)

Public

- Administrateurs de la sécurité
- Conseillers en sécurité
- Administrateurs réseau
- Ingénieurs système
- Personnel de soutien technique
- Partenaires de distribution et revendeurs

Pré-requis

Compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau

Connaissance de base des concepts de pare-feu et d'IPS

Certification

Cette formation prépare au test 300-710 SNCF (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- Cette formation permet aux participants d'apprendre à déployer et à utiliser le système de défense Cisco Firepower Threat Defense.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

Programme

1 - Aperçu de Cisco Firepower Threat Defense
- Examen de la technologie des pares-feux et IPS
- Caractéristiques et composants de Firepower Threat Defense
- Examen des plates-formes de Firepower
- Cas d'utilisation de la mise en œuvre de Cisco Firepower

2 - Configuration du dispositif Cisco Firepower NGFW
- Enregistrement des dispositifs à Firepower Threat Defense
- FXOS et Firepower Device Manager
- Configuration initiale de l'appareil
- Gestion des dispositifs de NGFW
- Examen des politiques du Centre de gestion de Firepower
- Examen des objets
- Examen de la configuration du système et de la surveillance de la santé
- Gestion des appareils
- Examen de la haute disponibilité de Firepower
- Configuration de la haute disponibilité
- Migration de Cisco ASA vers Firepower
- Migration de Cisco ASA vers Firepower Threat Defense

3 - Contrôle du trafic de Cisco Firepower NGFW
- Traitement des paquets de Firepower Threat Defense
- Mise en œuvre de la QoS
- Contournement de la circulation

4 - Traduction d'adresses Cisco Firepower NGFW
- Principes de base du NAT
- Implémentation de NAT
- Exemples de règles NAT
- Implémentation de NAT

5 - Découverte de Cisco Firepower (Cisco Firepower Discovery)
- Examen de la découverte du réseau
- Configuration de la découverte du réseau
- Mise en œuvre des politiques de contrôle d'accès
- Examen des politiques de contrôle d'accès
- Examen des règles de la politique de contrôle d'accès et des mesures par défaut
- Mise en œuvre d'une inspection plus poussée
- Examen des événements de connexion
- Politique de contrôle d'accès Paramètres avancés
- Considérations relatives à la politique de contrôle d'accès
- Mise en œuvre d'une politique de contrôle d'accès

6 - Security Intelligence
- Examen de Security Intelligence
- Examen des objets de Security Intelligence
- Déploiement et enregistrement de Security Intelligence
- Mise en œuvre de Security Intelligence

7 - Contrôle des fichiers et protection avancée contre les logiciels malveillants
- Examen des logiciels malveillants et de la politique des fichiers
- Examen de la protection avancée contre les logiciels malveillants

8 - Systèmes Next-generation de prévention des intrusions
- Examen de la prévention des intrusions et des règles de Snort
- Examen des variables et des ensembles de variables
- Examen des politiques d'intrusion

9 - VPN de site-à-site
- Examen d'IPsec
- Configuration VPN de site à site
- Dépannage VPN de site à site
- Mise en place d'un VPN de site à site

10 - VPN d'accès à distance
- Examen du VPN d'accès à distance
- Examen de la cryptographie à clé publique et des certificats
- Inscription au certificat d'examen
- Configuration du VPN d'accès à distance
- Mise en œuvre d'un VPN d'accès à distance

11 - Décryptage SSL
- Examen du décryptage SSL
- Configuration des politiques SSL
- Best Practices et surveillance du décryptage SSL

12 - Techniques d'analyse détaillée
- Examen de l'analyse des événements
- Examen des types d'événements
- Examen des données contextuelles
- Examen des outils d'analyse
- Analyse de la menace

13 - Administration du système
- Gestion des mises à jour
- Examen des caractéristiques de la gestion des comptes utilisateurs
- Configuration des comptes d'utilisateur
- Administration du système

14 - Dépannage de Cisco Firepower
- Examen des erreurs de configuration courantes
- Examen des commandes de dépannage
- Dépannage de Firepower

Réf. CS131
5 jours
(35h présentiel)

4 280 €HT

À DISTANCE
19/09, 28/11

PARIS
19/09, 28/11

Autres sites, nous consulter

Sécuriser les réseaux avec les IPS de dernière génération Cisco Firepower (SSFIPS)

ACCESSIBLE À DISTANCE

Prévenir les intrusions avec un pare-feu de dernière génération Cisco Firepower

OBJECTIFS

- Décrire les composants de Cisco Firepower Threat Defense et le processus d'enregistrement des périphériques gérés
- Être capable de détailler le contrôle du trafic des pare-feu Next-Generation (NGFW) et configurer le système Cisco Firepower pour la découverte du réseau
- Savoir mettre en place des politiques de contrôle d'accès et décrire les fonctionnalités avancées de la politique de contrôle d'accès
- Comprendre comment configurer les fonctions d'intelligence de sécurité et la procédure de mise en œuvre de la protection avancée contre les logiciels malveillants (AMP) pour les réseaux pour le contrôle des fichiers et la protection avancée contre les logiciels malveillants
- Pouvoir mettre en œuvre et gérer les politiques d'analyse d'intrusion et de réseau pour l'inspection du NGIPS
- Être en mesure de décrire et démontrer les techniques d'analyse détaillée et les fonctions de rapport fournies par le Cisco Firepower Management Center
- Comprendre comment intégrer le Cisco Firepower Management Center avec une destination de journalisation externe
- Savoir décrire et démontrer les options d'alerte externe disponibles dans le Cisco Firepower Management Center et configurer une politique de corrélation

Programme

1 - Aperçu de Cisco Firepower Threat Defense
2 - Configuration du dispositif Cisco Firepower NGFW
3 - Contrôle du trafic Cisco Firepower NGFW
4 - Découverte de Cisco Firepower
5 - Mise en œuvre des politiques de contrôle d'accès
6 - Renseignement de sécurité
7 - Contrôle des fichiers et protection avancée contre les logiciels malveillants
8 - Systèmes de prévention des intrusions de nouvelle génération
9 - Politiques d'analyse de réseau
10 - Techniques d'analyse détaillée
11 - Intégration de la plate-forme Cisco Firepower
12 - Politiques d'alerte et de corrélation
13 - Administration du système
14 - Dépannage de Cisco Firepower

Public

- Professionnels techniques qui souhaitent apprendre à déployer et à gérer un Cisco Firepower NGIPS dans leur environnement réseau
- Administrateurs sécurité
- Conseillers en sécurité
- Administrateurs réseau
- Ingénieurs système
- Personnel de soutien technique
- Partenaires de distribution et revendeurs

Pré-requis

Compréhension technique des réseaux TCP/IP et de l'architecture des réseaux

Connaissance de base des concepts de systèmes de détection d'intrusion (IDS) et IPS

Certification

Cette formation prépare au test 300-710 SNCF (en option) qui permet d'obtenir la certification Cisco Certified Network Professional Security (CCNP Security)

Les + de cette formation

- Cette formation permettra aux participants d'apprendre à déployer et à utiliser le Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS).
- Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de mise en pratique et de partages d'expériences.
- La qualité d'une formation officielle Cisco (support de cours numérique en anglais).

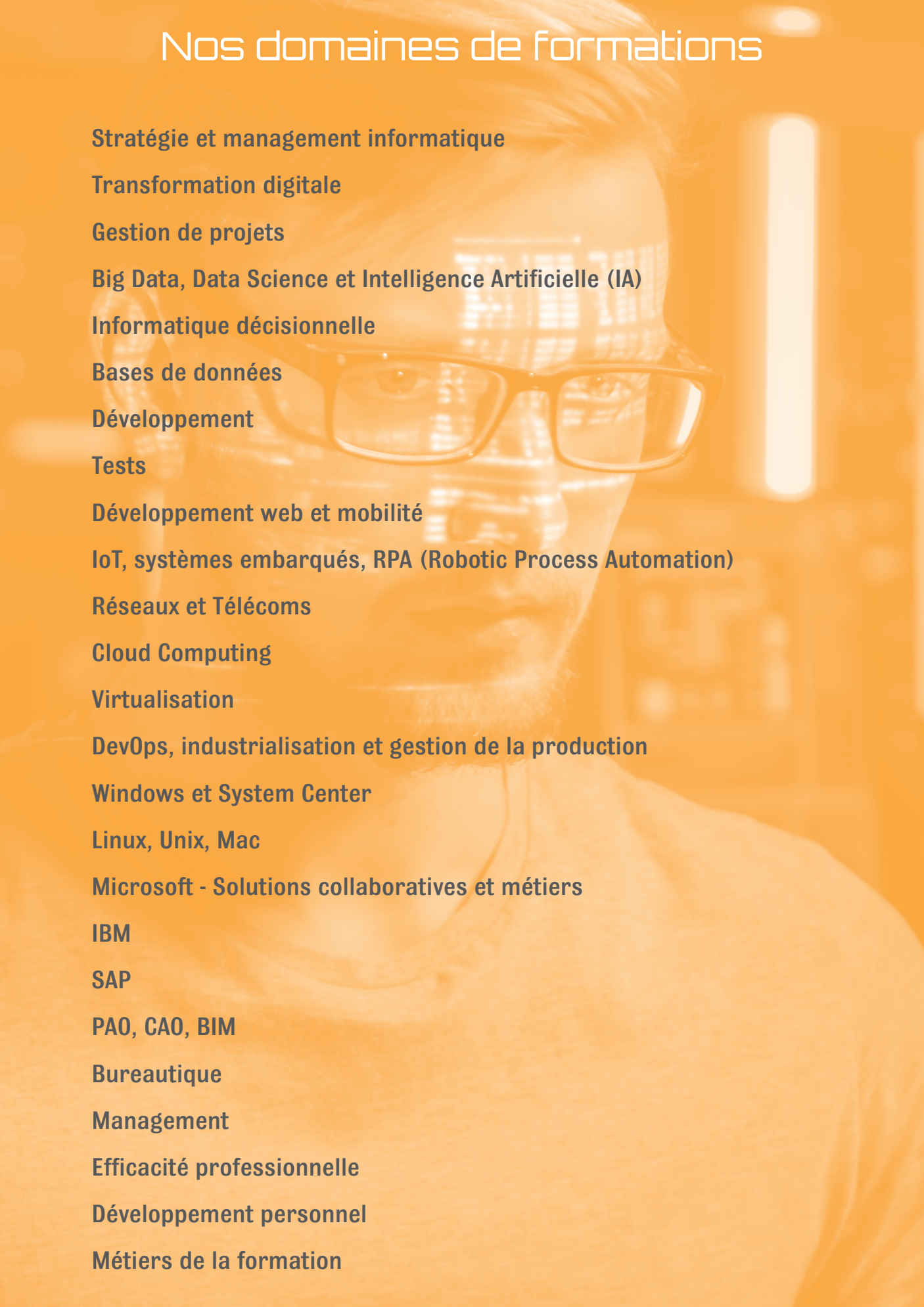
Réf. CS132
5 jours
(35h présentiel)

4 280 €HT

À DISTANCE
26/09, 05/12
PARIS
26/09, 05/12

Autres sites, nous consulter

Nos domaines de formations



Stratégie et management informatique

Transformation digitale

Gestion de projets

Big Data, Data Science et Intelligence Artificielle (IA)

Informatique décisionnelle

Bases de données

Développement

Tests

Développement web et mobilité

IoT, systèmes embarqués, RPA (Robotic Process Automation)

Réseaux et Télécoms

Cloud Computing

Virtualisation

DevOps, industrialisation et gestion de la production

Windows et System Center

Linux, Unix, Mac

Microsoft - Solutions collaboratives et métiers

IBM

SAP

PAO, CAO, BIM

Bureautique

Management

Efficacité professionnelle

Développement personnel

Métiers de la formation

PARIS LA DÉFENSE
Tour Atlantique
1, place de la Pyramide
La Défense 9 - 92911 Paris La Défense
Tél : 01 41 99 20 20

LYON
Le 6ème Sens
186, avenue Thiers
69465 Lyon Cedex 06
Tél : 04 72 68 60 60

AIX-EN-PROVENCE
Pôle d'activités d'Aix-en-Provence
Espace Cézanne
135, rue André Ampère
13290 Aix-en-Provence
Tél : 04 65 07 08 39

TOULOUSE
Immeuble TEA - Innoparc A
41, rue de la Découverte
31676 Labège Cedex
CS 37621
Tél : 05 62 24 75 14

BORDEAUX
9, rue de Condé
33064 Bordeaux
Tél : 05 56 00 43 01

NANTES
Immeuble Atalante 2
ZAC du Moulin Neuf
2, impasse Augustin Fresnel
44822 Saint Herblain Cedex
Tél : 02 51 89 99 58

RENNES
ZAC de Saint Sulpice
Immeuble Osiris II
12J, rue du Patis Tatelin
35000 Rennes
Tél : 02 23 45 69 60

ROUEN
Parc d'Activités Technologiques
de la Vatine
8, rue Pierre Gilles de Gennes
76130 Mont-Saint-Aignan
Tél : 02 79 16 01 96

LILLE
Immeuble Le Corbusier
19, avenue Le Corbusier
59000 Lille
Tél : 03 67 18 20 30

STRASBOURG
Immeuble l'Avancée
26C, bd du Président Wilson
67000 Strasbourg
Tél : 03 88 23 91 40

Sophia-Antipolis
400, avenue Roumanille
Village d'Entreprises Green Side
Bâtiment Baya Axess
BP 309 - 06906 Sophia-Antipolis

Service Conseil Clients
Tél : 0 825 07 6000
Fax : 0 825 07 6005

www.ib-formation.fr