ACG | Cybersecurity

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

ACG CYBERACADEMY

Catalogue de Formations
Formations & Sensibilisation

Le Leader de l'Innovation en Formation et le Développement des Compétences en Cybersécurité

NOTRE HISTOIRE, NOTRE MISSION

ACG CyberAcademy. Là où se forment les experts de demain !

Dans un monde numérique en constante accélération, la cybersécurité n'est plus une option : c'est une priorité stratégique.

Chez ACG CyberAcademy, nous avons conçu l'un des catalogues de formation les plus complets et spécialisés du marché, intégralement tourné vers les enjeux actuels et futurs de la cybersécurité.

Objectif : former des professionnels immédiatement opérationnels, capables de répondre aux défis concrets des organisations, aujourd'hui et demain.

Gouvernance, gestion des risques, audit, conformité, SOC, sécurité offensive, cloud, NIS2, ISO… Chaque programme est pensé pour renforcer l'expertise, cultiver la posture cyber et soutenir la performance des organisations.

Grâce à un réseau de partenaires stratégiques et un ancrage fort dans l'écosystème, nous offrons un accès privilégié à des contenus de pointe, certifiants, finançables et animés par des experts du terrain.

Former. Accompagner. Faire grandir. Rejoignez une communauté engagée, prête à bâtir la cybersécurité de demain.

Bienvenue chez ACG CyberAcademy.

L'équipe ACG CyberAcademy

PRÉSENTATION

Chez ACG Cybersecurity nous comprenons les défis croissants des entreprises dues aux évolutions rapides des menaces numériques. C'est pourquoi, nous avons créé un centre de formation dédié à la sécurité de l'information : « ACG CyberAcademy ».

En tant que pure player de la cybersécurité, nous mettons notre expertise de pointe au service de votre protection numérique, la sécurité de vos systèmes d'information, la gestion des risques ou le développement de votre stratégie cyber. ACG CyberAcademy permettra de faire monter en compétences vos collaborateurs, via des formations certifiantes et des parcours spécifiques.

Grâce à différents partenariats stratégiques, nous offrons une large gamme de formations, allant de la sensibilisation à la gouvernance, en passant par des parcours académiques (Executive MBAs).

Nous sommes certifiés Qualiopi afin de vous offrir des formations et certifications de qualité, et notre CEO a été récompensé cinq années de suite **« Best French Trainer »** par notre partenaire Gold PECB. Nos formateurs, experts dans le domaine, s'engagent à adapter leurs approches à vos besoins et accordent la priorité à votre satisfaction.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

ACG CyberAcademy, l'assemblée des experts Cyber.

ACG CYBERSECURITY est certifié ISO 27001 - 2022.

Une certification ISO 27001 sur nos principales activités (formation, audit et consulting cybersécurité).

ACG CYBERSECURITY est certifié PASSI.

Cette reconnaissance par l'ANSSI met en valeur notre expertise en audits de sécurité, tests d'intrusion et conseil, garantissant les normes Les Plus élevées en matière de cybersécurité

ACG CYBERSECURITY est partenaire de SWIFT CSP.

ACG CYBERSECURITY est membre de la fédération française de la Cybersécurité.

ACG CYBERSECURITY est membre de :

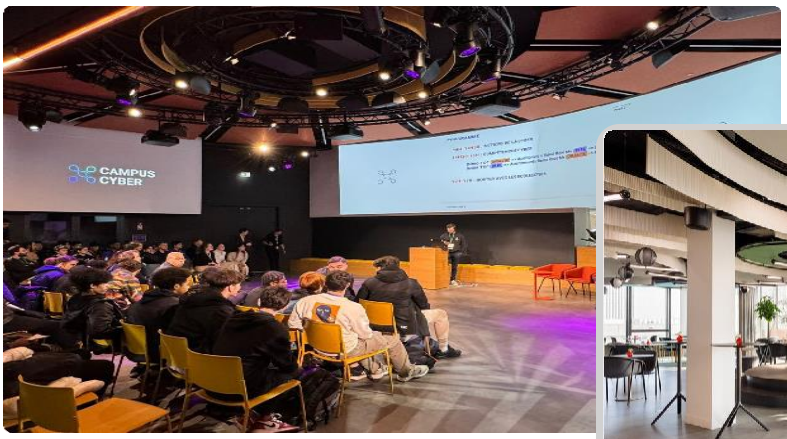
Club EBIOS

Alliance pour la Confiance Numérique

ACG CYBERSECURITY référencé officiellement comme Prestataire de Terrain par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

NOTRE CENTRE DE FORMATION
ACG CYBERACADEMY

ACG Cybersecurity est membre associé du Campus Cyber, lieu totem de la cybersécurité en France qui rassemble les principaux acteurs nationaux et internationaux du domaine.



Nos partenaires de certification

PECB ISACA mile2 CompTIA EC-Council ISC2

ACG Cybersecurity

ACG Cybersecurity membre associé et résident du Campus Cyber

Un engagement pour le développement de nos activités et services dans un éco-système international de la Cybersécurité.

CAMPUS CYBER RÉSIDENT · CAMPUS CYBER ASSOCIÉ · CAMPUS CYBER ACTEUR ENGAGÉ

Adresse : Tour Eria, 5-7 rue Bellini, 92800 Puteaux, FRANCE

Sommaire

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/IEC 27001:2022 Transition

Objectifs

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

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Personnes souhaitant rester à jour avec les exigences de la norme ISO/IEC 27001 pour un SMSI.
- Personnes cherchant à comprendre les différences entre les exigences de la norme ISO/IEC 27001:2013 et celles de la norme ISO/ IEC 27001:2022.
- Personnes chargées d'assurer la transition d'un SMSI de la norme ISO/IEC 27001:2013 à la norme ISO/IEC 27001:2022.
- Responsables, formateurs et consultants impliqués dans le maintien d'un SMSI.
- Professionnels souhaitant mettre à jour leur certification à la norme ISO/IEC 27001.

Programme

Jour 1

- Introduction à la norme ISO/IEC 27001:2022 et comparaison avec la norme ISO/IEC 27001:2013.

Jour 2

- Comparaison entre les mesures de l'Annexe A de la norme ISO/IEC 27001:2013 et de la norme ISO/IEC 27001:2022.
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/IEC 27001:2022 Foundation

Objectifs

- Comprendre la mise en œuvre des mesures de sécurité de l'information conformément à la norme ISO/CEI 27002.
- Comprendre la corrélation entre les normes ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes et cadres réglementaires.
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information.

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne impliquée dans le management de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information

Programme

Jour 1

- Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001:2022

Jour 2

- Exigences relatives au Système de management de la sécurité de l'information
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/CEI 27001:2022 Lead Implementer

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.
- Maîtrisez 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.

Prérequis de la Formation

- Pour suivre cette formation ISO 27001 Lead Implementer, une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre sont demandées.

Audience Ciblée

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

Programme

Jour 1

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

Jour 2

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

Jour 3

- Mise en œuvre d'un SMSI.

Jour 4

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

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/CEI 27001:2022 Lead Auditor

Objectifs

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

Prérequis de la Formation

- Pour suivre cette formation ISO 27001 Lead Auditor, une connaissance préalable de la norme ISO 27001 ainsi que des connaissances approfondies sur les principes de l'audit sont nécessaires.

Audience Ciblée

- Auditeurs souhaitant effectuer et diriger des audits de certification du système de management de sécurité de l'information (SMSI)
- Managers ou consultants souhaitant maîtriser le processus d'audit d'un système de management de sécurité de l'information
- Personnes responsables de maintenir la conformité aux exigences du système de management de sécurité de l'information.
- Experts techniques souhaitant se préparer à un audit du système de management de sécurité de l'information.
- Conseillers experts en management de sécurité de l'information

Programme

Jour 1

- Introduction au Système de management de la sécurité de l'information et à la norme ISO/CEI 27001.

Jour 2

- Principes, préparation et déclenchement de l'audit.

Jour 3

- Activités d'audit sur site.

Jour 4

- Clôture de l'audit.

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/IEC 27002 Foundation

Objectifs

- Comprendre la mise en œuvre des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002
- Comprendre la corrélation entre les normes ISO/IEC 27001 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

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

Programme

Jour 1

- Introduction à la norme ISO/IEC 27002 et au Système de management de la sécurité de l'information

Jour 2

- Mesures ISO/IEC 27002
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/CEI 27002 Lead Manager

Objectifs

- Expliquer les concepts fondamentaux de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée conformément à la norme ISO/CEI 27002
- Comprendre la relation entre les normes ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires
- Interpréter les mesures de sécurité de l'information de la norme ISO/IEC 27002 dans le contexte spécifique d'un organisme
- Soutenir une organisation dans la définition, la mise en œuvre et la gestion efficaces des mesures de sécurité de l'information conformément à la norme ISO/CEI 27002
- Expliquer les approches et les techniques utilisées pour la mise en œuvre et la gestion efficace des mesures de la sécurité de l'information

Prérequis de la Formation

Pour participer à cette formation, il faut avoir une connaissance fondamentale de la norme ISO/IEC 27002 et une connaissance approfondie des mesures de sécurité de l'information.

Audience Ciblée

- Managers ou consultants cherchant à améliorer leurs connaissances concernant la mise en œuvre des mesures de sécurité de l'information dans un SMSI conformément à la norme ISO/IEC 27001
- Personnes responsables de la gestion de la sécurité de l'information, de la conformité, du risque ou de la gouvernance dans une organisation
- Professionnels de l'informatique ou consultants souhaitant améliorer leurs connaissances en matière de sécurité de l'information
- Membres d'une équipe de mise en œuvre d'un SMSI ou de la sécurité de l'information

Programme

Jour 1

- Introduction à la norme ISO/IEC 27002.

Jour 2

- Rôles et responsabilités en matière de sécurité de l'information, de mesures relatives aux personnes et de mesures physiques.

Jour 3

- Actifs de sécurité de l'information, contrôles d'accès et protection des systèmes et réseaux d'information.

Jour 4

- Gestion des incidents de sécurité de l'information et test et surveillance des mesures de sécurité de l'information conformément à la norme ISO/IEC 27002

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/CEI 27035 Foundation

Objectifs

- Comprendre les concepts fondamentaux de la gestion des incidents de sécurité de l'information
- Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres règlementaires
- Comprendre l'approche processus permettant de gérer efficacement les incidents de sécurité de l'information

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne intéressée par l'approche processus de gestion des incidents de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances sur les principes et concepts de gestion des incidents de sécurité d'information
- Personnes souhaitant poursuivre une carrière dans la gestion des incidents de sécurité de l'information

Programme

Jour 1

- Introduction aux principes et concepts fondamentaux de la gestion des incidents de la sécurité de l'information, tels que définis par la norme ISO/CEI 27035

Jour 2

- Approches processus de gestion des incidents de la sécurité de l'information
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED ISO/IEC 27035 Lead Incident Manager

Objectifs

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

Prérequis de la Formation

- Avoir une bonne connaissance des processus de gestion des incidents, des principes de sécurité de l'information et de la famille de normes ISO/IEC 27000.

Audience Ciblée

- 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.
- Membres de l'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.
- Personnes responsables de la sécurité de l'information au sein d'une organisation.

Programme

Jour 1

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

Jour 2

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

Jour 3

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

Jour 4

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

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

PECB CERTIFIED Chief Information Security Officer

Objectifs

- D'expliquer les principes et concepts fondamentaux de la sécurité de l'information
- De comprendre les rôles et les responsabilités du RSSI, les considérations éthiques qu'ils impliquent et aborder les défis associés à ce rôle
- De concevoir et d'élaborer un programme de sécurité de l'information efficace, adapté aux besoins de l'organisme
- D'adopter les cadres, lois et règlements applicables.
- De communiquer et de mettre en œuvre des politiques efficaces visant à assurer la conformité de la sécurité de l'information
- D'identifier, d'analyser, d'évaluer et de traiter les risques liés à la sécurité de l'information, en utilisant une approche systématique et efficace

Prérequis de la Formation

La principale condition pour participer à cette formation est d'avoir une compréhension fondamentale des principes et des concepts de la sécurité de l'information.

Audience Ciblée

- Professionnels activement impliqués dans la gestion de la sécurité de l'information
- Responsables informatiques chargés de superviser les programmes de sécurité de l'information
- Professionnels de la sécurité qui aspirent à accéder à des postes de direction, tels que les architectes de la sécurité, les analystes de la sécurité et les auditeurs de la sécurité
- Professionnels responsables de la gestion des risques et de la conformité en matière de sécurité de l'information au sein des organismes
- RSSI expérimentés désireux d'améliorer leurs connaissances, de rester à jour sur les dernières tendances et d'affiner leurs compétences en matière de leadership
- Cadres, y compris les DSI, les PDG et les directeurs de l'exploitation, qui jouent un rôle crucial dans les processus de prise de décision liés à la sécurité de l'information
- Professionnels souhaitant accéder à des postes de direction dans le domaine de la sécurité de l'information

Programme

Jour 1

- Fondamentaux de la sécurité de l'information et rôle d'un RSSI

Jour 2

- Programme de conformité en matière de sécurité de l'information, gestion des risques, architecture et conception de la sécurité

Jour 3

- Mesures de sécurité, gestion des incidents et gestion des changements

Jour 4

- Sensibilisation à la sécurité de l'information, surveillance et mesurage, amélioration continue

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

ISACA CERTIFIED Information Security Manager

Objectifs

- Apprendre les processus et les meilleures pratiques pour gérer et évaluer les risques liés à la sécurité de l'information.
- Développez les compétences nécessaires pour concevoir et mettre en œuvre un programme de sécurité de l'information qui s'aligne sur Objectifs et les stratégies d'une organisation.

Prérequis de la Formation

Pour être éligible à passer l'examen CISM, vous devez avoir cinq ans ou plus d'expérience professionnelle dans la sécurité de l'information. Au moins trois de ces années doivent être réparties dans un minimum de trois domaines de pratique professionnelle, avec une année ou plus dans chacun. Ces domaines comprennent la gestion de la sécurité de l'information.

Audience Ciblée

CISM s'adresse aux professionnels de la sécurité de l'information ayant au moins cinq années d'expérience professionnelle pertinente, dont au moins trois années dans le rôle de responsable de la sécurité de l'information. Les titres de poste incluent :

- CISO (Chief Information Security Officer).
- CSO (Chief Security Officer).
- Directeur/Gestionnaire/Consultant en Sécurité.
- Directeur/Gestionnaire/Consultant en Technologies de l'Information (TI).
- Directeur et Gestionnaire en Conformité / Risques / Vie privée.

Programme

Domaine 1

- Gouvernance de la sécurité de l'information.

Domaine 2

- Gestion des risques liés à la sécurité de l'information.

Domaine 3

- Programme de sécurité de l'information.

Domaine 4

- Gestion des incidents.

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

ISACA CERTIFIED Information Systems Auditor

Objectifs

- Développer et mettre en œuvre une stratégie d'audit informatique basée sur les normes d'audit informatique.
- Planifier des audits spécifiques pour déterminer si les systèmes d'information sont protégés, contrôlés et apportent de la valeur à l'organisation.
- Mener des audits conformément aux normes d'audit informatique pour atteindre Objectifs d'audit planifiés.
- Rapporter les conclusions de l'audit et formuler des recommandations aux parties prenantes clés pour communiquer les résultats et apporter des changements lorsque nécessaire.
- Effectuer des suivis ou préparer des rapports d'état pour s'assurer que des mesures appropriées ont été prises par la direction en temps opportun.

Prérequis de la Formation

- Un an d'expérience en tant qu'auditeur de systèmes d'information. Vous pouvez également soumettre un an d'expérience en audit non informatique. Un diplôme de deux ou quatre ans peut être substitué à l'exigence d'expérience, à condition que votre diplôme ait été obtenu au cours des 10 dernières années.

Audience Ciblée

Professionnels en début de carrière à mi-carrière cherchant à obtenir une reconnaissance et une crédibilité accrues dans leurs interactions avec les parties prenantes internes et externes, les régulateurs et les clients. Les rôles professionnels incluent :

- Directeurs/Responsables/Consultants en audit informatique.
- Auditeurs informatiques et internes.
- Directeurs de la conformité, des risques et de la confidentialité.
- Directeurs / Responsables / Consultants en informatique.

Programme

Domaine 1

- Processus d'audit du système d'information.

Domaine 2

- Gouvernance et gestion des technologies de l'information.

Domaine 3

- Acquisition, développement et mise en œuvre de systèmes d'information.

Domaine 4

- Exploitation des systèmes d'information et résilience de l'entreprise.

Domaine 5

- Protection des actifs informationnels.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CISA

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

MILE2 CERTIFIED Information System Security Officer

Objectifs

Upon completion, Certified Information Systems Security Officer students be able to establish industry acceptable Cyber Security and Information Systems management standards with current best practices.

Prérequis de la Formation

- Mile2's C)SP
- Mile2's C)ISSM
- 12 months of Information Systems Management Experience

Audience Ciblée

- IS Security Officers
- IS Managers
- Risk Managers
- Auditors
- Info Systems Owners
- IS Control Assessors
- System Managers
- Government Employees

Programme

Module 1
- Risk Management

Module 2
- Security Management

Module 3
- Identification and Authentication

Module 4
- Access Control

Module 5
- Security Models and Evaluation Criteria

Module 6
- Operations Security

Module 7
- Vulnerability Assessments

Module 8
- Symmetric Cryptography and Hashing

Module 9
- Network Connections

Module 10
- Network Protocols and Devices

Module 11
- Telephony, VPNs, and Wireless

Module 12
- Security Architecture and Attacks

Module 13
- Software Development Security

Module 14
- Database Security

Module 15
- Malware and Attacks XVI

Module 16
- Business Continuity

Module 17
- Incident Management, Law and Ethics

Module 18
- Physical Security

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 300

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Cybersécurité Industrielle

Objectifs

- Sensibiliser aux risques OT avec des cas concrets d'attaques (Stuxnet, Colonial Pipeline, etc.).
- Présenter les bonnes pratiques élémentaires pour réduire la surface d'exposition.
- Engager les parties prenantes (métiers, IT, terrain) dans une démarche collective de sécurité.

Prérequis de la Formation

- Connaissances générales en réseau ou cybersécurité.
- Sensibilité aux environnements techniques industriels

Audience Ciblée

- Opérateurs industriels, techniciens d'exploitation.
- Responsables de sites, de production ou de sécurité.
- Collaborateurs en contact avec des automates ou des systèmes OT.

Programme

- Introduction : OT vs IT – pourquoi l'OT devient stratégique
- Retours d'expérience : Stuxnet, Triton, ransomware industriels
- Bonnes pratiques essentielles : pour les opérateurs, techniciens et managers
- Jeux de rôle ou quiz interactif : identifier les erreurs de cybersécurité
- Plan d'action individuel : Q&A et remise des supports

Informations Pratiques

1/2 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Cybersécurité des systèmes industriels

Objectifs

- Expliquer les spécificités des systèmes industriels et leur exposition aux cybermenaces.
- Identifier les risques typiques liés à l'OT (Operational Technology).
- Lire et interpréter les principales exigences des normes IEC 62443 et ISO/IEC 27019.
- Proposer des mesures de protection adaptées (zonage, segmentation, durcissement).
- Initier une stratégie de cybersécurité dans un environnement industriel mixte IT/OT.

Prérequis de la Formation

- Connaissances générales en réseau ou cybersécurité.
- Sensibilité aux environnements techniques industriels

Audience Ciblée

- Ingénieurs automatisme, RSSI, exploitants de sites industriels.
- Responsables de maintenance, responsables sécurité, DSI en milieu OT.
- Consultants ou intégrateurs OT/IT.

Programme

- Accueil : panorama des cybermenaces en milieu industriel
- Comprendre les architectures OT : SCADA, PLC, DCS, IoT industriel
- Vulnérabilités : vecteurs d'attaque et spécificités OT
- Norme IEC 62443 : principes, segments, rôles, SL-Tiers
- Norme ISO/IEC 27019 : gouvernance de la sécurité pour l'énergie
- Bonnes pratiques OT : durcissement, segmentation, journalisation
- Cas pratique guidé : audit de sécurité simplifié d'un site industriel
- QCM final : plan d'action post-formation

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Sécurité des systèmes quantiques

Objectifs

- Expliquer les bases de l'ordinateur quantique et les menaces qu'il fait peser sur la cryptographie actuelle.
- Identifier les types de données et systèmes vulnérables face aux attaques quantiques.
- Analyser les enjeux de migration vers des solutions post-quantiques.
- Évaluer les grandes familles d'algorithmes post-quantiques proposés par le NIST.
- Concevoir une stratégie de veille et d'anticipation adaptée à leur environnement technique.

Prérequis de la Formation

- Bonnes connaissances générales en cybersécurité et cryptographie.
- Sensibilité aux enjeux de normalisation et anticipation technologique.

Audience Ciblée

- RSSI, architectes sécurité, responsables techniques ou innovation.
- Consultants cybersécurité, auditeurs techniques.
- Experts cryptographie ou administrateurs d'infrastructures critiques.

Programme

- Introduction : informatique quantique, état de l'art, rupture technologique

Module 1

- Impact du quantique sur la cryptographie classique (RSA, ECC, AES)

Module 2

- Algorithmes post-quantiques (lattice, hash-based, code-based, etc.)

Module 3

- Enjeux normatifs et industriels : NIST PQC, ETSI, ANSSI

Module 4

- Planification d'une migration : analyse de risques et roadmap

- Atelier final : Étude de cas d'une entreprise confrontée à une transition PQC
- Debrief, QCM de validation et clôture

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Initiation à la Cybercriminalistique

Objectifs

- Identifier les principales étapes d'une investigation numérique conforme.
- Détecter et extraire des preuves numériques sur systèmes, réseaux et environnements web.
- Comprendre comment les données sont stockées, copiées, dissimulées ou effacées.
- Appliquer les bonnes pratiques d'acquisition et de préservation de preuve.
- Utiliser des outils de base pour collecter, examiner et documenter des incidents.

Prérequis de la Formation

- Notions de base en systèmes d'exploitation et réseaux.
- Une curiosité pour la cybersécurité technique (niveau débutant à intermédiaire).

Audience Ciblée

- Professionnels IT, analystes sécurité, administrateurs systèmes/réseaux.
- Équipes SOC, CERT/CSIRT, débutants en investigation numérique.
- Étudiants et professionnels en reconversion vers la cybersécurité technique.

Programme

- Accueil & contexte : rôle de l'investigation numérique dans la cybersécurité

Module 1

- Introduction à la criminalistique numérique & processus d'investigation

Module 2

- Systèmes de fichiers, disques & acquisition des données

Module 3

- Analyse de systèmes Windows, Linux & Mac OS

Module 4

- Investigation sur réseaux, emails et incidents web

Module 5

- Forensics avancé : anti-forensics, dark web et malwares

- Atelier pratique guidé : scénario d'investigation avec artefacts
- Débrief & QCM d'évaluation

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Maîtrise Opérationnelle de la Gestion des Vulnérabilités

Objectifs

- Concevoir un processus complet de gestion des vulnérabilités conforme à l'ISO 27001, ISO 27002 et aux guides NIST.
- Cartographier les actifs à risque et intégrer les résultats de scans dans un cycle de traitement.
- Choisir les bons outils de détection, d'évaluation et de remédiation.
- Mettre en place un reporting structuré et communiquer efficacement avec la direction.
- Évaluer la maturité de leur démarche et construire un plan

Prérequis de la Formation

- Connaissances de base en infrastructure IT et en sécurité des systèmes d'information.
- Aucune certification préalable requise.

Audience Ciblée

- Responsables et techniciens IT, administrateurs systèmes et réseaux.
- Responsables cybersécurité, RSSI, analystes SOC ou ITSM.
- Toute personne impliquée dans la sécurité ou la gestion des risques techniques.

Programme

- Accueil & introduction : enjeux de la gestion des vulnérabilités
- Normes et standards : ISO 27001 / 27002, NIST SP 800-40, CIS Benchmarks
- Cycle de gestion des vulnérabilités : identification, analyse, remédiation, suivi
- Pause déjeuner
- Panorama des outils : Nessus, OpenVAS, Qualys, Tenable, Rapid7
- Atelier pratique : concevoir un processus de gestion basé sur ISO & NIST
- Cas pratique guidé : simulation de détection, analyse et réponse
- Conclusion : bonnes pratiques, pièges à éviter, plan d'action

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Gestion de crise, s'organiser pour faire face à la crise

Objectifs

- Cartographier les risques
- Développer un plan de continuité informatique
- Évaluer la gravité de la crise
- Mettre en place un dispositif de gestion de crise
- Mettre en œuvre un plan de communication de crise

Prérequis de la Formation

- Connaissances de base des composantes et du rôle d'une DSI. Expérience requise en gestion du SI.

Audience Ciblée

- Responsables SI
- Ingénieurs
- Chefs de projet et tout intervenant ayant à traiter des situations de crise.

Programme

Module 1

- Architecture d'un dispositif de crise

Module 2

- Anticipation à la gestion de crise

Module 3

- Évaluation de la crise

Module 4

- Gestion de la crise

Module 5

- La communication de crise

Module 6

- Les outils de management de crise

Module 7

- Le plan de continuité d'activité (PCA)

Module 8

- Maintenance du dispositif de crise

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Maîtriser le rôle de RSSI et piloter efficacement la gouvernance de la cybersécurité

Objectifs

- Assumer efficacement le rôle de RSSI dans la gouvernance SSI de l'organisation.
- Structurer un SMSI selon l'ISO/IEC 27001 et piloter sa mise en œuvre.
- Appliquer les méthodes d'analyse de risques via EBIOS RM et ISO 27005.
- Intégrer les bonnes pratiques de l'ANSSI pour renforcer la posture SSI.
- Définir une stratégie cybersécurité en phase avec les enjeux métier et réglementaires.

Prérequis de la Formation

- Expérience en informatique ou participation à des missions SSI

Audience Ciblée

- Futurs ou actuels RSSI
- Ingénieurs sécurité
- DSI
- Consultants SSI

Programme

Jour 1

- Gouvernance SSI et ISO/IEC 27001

Jour 2

- Analyse de risques & audit (EBIOS RM & ISO/IEC 27005)

Jour 3

- Stratégie SSI, réglementation et acteurs

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

RGPD, DPO, rôle, missions et obligations du délégué à la protection des données

Objectifs

- Maîtriser le contenu de la réglementation générale de la protection des données
- Identifier le rôle déterminant et les missions du Délégué à la Protection des Données
- Déterminer les informations à échanger avec la CNIL
- Être en mesure de mettre en place des outils de reporting et de suivi interne
- Être en capacité de mener des audits auprès des sous-traitants
- Etablir et suivre un plan d'actions, de pertes ou de vols de données ou dans le cas de transfert de données hors CE
- Déterminer les actions à mettre en place et les informations à transmettre aux collaborateurs de l'entreprise

Prérequis de la Formation

- Connaissances de base en infrastructure IT et en sécurité des systèmes d'information.
- Aucune certification préalable requise.

Audience Ciblée

- Correspondant informatique et libertés, DSI, DRH, juriste, toute personne impliquée dans la conception de projets traitant des données à caractère personnel.

Programme

Module 1

- GDPR et principes de confidentialité

Module 2

- DPO

Module 3

- Gestion des risques et sécurité de l'information

Module 4

- Incidents et protection

Module 5

- Communication

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

Responsable de la Sécurité des Systèmes d'Information (RSSI)

Objectifs

- Comprendre les enjeux de la sécurité des services informatique dans une organisation.
- Connaître les techniques de base de la fonction RSSI.
- Maîtriser la norme ISO 27001 et mettre en œuvre un SMSI dans son organisation.
- Connaître la politique de sécurité et auditer la sécurité et les indicateurs.
- Connaître les règlementations et aspects juridiques de la sécurité des systèmes informatiques.
- Savoir réagir face à un incident.

Prérequis de la Formation

- Avoir une expérience au sein d'une direction informatique en tant qu'informaticien.
- Avoir des notions de base en sécurité appliquées aux systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.

Audience Ciblée

Toute personne amenée à exercer la fonction de responsable sécurité des systèmes d'information :

- RSSI,
- Futurs RSSI,
- RSSI adjoint, …

Programme

Jour 1

- Matin : Enjeux de la sécurité des systèmes d'information
- Après-midi : Gestion des incidents liés à la SSI

Jour 2

- Matin : Introduction à la menace cyber et gestion du risque
- Après-midi : Sécurité applicative & système / Protection des postes / Audit de sécurité

Jour 3

- Matin : Processus et Système de Management de la Sécurité de l'Information (SMSI) / Normes ISO 27000 / Politiques de sécurité
- Après-midi : Indicateurs de sécurité / Audit : typologies, déroulement, actions correctives

Jour 4

- Matin : Gestion des risques SSI : méthodes (ISO 27001, EBIOS, Mehari), identification des actifs, estimation des risques
- Après-midi : Aspects juridiques de la SSI : obligations, prévention, répression

Jour 5

- Matin : Gestion des prestataires en SSI / Sensibilisation à la sécurité des SI
- Après-midi : Mise en situation finale / Restitution, clôture, évaluation

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

CYBERSÉCURITÉ

PECB

PECB Cybersecurity Foundation

Objectifs

- Expliquer les concepts et principes fondamentaux de la cybersécurité
- Identifier les principales normes et les principaux cadres de cybersécurité, tels que l'ISO/IEC 27032 et le cadre de cybersécurité du NIST
- Expliquer les approches, les méthodes et les techniques permettant d'assurer la la cybersécurité

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Managers et consultants souhaitant approfondir leurs connaissances en matière de connaissances en matière de cybersécurité
- Les professionnels souhaitant se familiariser avec les meilleures pratiques en matière de gestion de la cybersécurité
- Les chargées de mener des activités de cybersécurité au sein de leur organisation
- Personnes sopersonnesuhaitant faire carrière dans la cybersécurité

Programme

Jour 1

- Introduction aux concepts fondamentaux de la cybersécurité

Jour 2

- Approches du programme de cybersécurité
- Examen du certificat

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Lead Pen Test Professional

Objectifs

- Savoir interpréter et illustrer les principaux concepts et principes relatifs au test d'intrusion.
- Comprendre les connaissances techniques de base nécessaires pour organiser et mener à bien un ensemble efficace de tests d'intrusion.
- Apprendre comment planifier efficacement un test d'intrusion et identifier un domaine d'application approprié et adapté en fonction du risque.
- Acquérir les connaissances et les compétences pratiques sur les outils et les techniques utilisés pour effectuer efficacement un test d'intrusion.
- Gérer efficacement le temps et les ressources nécessaires à l'échelle d'un test d'intrusion spécifique.

Prérequis de la Formation

- Une compréhension fondamentale des tests d'intrusion et une connaissance approfondie de la cybersécurité.

Audience Ciblée

- Professionnels informatiques souhaitant améliorer leurs connaissances et leurs compétences techniques.
- Auditeurs souhaitant comprendre les processus du test d'intrusion.
- Responsables des technologies de l'information et de gestion de risques souhaitant acquérir une compréhension plus détaillée de l'utilisation appropriée et bénéfique des tests d'intrusion.
- Gestionnaires d'incidents et professionnels de la continuité des activités cherchant à utiliser les tests dans le cadre de leurs régimes de test.
- Testeurs d'intrusion.
- Pirates respectant le code déontologique.
- Professionnels de la cybersécurité.

Programme

Jour 1

- Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application.

Jour 2

- Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines).

Jour 3

- Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test

Jour 4

- Analyse des résultats des tests, rapports et suivi

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/IEC 27034 Lead Application Security Implementer

Objectifs

- Expliquer les concepts et principes fondamentaux de la sécurité des applications selon ISO/IEC 27034
- Interpréter les lignes directrices d'ISO/IEC 27034 pour gérer un programme de sécurité des applications du point de vue d'un responsable de mise en œuvre
- Initier et planifier la mise en œuvre d'un programme de sécurité des applications selon ISO/IEC 27034 en utilisant les bonnes pratiques
- Soutenir une organisation dans l'exploitation, la maintenance et l'amélioration continue d'un programme de sécurité des applications selon ISO/IEC 27034

Prérequis de la Formation

Une connaissance de base en sécurité de l'information, une compréhension générale du cycle de vie du développement des applications, ainsi qu'une familiarité souhaitable avec les normes ISO/IEC 27001 ou 27002. Une expérience préalable en développement ou en gestion des applications est également recommandée, bien que non obligatoire.

Audience Ciblée

- Professionnels de la sécurité des applications responsables de la gestion et de la mise en œuvre des mesures de sécurité dans le cycle de développement des logiciels
- Responsables informatiques et de la sécurité de l'information qui doivent assurer le développement sécurisé des applications au sein de leur organisation
- Responsables de la conformité et de la gestion des risques chargés de respecter la réglementation et de réduire les risques de sécurité liés aux applications
- Développeurs et architectes de logiciels qui souhaitent intégrer les pratiques de sécurité dans les processus de développement et de conception
- Consultants qui cherchent à développer leur expertise en matière de sécurité des applications et de mise en œuvre de la norme ISO/IEC 27034
- Personnes souhaitant faire progresser leur carrière dans la sécurité de l'information, avec une spécialisation en sécurité des applications

Programme

Jour 1

- Introduction à la sécurité des applications et à la norme ISO/IEC 27034

Jour 2

- Planification de la mise en œuvre d'ISO/IEC 27034

Jour 3

- Mise en œuvre d'ISO/IEC 27034 et gestion et réponse aux incidents

Jour 4

- Surveillance, amélioration continue et audits de sécurité

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/IEC 27033 Lead Network Security Manager

Objectifs

- Gain a comprehensive understanding of the concepts, approaches, methods, and techniques of the implementation and effective management of network security
- Acknowledge the correlation between the ISO/IEC 27033 series of standards and other standards and regulatory frameworks Interpret the guidelines of ISO/IEC 27033 series of standards in the specific context of an organization
- Develop the necessary knowledge and competence to support an organization in effectively planning, implementing, managing, monitoring, and maintaining network security
- Acquire the practical knowledge to advise an organization in managing network security by following best practices

Prérequis de la Formation

- The main participation requirement is a fundamental understanding of the ISO/IEC 27033 series of standards and a general knowledge of network security concepts.

Audience Ciblée

- Network security and information security professionals seeking to manage network security
- Managers or consultants seeking to master network security best practices
- Individuals involved in the planning and implementation of the architectural aspects of network security
- Technical experts seeking to enhance their network security knowledge
- Network security expert advisors

Programme

Day 1

- Introduction to ISO/IEC 27033 series of standards and initiation of network security implementation

Day 2

- Network security team, policy, risk management, and documentation management

Day 3

- Internet access services, network segmentation, securing network communications using security gateways, VPNs, and wireless IP network access

Day 4

- Network security testing, incident management, monitoring, and continual improvement

Day 5

- Certification Exam

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Cyber Threat Analyst

Objectifs

- Identify various types of cyber threats, understand their characteristics, and analyze their potential impact on organizational security
- Establish robust incident response plans to effectively manage and mitigate security breaches and cyberattacks
- Utilize advanced threat hunting techniques and tools to proactively search for and identify security threats within an organization's network
- Formulate and validate threat hunting hypothesis using data-driven approaches and identify potential threats by leveraging
- Design, implement, and continuously improve threat hunting programs within organizations

Prérequis de la Formation

- The main requirement for participating in this training course is having a fundamental understanding of cybersecurity principles and concepts.

Audience Ciblée

- Cybersecurity professionals such as incident responders and security operations center (SOC)
- IT professionals who are involved in managing and security IT infrastructure
- Security managers and directors who are responsible for an organization's security strategy
- Professionals involved in penetration testing and ethical hacking in order to gain insights into the latest threats and defensive techniques
- Individuals responsible for risk management, compliance, and governance
- Aspiring cybersecurity professionals who want to gain foundational knowledge and skills in threat analysis

Programme

Day 1

- Fundamentals of cyber threat analysis and threat hunting frameworks

Day 2

- Prepare, execute phase of threat hunting program and incident management plan

Day 3

- Analyze and knowledge phase of threat hunting framework

Day 4

- Building a cybersecurity culture, monitoring and measurement, and continual improvement

Day 5

- Certification Exam

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Lead Cybersecurity Manager

Objectifs

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en œuvre et gérer un programme de cybersécurité.
- Expliquer la corrélation entre la norme ISO/ IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents.
- Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes.
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité.

Prérequis de la Formation

- Pour bénéficier pleinement de cette formation, les participants doivent avoir une compréhension fondamentale des concepts et de la gestion de la cybersécurité.

Audience Ciblée

- Aux responsables et dirigeants impliqués dans la gestion de la cybersécurité
- Aux personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité
- Aux professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité
- Aux professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes
- Aux cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité

Programme

Jour 1

- Introduction to cybersecurity and initiation of a cybersecurity program implementation

Jour 2

- Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaque

Jour 3

- Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité

Jour 4

- Management des incidents de cybersécurité, surveillance et amélioration continue

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Lead Ethical Hacker

Objectifs

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

Prérequis de la Formation

- La principale condition pour participer à cette formation est d'avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation. Il est recommandé aux participants d'avoir une connaissance des réseaux informatiques et des concepts de programmation.

Audience Ciblée

- Personnes souhaitant acquérir des connaissances sur les principales techniques utilisées pour réaliser des tests d'intrusion.
- Personnes impliquées dans la sécurité de l'information qui cherchent à maîtriser les techniques de piratage éthique et de tests d'intrusion.
- Personnes responsables des systèmes de la sécurité d'information, telles que les responsables de la sécurité de l'information et les professionnels de la cybersécurité.
- Membres de l'équipe de sécurité de l'information voulant améliorer leurs connaissances de la sécurité de l'information.
- Managers ou conseillers experts souhaitant apprendre à gérer des activités de piratage éthique.
- Experts techniques souhaitant apprendre comment planifier et réaliser un test d'intrusion.

Programme

Jour 1

- Introduction au piratage éthique.

Jour 2

- Lancement de la phase de reconnaissance.

Jour 3

- Lancement de la phase d'exploitation.

Jour 4

- Post-exploitation et rapports.

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Lead Cloud Security Manager

Objectifs

- Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un programme de sécurité du cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes et cadres réglementaires.
- Apprendre à interpréter les lignes directrices des normes ISO/IEC 27017 et ISO/IEC 27018 dans le contexte spécifique d'un organisme.
- Développer les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud.
- Acquérir les connaissances pratiques pour conseiller un organisme dans la gestion d'un programme de sécurité du cloud en suivant les bonnes pratiques.

Prérequis de la Formation

- La principale exigence participer à cette formation est d'avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/ IEC 27018 et une connaissance générale des concepts du cloud computing.

Audience Ciblée

- Professionnels de la sécurité du cloud et de la sécurité de l'information cherchant à gérer un programme de sécurité du cloud
- Managers ou consultants cherchant à maîtriser les bonnes pratiques de sécurité du cloud
- Personnes chargées de maintenir et de gérer un programme de sécurité du cloud
- Experts techniques cherchant à améliorer leurs connaissances en matière de sécurité du cloud
- Conseillers experts en sécurité du cloud

Programme

Jour 1

- Introduction aux normes ISO/IEC 27017 et ISO/ IEC 27018 et à l'initiation d'un programme de sécurité du cloud.

Jour 2

- Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud.

Jour 3

- Gestion de l'information documentée, sensibilisation et formation à la sécurité du cloud.

Jour 4

- Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue.

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED Lead SCADA Security Manager

Objectifs

- Comprendre et expliquer l'objectif et les risques des systèmes SCADA, des systèmes de contrôle distribués et des automates programmables logiques programmables.
- Comprendre les risques auxquels sont confrontés ces environnements et les approches appropriées pour gérer ces risques.
- Développer l'expertise nécessaire pour soutenir un programme de sécurité SCADA proactif, y compris les politiques et la gestion des vulnérabilités.
- Définir et concevoir une architecture de réseau intégrant des contrôles de sécurité avancés pour SCADA.
- Expliquer la relation entre les contrôles de gestion, opérationnels et techniques dans un programme de sécurité SCADA.
- Améliorer la capacité à concevoir des systèmes SCADA résilients et à haute disponibilité.
- Apprendre à gérer un programme d'activités de tests de sécurité efficaces.

Prérequis de la Formation

- Une compréhension fondamentale de la sécurité SCADA.

Audience Ciblée

- Les professionnels de la sécurité souhaitant acquérir des compétences professionnelles en matière de sécurité SCADA.
- Les professionnels de l'informatique qui souhaitent améliorer leurs compétences et leurs connaissances techniques.
- Les responsables des technologies de l'information et de la gestion des risques qui cherchent à mieux comprendre les systèmes ICS et SCADA.
- Les développeurs de systèmes SCADA.
- Ingénieurs et opérateurs SCADA.
- Les professionnels de l'informatique SCADA.

Programme

Jour 1

- Introduction à SCADA et ICS.

Jour 2

- Conception d'un programme de sécurité et d'une architecture de sécurité du réseau.

Jour 3

- Mise en œuvre des contrôles de sécurité ICS, de la gestion des incidents et de la continuité des activités.

Jour 4

- Tests de sécurité des systèmes SCADA.

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

ISC2 CERTIFIED in Cybersecurity

Objectifs

- Discuss the foundational concepts of cybersecurity principles.
- Recognize foundational security concepts of information assurance.
- Define risk management terminology and summarize the process.
- Relate risk management to personal or professional practices.
- Classify types of security controls.
- Distinguish between policies, procedures, standards, regulations and laws.
- Demonstrate the relationship among governance elements.
- Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given examples.
- Practice the terminology of and review security policies.
- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions.
- Recall the terms and components of incident response.
- Summarize the components of a business continuity plan.
- Identify the components of disaster recovery.
- Practice the terminology and review concepts of business continuity, disaster recovery and incident response.
- Select access controls that are appropriate in a given scenario.
- Relate access control concepts and processes to given scenarios.
- Compare various physical access controls.
- Describe logical access controls.
- Practice the terminology and review concepts of access controls.
- Explain the concepts of network security.

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

- None. No prior work experience or formal degree required. You only need to become an ISC2 Candidate.

Audience Ciblée

- CC training is for IT professionals, career changers, college students, recent college graduates, advanced high school students and recent high school graduates looking to start their path toward cybersecurity leadership by taking the Certified in Cybersecurity entry-level exam. There are no prerequisites.

Programme

Chapter 1

- Security Principles

Chapter 2

- Incident Response, Business Continuity and Disaster Recovery

Chapter 3

- Access Controls Concepts

Chapter 4

- Network Security

Chapter 5

- Security Operations

Chapter 6

- Course Summary and Test Preparation

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

ISC2 CERTIFIED Information Systems Security Professional

Objectifs

- Apply fundamental concepts and methods related to the fields of information technology and security.
- Align overall organizational operational goals with security functions and implementations.
- Determine how to protect assets of the organization as they go through their lifecycle.
- Leverage the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
- Apply security design principles to select appropriate mitigations for vulnerabilities present in common information system types and architectures.
- Explain the importance of cryptography and the security services it can provide in today's digital and information age.
- Evaluate physical security elements relative to information security needs.
- Apply physical and logical access controls to meet information security needs.
- Differentiate between primary methods for designing and validating test and audit strategies that support information security requirements.
- Apply appropriate security controls and countermeasures to optimize an organization's operational function and capacity.

Prérequis de la Formation

- Basic knowledge of networks and operating systems, as well as information security. Basic knowledge of audit standards and business continuity.

Audience Ciblée

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response. Individuals in industries such as Banking, Defense and Law Enforcement.

Programme

Domain 1

Security and Risk Management

Domain 2

Asset Security

Domain 3

Security Architecture and Engineering

Domain 4

Communication and Network Security

Domain 5

Identity and Access Management (IAM)

Domain 6

Security Assessment and Testing

Domain 7

Security Operations

Domain 8

Software Development Security

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CISSP®

ISC2 CERTIFIED Cloud Security Professional

Objectifs

- Se préparer efficacement à l'examen Certified Cloud Security Professional CCSP de l'(ISC)².
- Maîtriser les meilleures pratiques de la sécurité cloud à l'échelle internationale.
- Acquérir une expertise transversale sur les architectures, les données, les plateformes et les aspects juridiques du cloud.
- Valider les acquis par des exercices pratiques et des quiz inspirés de l'examen officiel.

Prérequis de la Formation

- Expérience recommandée en sécurité des systèmes d'information ou en environnement cloud.

Audience Ciblée

- Professionnels de la cybersécurité, administrateurs cloud, architectes, ingénieurs sécurité.
- Consultants, chefs de projets, RSSI impliqués dans des environnements cloud.
- Toute personne souhaitant valoriser une expertise de haut niveau en sécurité cloud.

Programme

Jour 1

- Module 1 : Concepts d'architecture et exigences de conception cloud

Jour 2

- Module 2 : Sécurité des données dans le cloud

Jour 3

- Module 3 : Sécurité des plateformes et infrastructures cloud

Jour 4

- Module 4 : Sécurité des applications cloud

Jour 5

- Module 5 : Opérations + Module 6 : Aspects juridiques et conformité

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CCSP®

EC-Council

EC-Council CERTIFIED Incident Handler (ECIH)

Objectifs

EC-Council's Certified Incident Handler program equips students with the knowledge, skills, and abilities to effectively prepare for, deal with, and eradicate threats and threat actors in an incident. This program provides the entire process of incident handling and response and hands-on labs that teach the tactical procedures and techniques required to effectively plan, record, triage, notify and contain. Students will learn the handling of various types of incidents, risk assessment methodologies, as well as laws and policies related to incident handling. After attending the course, students will be able to create IH&R policies and deal with different types of security incidents such as malware, email security, network security, web application security, cloud security, and insider threat-related incidents. The E|CIH also covers post incident activities such as containment, eradication, evidence gathering and forensic analysis, leading to prosecution or countermeasures to ensure the incident is not repeated.

Prérequis de la Formation

- Mid-level to high-level cybersecurity professionals with at least 3 years of experience
- Information security professionals seeking to enhance their skills and knowledge in incident handling and response
- Individuals interested in preventing cyber threats.

Audience Ciblée

- Any mid-level to high-level cyber security professionals with a minimum of 3 years of experience
- Individuals from the information security profession and who want to enrich their skills and knowledge in the field of incident handling and response.
- Individuals interested in preventing cyber threats.

Prérequis de la Formation

Module 1

- Introduction to Incident Handling and Response

Module 2

- Incident Handling and Response Process

Module 3

- First Response

Module 4

- Handling and Responding to Malware Incidents

Module 5

- Handling and Responding to Email Security Incidents

Module 6

- Handling and Responding to Network Security Incidents

Module 7

- Handling and Responding to Web Application Security Incidents

Module 8

- Handling and Responding to Cloud Security Incidents

Module 9

- Handling and Responding to Insider Threats

Module 10

- Handling and Responding to Endpoint Security Incidents

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

E|CIH EC-Council Certified Incident Handler

EC-Council

EC-Council CERTIFIED SOC Analyst

Objectifs

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers and workstations).
- Gain knowledge of Centralized Log Management (CLM) process.
- Able to perform Security events and log collection, monitoring, and analysis.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Gain knowledge on administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/AlienVault/OSSI.

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

- A minimum of 1 year of professional experience in network administration or information security.

Audience Ciblée

- SOC Analysts (Tier I and Tier II)
- Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network, Defense Technicians, Network, Security Specialist, Network, Security Operator, and any security professional handling network security operations
    - Cybersecurity Analyst
    - Entry-level cybersecurity professionals
    - Anyone who wants to become a SOC Analyst.

Programme

Module 0

- SOC Essential Concepts

Module 1

- Security Operations and Management

Module 2

- Understanding Cyber Threats, IoCs, and Attack Methodology

Module 3

- Incidents, Events, and Logging

Module 4

- Incident Detection with Security Information and Event Management (SIEM)

Module 5

- Enhanced Incident Detection with Threat Intelligence

Module 6

- Incident Response

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CSA Certified SOC Analyst™

EC-Council

EC-Council BECOME A CERTIFIED Ethical Hacker

Objectifs

Armed with your attack platform (Parrot OS) and a plethora of tools used by ethical hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP, and experience the real thing in a controlled environment with no consequences. It's the ultimate learning experience to support your career as an ethical hacker! Each phase builds on the last as you progress through your ABCDorg engagement.

Prérequis de la Formation

- You need only an internet connection and can compete through your browser.
- We provide the attack platform, targets and all the required tools. You bring the skills to win!

Audience Ciblée

- In-depth knowledge of ethical hacking methodologies and practices, augmented with AI techniques
- The skills to integrate AI across ethical hacking phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks
- AI techniques to automate tasks, boost efficiency, and detect sophisticated threats beyond traditional methods
- Tools that will utilize AI for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks

Programme

Module 1
- Introduction to Ethical Hacking

Module 2
- Footprinting and Reconnaissance

Module 3
- Scanning Networks

Module 4
- Enumeration

Module 5
- Vulnerability Analysis

Module 6
- System Hacking

Module 7
- Malware Threats

Module 8
- Sniffing

Module 9
- Social Engineering

Module 10
- Denial-of-Service

Module 11
- Session Hijacking

Module 12
- Evading IDS, Firewalls, and Honeypots

Module 13
- Hacking Web Servers

Module 14
- Hacking Web Applications

Module 15
- SQL Injection

Module 16
- Hacking Wireless Networks

Module 17
- Hacking Mobile Platforms

Module 18
- IoT Hacking

Module 19
- Cloud Computing

Module 20
- Cryptography

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

C|EH Certified Ethical Hacker

EC-Council

EC-Council – Threat Intelligence Essentials (T|IE)

Objectifs

- This course aims to equip participants with foundational knowledge and practical skills in cyber threat intelligence. Learners will understand the threat landscape, identify and analyze cyber threats, gather and interpret intelligence data, and apply it to strengthen organizational security. By the end of the training, participants will be able to proactively detect, respond to, and mitigate cyber threats using structured intelligence approaches.

Prérequis de la Formation

- Basic knowledge of networking and cybersecurity principles
- Familiarity with common cyber threats and attack methods
- Experience in IT, security operations, or incident response is helpful but not mandatory
- No advanced technical skills required

Audience Ciblée

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity or threat intelligence.
- Anyone interested in threat intelligence, Indicators of Compromise (IoC) analysis, defensive cybersecurity operations, and incident response.
- Any professional involved in securing public, private, and hybrid cloud infrastructures, identities, data, and applications.
- IT / Cybersecurity professionals, system administrators, cloud administrators, cybersecurity administrators, engineers, and architects will also benefit from this course.

Programme

Module 1
- Introduction to Threat Intelligence

Module 2
- Types of Threat Intelligence

Module 3
- Cyber Threat Landscape

Module 4
- Data Collection and Sources of Threat Intelligence

Module 5
- Threat Intelligence Platforms

Module 6
- Threat Intelligence Analysis

Module 7
- Threat Hunting and Detection

Module 8
- Threat Intelligence Sharing and Collaboration

Module 9
- Threat Intelligence in Incident Response

Module 10
- Future Trends and Continuous Learning

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

T | IE
Threat Intelligence Essentials

EC-Council

EC-Council – Digital Forensics Essentials (D|FE)

Objectifs

- The Digital Forensics Essentials (D|FE) course aims to enhance your competency and expertise in digital forensics and information security skills, offering 12 comprehensive modules, 11 hours of premium self-paced video training, courseware, and 11 labs.

Prérequis de la Formation

- No prior cybersecurity knowledge or IT work experience required.

Audience Ciblée

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- High school students who want to get an early start on their cybersecurity careers and master the fundamentals of security online.
- College or university students interested in preparing for a cybersecurity career and aiding their IT education.
- Working professionals who want to get into the cybersecurity field and don't know where to start their education journey.

Programme

Module 1
- Computer Forensics Fundamentals

Module 2
- Computer Forensics Investigation Process

Module 3
- Understanding Hard Disks and File Systems

Module 4
- Data Acquisition and Duplication

Module 5
- Defeating Anti-forensics Techniques

Module 6
- Windows Forensics

Module 7
- Linux and Mac Forensics

Module 8
- Network Forensics

Module 9
- Investigating Web Attacks

Module 10
- Dark Web Forensics

Module 11
- Investigating Email Crimes

Module 12
- Malware Forensics

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

D|FE Digital Forensics Essentials

EC-Council

EC-Council – CERTIFIED Encryption Specialist (E|CES)

Objectifs

- Types of Encryption Standards and their differences
- How to select the best standard for your organization
- How to enhance your pen-testing knowledge in encryption
- Correct and incorrect deployment of encryption technologies
- Common mistakes made in implementing encryption technologies
- Best practices when implementing encryption technologies
- Quantum computing and cryptography

Prérequis de la Formation

- No prior knowledge of cryptography is assumed, and no mathematical skills beyond basic algebra are required

Audience Ciblée

- Penetration Testers and Computer Forensics Specialists
- Cloud security architects, designers, and developers
- Anyone involved in selecting and implementing VPNs or digital certificates, or information security operations.
- Anyone involved in developing operating systems, cryptography systems, blockchain based solutions, etc.

Programme

Module 1

- Introduction and History of Cryptography

Module 2

- Symmetric Cryptography and Hashes

Module 3

- Number Theory and Asymmetric Cryptography

Module 4

- Applications of Cryptography

Module 5

- Cryptanalysis

Module 6

- Quantum Computing and Cryptography

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

E|CES EC-Council Certified Encryption Specialist

EC-Council

EC-Council – IoT Security Essentials (I|SE)

Objectifs

The IoT Security Essentials (I|SE) course provides foundational knowledge and skills to secure Internet of Things (IoT) devices and networks.

- Gain insights into the emergence of the Internet of Things (IoT).
- Learn about the devices that make your home a smart home.+
- Dive deep into IoT communication models.
- Gain a deep understanding of IoT networking and communication.
- Understand cloud computing in depth.
- Learn about the different types of threats to IoT.

Prérequis de la Formation

- No prior cybersecurity knowledge or IT work experience required.

Audience Ciblée

- School students, graduates, professionals, career starters and changers, IT/Technology/Cybersecurity teams with little or no work experience.
- Individuals who want to start a career in cybersecurity and are interested in IoT Security.
- Anyone interested in gaining in-depth knowledge on safeguarding their smart devices or those within their organization.

Programme

Module 1
- IoT Fundamentals

Module 2
- IoT Networking and Communication

Module 3
- IoT Processors and Operating Systems

Module 4
- Cloud and IoT

Module 5
- IoT Advanced Topics

Module 6
- IoT Threats

Module 7
- Basic Security

Module 8
- Cloud Security

Module 9
- Threat Intelligence

Module 10
- IoT Incident Response

Module 11
- IoT Security Engineering

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

I | SE
IoT Security Essentials

EC-Council

EC-Council – CERTIFIED DevSecOps Engineer (E|CDE)

Objectifs

- You will be well-prepared to manage security incidents and maintain operational resilience
- You will discover how to leverage AI-powered tools for the DevSecOps pipeline, thereby enhancing automation
- You will gain familiarity with various open-source and commercial third-party DevSecOps tools, which enable the secure development of software and web applications within an organization's internal IT infrastructure as well as in a public cloud environment
- You will gather insights into application DevSecOps as well as infrastructure DevSecOps
- You will hone your skills to detect and remediate security issues while developing application codes by utilizing automated application security testing such as SAST, DAST, IAST, and RASP

Prérequis de la Formation

- Students should have an understanding of application security concepts.

Audience Ciblée

- C|ASE-certified professionals
- Application security professionals
- DevOps engineers
- Software engineers and testers
- IT security professionals
- Cybersecurity engineers and analysts
- Anyone with prior knowledge of application security who wants to build their career in DevSecOps

Programme

Module 1

- Understanding DevOps Culture

Module 2

- Introduction to DevSecOps

Module 3

- DevSecOps Pipeline – Plan Stage

Module 4

- DevSecOps Pipeline – Code Stage

Module 5

- DevSecOps Pipeline – Build and Test Stage

Module 6

- DevSecOps Pipeline – Release and Deploy Stage

Module 7

- DevSecOps Pipeline – Operate and Monitor Stage

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

E|CDE EC-Council Certified DevSecOps Engineer

EC-Council

EC-Council – ICS/SCADA Cybersecurity

Objectifs

The ICS/SCADA Cyber Security Training Course is a hands-on training which will enable you to learn the foundation of security and defending architectures from attacks. You will look at the concept of "thinking like a hacker" to learn techniques to defend from the types of attacks that are commonly conducted against the oil and gas IT corporate and control network.

Prérequis de la Formation

- The course is designed for IT professionals who manage or oversee their organization's IT infrastructure and are responsible for implementing and maintaining information security policies and procedures. It focuses specifically on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

Audience Ciblée

This course is specially designed for IT professionals who are involved in managing or directing their organization's IT infrastructure and who are responsible for establishing and maintaining information security policies, practices and procedures. The focus in the course is on the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems.

Programme

Module 1

- Introduction to ICS/SCADA Network Defense

Module 2

- TCP/IP 101

Module 3

- Introduction to Hacking

Module 4

- Vulnerability Management

Module 5

- Standards and Regulation for Cybersecurity

Module 6

- Securing the ICS/SCADA Network

Module 7

- Bridging the Air Gap

Module 8

- Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

ICS/SCADA CYBER SECURITY

EC-Council

EC-Council – CERTIFIED Network Defender (C|ND)

Objectifs

According to Gartner, 'traditional « prevent and detect » approaches are inadequate.' Opportunistic by nature, malicious actors look for the easiest ways to attack most users and siphon off maximum gains. Developing a continuous Adaptive Security Cycle helps organizations stay ahead of cybercriminals by creating and improving security systems. And that's what you learn in the C|ND program.

Prérequis de la Formation

- Fundamental knowledge of networking concepts
- Educational background in IT, cybersecurity, or related fields
- Working experience in the respective fields

Audience Ciblée

- Students/IT Professionals/Any other industry professionals planning a career in cybersecurity.
- Anyone who wants to start a career in the blue team and network security.

Programme

Module 1
- Network Attacks and Defense Strategies

Module 2
- Administrative Network Security

Module 3
- Technical Network Security

Module 4
- Network Perimeter Security

Module 5
- Endpoint Security-Windows Systems

Module 6
- Endpoint Security-Linux Systems

Module 7
- Endpoint Security- Mobile Devices

Module 8
- Endpoint Security-IoT Devices

Module 9
- Administrative Application Security

Module 10
- Data Security

Module 11
- Enterprise Virtual Network Security

Module 12
- Enterprise Cloud Security

Module 13
- Wireless Network Security

Module 14
- Network Traffic Monitoring and Analysis

Module 15
- Network Logs Monitoring and Analysis

Module 16
- Incident Response and Forensic Investigation

Module 17
- Business Continuity and Disaster Recovery

Module 18
- Risk Anticipation with Risk Management

Module 19
- Threat Assessment with Attack Surface Analysis

Module 20
- Threat Prediction with Cyber Threat Intelligence

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

C|ND Certified Network Defender

EC-Council – Licensed Penetration Tester (Master)

Objectifs

- Demonstrate a repeatable and measurable approach to Penetration Testing
- Perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS),LFI, RFI vulnerabilities in web applications
- Perform privilege escalation to gain root access to a system Demonstrate 'Out-of-the-box' and 'lateral' thinking
- Get access to proprietary EC-Council Penetration Testing methodologies
- Exploit vulnerabilities in Operating systems such as Windows, Linux
- Identify and bypass perimeter protections
- Perl, Python and Ruby scripting for the penetration tester
- Advanced post exploitation and persistence.
- Extending Metasploit with custom modules and exploits
- Pivoting from external into internal networks
- Avoiding the most common mistakes when drafting a professional penetration testing report

Prérequis de la Formation

- There are no official prerequisites required in order to take this course. However, you will benefit from a basic knowledge of penetration testing concepts.

Audience Ciblée

- Penetration Testers
- Network Administrators
- IT Auditors
- Information Security Engineers
- Security Consultants

Programme

Module 1

- Introduction to Vulnerability Assessment and Penetration Testing

Module 2

- Information Gathering Methodology

Module 3

- Scanning and Enumeration

Module 4

- Identify Vulnerabilities

Module 5

- Exploitation

Module 6

- Post Exploitation

Module 7

- Advanced Tips and Techniques

Module 8

- Preparing a Report

Module 9

- Practice Ranges

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

EC-Council

EC-Council – Certified Threat Intelligence Analyst (C|TIA)

Objectifs

- Gain skills for performing various types of threat intelligence
- Learn various data collection techniques from multiple sources and feeds
- Emphasis on collection, creation, and dissemination of Indicators of Compromise (IoCs) in various formats
- Gain proficiency in developing a structured approach for performing threat analysis and threat intelligence evaluation.
- Learn various techniques for threat intelligence reporting and dissemination
- Know the latest threat intelligence tools/platforms and frameworks
- Know how to perform threat intelligence through Python Scripting
- Gain skills in threat hunting and detection
- Learn threat intelligence in SOC Operations, Incident Response, and Risk Management
- Enhance your threat intelligence skills in the cloud environment
- Based on a comprehensive industry-wide Job Task Analysis (JTA)

Prérequis de la Formation

- There are no formal prerequisites to attend the CTIA v2 training. However, to be eligible for the certification exam, candidates must have at least three years of professional experience in cybersecurity or software development.

Audience Ciblée

- Mid-level to high-level cybersecurity professionals with a minimum of three years of experience.
- Individuals with EC-Council's C|EH and C|ND certifications can enroll in this

Programme

Module 1

- Introduction to Threat Intelligence

Module 2

- Cyber Threats and Attack Frameworks

Module 3

- Requirements, Planning, Direction, and Review

Module 4

- Data Collection and Processing

Module 5

- Data Analysis

Module 6

- Intelligence Reporting and Dissemination

Module 7

- Threat Hunting and Detection

Module 8

- Threat Intelligence in SOC Operations, Incident Response, and Risk Management

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

C|TIA Certified Threat Intelligence Analyst

EC-Council – Computer Hacking Forensic Investigator (C|HFI)

Objectifs

- Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, and regulations and standards that influence computer forensics investigation
- Various phases involved in the computer forensics investigation process
- Different types of disk drives and their characteristics, booting process and file systems in Windows, Linux, and Mac operating systems, file system examination tools, RAID and NAS/SAN storage systems, various encoding standards, and file format analysis
- Data acquisition fundamentals and methodology, eDiscovery, and how to prepare image files for forensics examination
- Various anti-forensics techniques used by attackers, different ways to detect them and related tools, and countermeasures

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

- IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response
- Prior completion of Certified Ethical Hacker (CEH) training would be an advantage

Audience Ciblée

- The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response. Individuals in industries such as Banking, Defense and Law Enforcement.

Programme

Module 1
- Computer Forensics in Today's World

Module 2
- Computer Forensics Investigation Process

Module 3
- Understanding Hard Disks and File Systems

Module 4
- Data Acquisition and Duplication

Module 5
- Defeating Anti-forensics Techniques

Module 6
- Windows Forensics

Module 7
- Linux and Mac Forensics

Module 8
- Network Forensics

Module 9
- Malware Forensics

Module 10
- Investigating Web Attacks

Module 11
- Dark Web Forensics

Module 12
- Cloud Forensics

Module 13
- Email and Social Media Forensics

Module 14
- Mobile Forensics

Module 15
- IoT Forensics

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

EC-Council

EC-Council DevSecOps Essentials (D|SE)

Objectifs

- Learn the fundamentals of application development.
- Gain knowledge of application security.
- Understand DevOps and DevSecOps.
- Explore the DevSecOps toolchain.
- Gain insights into DevSecOps and CI/CD pipelines.
- Learn about implementing and using tools for DevSecOps in CI/CD pipelines

Prérequis de la Formation

- No prior experience is required to take this course.

Audience Ciblée

- School students, graduates, professionals, career starters and changers, IT / Technology / Cybersecurity teams with little or no work experience.
- Anyone who wants to start a career in cybersecurity, application security, and development and is interested in cloud technology.
- Any professional involved in developing, testing, and deploying applications to production environments, including on-premises, public cloud, and hybrid environments.
- This program is also beneficial for application developers, risk managers, project managers, application administrators, administrators, engineers, and architects.

Programme

Module 1

- Application Development Concepts

Module 2

- Application Security Fundamentals

Module 3

- Module 3: Introduction to DevOps

Module 4

- Introduction to DevSecOps

Module 5

- Introduction to DevSecOps Management Tools

Module 6

- Introduction to DevSecOps Code and CI/CD Tools

Module 7

- Introduction to DevSecOps Pipelines

Module 8

- Introduction to DevSecOps CI/CD Testing and Assessments

Module 9

- Implementing DevSecOps Testing & Threat Modeling

Module 10

- Implementing DevSecOps Monitoring and Feedback

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

D|SE DevSecOps Essentials

CYBERSÉCURITÉ

CompTIA PenTest+ (PT0-003)

Objectifs

The Official CompTIA® PenTest+® (Exam PT0-002) is designed for cybersecurity professionals tasked with penetration testing and vulnerability management. This course prepares you to:

- Plan and scope a penetration testing engagement.
- Understand legal and compliance requirements.
- Perform vulnerability scanning and penetration testing using appropriate tools and techniques and then analyze the results.
- Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations.
- PenTest+ is a unique certification because it requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.

Prérequis de la Formation

- Recommended experience: 3–4 years in a penetration tester job role.

Audience Ciblée

- Individuals who pass the exam prove their ability to perform the intermediate-level duties of a penetration tester or security consultant. Skills include scoping and engagement, compliance, vulnerability scanning and analysis, exploits, communication, and remediation.
- Earning a PenTest+ certification gives learners an internationally recognized, vendor-neutral credential. Demonstrating their competency in penetration testing, vulnerability assessment, and reporting.
- Information security threats are rising around the world, leaving organizations increasingly concerned over the lack of adequately trained IT security staff. A PenTest+ certification qualifies learners to perform the penetration testing and vulnerability assessment needs of employers.

Programme

Module 1

- Penetration Testing: Before You Begin

Module 2

- Applying Pre-Engagement Activities

Module 3

- Enumeration and Reconnaissance

Module 4

- Scanning and Identifying Vulnerabilities

Module 5

- Conducting Pentest Attacks

Module 6

- Enterprise Attacks

Module 7

- Conducting Pentest Attacks

Module 8

- Specialized Attacks

Module 9

- Performing Penetration Testing Tasks

Module 10

- Reporting and Recommendations

- A.0 CompTIA PenTest+ PT0-003 Practice Exams

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIAIRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CompTIA SecurityX (Formerly CASP+) (CAS-005)

Objectifs

- Individuals who have passed this exam have proven that they can design and implement effective cybersecurity solutions on complex enterprise networks that exist on premises and in the cloud.
- SecurityX certification communicates that learners have the mastery-level skills of an enterprise-level Security Architect and Senior Security Engineer. They can design, assess, fix, automate, and operate a secure enterprise network while complying with various governance, risk, and compliance requirements.
- Earning the SecurityX certification gives learners an internationally recognized, vendor-neutral credential. They can demonstrate their competency in technical integration of enterprise business goals, secure systems design, senior engineering, and security architecture.
- Information security threats are rising around the world, leaving organizations increasingly concerned over lack of adequately trained IT security staff. A SecurityX certification qualifies learners to assess, manage, and protect their enterprise-wide cybersecurity needs using the latest techniques and best practices.

Prérequis de la Formation

- Target audience: Minimum 10 years general hands-on IT experience
- 5 years being hands-on security, with Network+, Security+, CySA+, Cloud+ and PenTest+ or equivalent knowledge.

Audience Ciblée

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations in an enterprise environment.
- Apply security practices to cloud, on-premises, and hybrid environments.
- Consider cryptographic technologies and techniques, as well as the impact of emerging trends (e.g. artificial intelligence) on information security.
- Use the appropriate governance, compliance, risk management, and threat modeling strategies throughout the enterprise.

Programme

Lesson 1

- Pre-Asseement

Lesson 2

- Summarizing Governance, Risk, and Compliance

Lesson 3

- Implementing Architecture & Design

Lesson 4

- Understanding Security Engineering

Lesson 5

- Applying Security Operations & Incident Response

- A.0 CompTIA SecurityX CAS-005 Practice Materials
- B.0 Practice Exam Module

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

CompTIA CySA+ (CS0-003)

Objectifs

The CompTIA Cybersecurity Analyst (CySA+) certification exam will certify the successful candidate has the knowledge and skills required to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize, and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability
- Management and incident response activities

Prérequis de la Formation

- Network+, Security+, or equivalent knowledge, with a minimum of 4 years of hands-on experience as an incident response analyst, security operations center (SOC) analyst, or equivalent experience.

Audience Ciblée

- Security Analyst
- Security Operations
- Center (SOC) Analyst
- Security Administrator
- Incident Response Analyst
- Vulnerability Management Analyst
- Security Engineer

Programme

Lesson 1

- Understanding Vulnerability Response, Handling, and Management

Lesson 2

- Exploring Threat Intelligence and Threat Hunting Concepts

Lesson 3

- Explaining Important System and Network Architecture Concepts

Lesson 4

- Understanding Process Improvement in Security Operations

Lesson 5

- Implementing Vulnerability Scanning Methods

Lesson 6

- Performing Vulnerability Analysis

Lesson 7

- Communicating Vulnerability Information

Lesson 8

- Explaining Incident Response Activities

Lesson 9

- Demonstrating Incident Response Communication

Lesson 10

- Applying Tools to Identify Malicious Activity

Lesson 11

- Analyzing Potentially Malicious Activity

Lesson 12

- Understanding Application Vulnerability Assessment

Lesson 13

- Exploring Scripting Tools and Analysis Concepts

Lesson 14

- Understanding Application Security and Attack Mitigation Best Practices

- Appendix 0: Student Resources
- Appendix 1: Instructor Resources

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIAIRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

CompTIA a+ Cyber

Objectifs

The CompTIA a+ Cyber course serves as the ideal starting point for learners pursuing a career in cybersecurity, delivering the foundational knowledge required to begin Security+ training, a critical first step for cybersecurity professionals. With approximately 35 hours of instruction, learners will gain the skills to secure devices and home networks, leverage tools and methods to protect networks of all sizes, and efficiently manage both Linux and Windows systems. This course prepares learners to sit for training for the ISO/ANSI-accredited CompTIA Security+ certification.

- Learn to keep Window PCs and home networks safe with simple security steps
- Get to know how to use tools and methods to safeguard large and small company networks
- Discover how to handle Linux systems and write scripts to automate tasks and save time
- Gain the essentials to progress to CompTIA Security+ certification training

Programme

Module 1

- Cybersecurity Support Roles3

Module 2

- Microsoft Windows Administration Fundamentals

Module 3

- Secure Network Client Fundamentals

Module 4

- Enterprise Campus Network Fundamentals

Module 5

- Enterprise Network Application Fundamentals

Module 6

- Cybersecurity Controls

Module 7

- Linux App Server Fundamentals

Module 8

- Automation Scripting Fundamentals

Module 9

- Data Management Fundamentals

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIAIRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

CompTIA Soft Skills Essentials

Objectifs

CompTIA Soft Skills Essentials is designed to provide learners and employees across industries with a comprehensive understanding of essential nontechnical skills required for workplace success. This course focuses on enhancing professionalism, communication, teamwork, critical thinking, and career development, equipping learners with the tools to thrive in professional environments.

Soft Skills Essentials supports competency in critical workplace skills, offering learners a competitive edge in their careers. Learners will receive a CompTIA Competency Certificate upon completion, validating their mastery of the course content.

The course is hosted on the CompTIA Learning platform and follows a skills-based framework aligned with the Progression Model of Learning. It incorporates narrative text, videos, interactive activities, and assessments to ensure an engaging and effective learning experience.

- Demonstrate professionalism and workplace readiness.
- Communicate effectively using active listening and clear writing.
- Collaborate in teams by adapting communication styles and resolving conflicts.
- Apply critical thinking to solve workplace problems.
- Provide and receive constructive feedback.
- Manage time and prioritize tasks effectively.
- Build career success with resumes, profiles, and interview skills.
- Adapt to different communication styles to enhance collaboration.

Programme

Module 1

- Character and Professionalism

Module 2

- Communications

Module 3

- Collaboration and Teamwork

Module 4

- Critical Thinking and Problem-Solving

Module 5

- Career Success

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIAIRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Cybersecurity Systems Manager

Objectifs

- Upon completion, Certified Cybersecurity Systems Manager students will have a strong foundation in Cyber Security & IS management standards with current best practices and will be prepared to competently take the C)CSSM exam.

Prérequis de la Formation

- Mile2's C)SP
- 12 months of Information Systems Experience

Audience Ciblée

- Penetration Testers
- Microsoft Administrators
- Security Administrators
- Active Directory Admins

Programme

Module 1
- Introduction

Module 2
- Architectural Frameworks and Compliance

Module 3
- Risk Management and Controls

Module 4
- Evaluating Systems and Management Strategies

Module 5
- Incident Management, Law, and Ethics

Module 6
- Business Continuity and Disaster Recovery Processes

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Cybersecurity Systems Auditor

Objectifs

- Upon completion, Certified Cybersecurity Systems Auditor students will be able to establish industry acceptable Cyber Security & IS management standards with current best practices and be prepared to competently take the C)CSSA

Prérequis de la Formation

- Mile2's C)SP
- 12 months of Information Systems Experience

Audience Ciblée

- IS Security Officers
- Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security managers
- Government employees

Programme

Module 1

- The Process of Auditing Information Systems

Module 2

- Risk-Based Auditing

Module 3

- Audit Planning and Performance

Module 4

- IS Systems Reports

Module 5

- IT Governance and Management

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Penetration Testing Engineer

Objectifs

Upon completion, the Certified Penetration Testing Engineer, C)PTE, candidate will have solid knowledge of testing and reporting procedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTE exam.

Prérequis de la Formation

- Mile2 C)PEH or equivalent knowledge
- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security experience

Audience Ciblée

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Programme

Module 1
- Business & Technical Logistics of Pen Testing

Module 2
- Information Gathering

Module 3
- Detecting Live Systems

Module 4
- Banner Grabbing and Enumeration

Module 5
- Automated Vulnerability Assessment

Module 6
- Hacking an OS

Module 7
- Advanced Assessment and Exploitation Techniques

Module 8
- Evasion Techniques

Module 9
- Hacking with PowerShell

Module 10
- Networks and Sniffing

Module 11
- Hacking Web Tech

Module 12
- Mobile and IoT Hacking

Module 13
- Report Writing Basics

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Penetration Testing Consultant

Objectifs

Upon completion, the Certified Penetration Testing Consultant, C)PTC, candidate will have solid knowledge of testing and reporting proceedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTC exam.

Prérequis de la Formation

- Mile2 C)PEH and C)PTE or equivalent knowledge
- 2 years of experience in Networking Technologies
- Sound Knowledge of TCP/IP
- Computer Hardware Knowledge

Audience Ciblée

- IS Security Officers
- Cybersecurity Managers / Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Programme

Module 1
- Penetration Testing 6 Team Formation

Module 2
- NMAP Automation

Module 3
- Exploitation Process

Module 4
- Fuzzing with Spike

Module 5
- Simple Buffer - Overflow

Module 6
- Stack Based Windows - Buffer Overflow

Module 7
- Web Application - Security and Exploitation

Module 8
- Linux Stack Smashing & Scanning

Module 9
- Linux Address Space - Layout Randomization

Module 10
- Windows Exploit - Protection

Module 11
- Getting Around SHE - ASLR

Module 12
- Penetration Testing - Report Writing

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

La cybersécurité pour tous : Bonnes pratiques et hygiène numérique

Objectifs

- Comprendre les enjeux de la cybersécurité dans un contexte professionnel.
- Identifier les principales menaces informatiques et les comportements a risque.
- Adopter les bonnes pratiques pour garantir une hygiène numérique efficace au quotidien.

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Toute personne souhaitant connaître les bonnes pratiques de la cybersécurité .

Programme

Jour 1

- Matin : Comprendre les enjeux et identifier les menaces
- Après-midi : Adopter les bonnes pratiques et appliquer l'hygiène numérique

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

Gestion des identités et des accès (IAM)

Objectifs

- Définir ce qu'est l'IAM et pourquoi il est central dans une politique de cybersécurité.
- Décrire les principales fonctions et processus du cycle de vie des identités.
- Comprendre la gouvernance des accès et les modèles de droits (RBAC, SoD…).
- Identifier les enjeux métiers, techniques et organisationnels liés à l'IAM.
- Appréhender les solutions IAM du marché et les leviers de transformation.

Prérequis de la Formation

- Avoir des bases en systèmes d'information ou en cybersécurité.
- Une première exposition aux problématiques de gestion des accès est un plus.

Audience Ciblée

- Responsables IT, RSSI, analystes sécurité, gestionnaires d'habilitations.
- Consultants en cybersécurité, auditeurs techniques.
- Responsables RH ou métiers impliqués dans la gestion des droits.

Programme

- Introduction : Pourquoi l'IAM est un pilier de la cybersécurité moderne

Module 1

- Concepts fondamentaux – identités, rôles, habilitation

Module 2

- Cycle de vie des identités : création, modification, retrait

Module 3

- Modèles de gouvernance des accès : RBAC, ABAC, Zero Trust

Module 4

- Panorama des outils IAM : Azure AD, Okta, CyberArk, etc

- Cas pratique guidé : cartographie des droits dans un SI fictif
- QCM + échanges autour des projets IAM en entreprise

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

Les enjeux de la cybersécurité dans son organisation – pour les dirigeants

Objectifs

- Comprendre les enjeux stratégiques de la cybersécurité dans une organisation
- Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture
- Connaître le cadre réglementaire et les obligations le gales
- Favoriser une culture cyber dans l'entreprise

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Dirigeants d'entreprises,
- Cadre d'entreprise,
- Responsable informatique.

Programme

Jour 1

- Matin : Comprendre la cybersécurité comme enjeu stratégique
- Après-midi : Gouvernance et obligations réglementaires

Jour 2

- Matin : Développer une culture de cybersécurité

Informations Pratiques

1/5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

Chiffrement & Gestion des Secrets

Objectifs

- Expliquer les mécanismes de base du chiffrement des données.
- Identifier les solutions adaptées selon l'environnement (cloud, datacenter, endpoint…).
- Gérer le cycle de vie des clés, certificats, tokens et secrets.
- Choisir des solutions de chiffrement adaptées à leur SI (on-prem et SaaS).
- Évaluer les exigences réglementaires et normatives associées au chiffrement.

Prérequis de la Formation

- Connaissances de base en systèmes d'information et sécurité.
- Aucune compétence mathématique en cryptographie requise.

Audience Ciblée

- RSSI, responsables sécurité, DSI, consultants SSI.
- Administrateurs système, cloud, réseau.
- Intégrateurs, architectes IT et toute personne impliquée dans la protection des données sensibles.

Programme

Module 1

- Principes fondamentaux du chiffrement

Module 2

- Gestion des secrets et des clés

Module 3

- Solutions de chiffrement selon l'environnement

Module 4

- Chiffrement & certificats : enjeux et pratiques

Module 5

- Gouvernance, audit et conformité

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SECURE SCADA – Piloter la cybersécurité d'un réseau industriel et prévenir les intrusions OT

Objectifs

- Identifier les vulnérabilités critiques d'un système industriel connecté
- Appliquer les bonnes pratiques de défense en profondeur dans un contexte OT
- Sécuriser les automates programmables et leurs interfaces
- Mettre en place un cloisonnement réseau adapté (VLAN, filtrage MAC, ACL)
- Installer et configurer un système de détection d'incident (SIEM) adapté à l'environnement industriel
- Réaliser un audit basique de sécurité sur un réseau OT

Prérequis de la Formation

- Connaissances de base en automatisme industriel (API, supervision)
- Connaissances générales en réseaux IP et architecture de supervision
- Appétence pour les environnements techniques (protocoles, topologies)

Audience Ciblée

- RSSI
- Intégrateurs OT/SCADA
- Responsables supervision ou maintenance industrielle
- Responsables techniques / industriels
- Administrateurs systèmes industriels
- Automaticiens

Programme

Jour 1

- Fondamentaux OT & vulnérabilités industrielles

Jour 2

- Cloisonnement, durcissement, sécurisation API

Jour 3

- Supervision, détection et audit OT

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

OSINT (Open Source Intelligence)

Objectifs

- Comprendre les principes et enjeux de l'OSINT
- Maîtriser les outils et techniques pour la collecte d'informations
- Collecter, trier et analyser les données recueillies
- Utiliser des outils d'intelligence artificielle (IA) pour automatiser, filtrer et analyser des données issues de sources ouvertes
- Intégrer l'OSINT dans un cadre opérationnel.

Prérequis de la Formation

- Connaissance de base en informatique, notions en analyse de données et de rédaction.

Audience Ciblée

- RSSI,
- SOC Manager,
- Analystes SOC,
- Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise.

Programme

Jour 1

- Matin : Introduction & cadre légal / Cycle du renseignement / Sources ouvertes / Quiz
- Après-midi : Méthodologies de recherche / Recherche avancée / Collecte automatique / Exercices pratiques

Jour 2

- Matin : Réseaux sociaux & métadonnées / Registres publics & bases de données / Dark web / deep web / Quiz
- Après-midi : Outils OSINT avancés (Maltego, Shodan…) / Corrélation des données / • IA appliquée / Étude de cas pratique

Jour 3

- Matin : Structuration d'un service OSINT & intégration / Reporting & restitution / Veille ciblée / Quiz
- Après-midi : Investigation de bout en bout / Atelier en groupe / Diffusion aux décideurs / Clôture & évaluation finale

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

Threat Intelligence

Objectifs

- Comprendre les fondamentaux de la CTI (Cyber Threat Intelligence)
- Savoir collecter et analyser les informations sur les menaces
- Utiliser l'intelligence artificielle (IA) pour automatiser la collecte, l'analyse et la corrélation d'informations liées aux menaces
- Transformer les données en données exploitables
- Intégrer les outils et méthodes de la CTI dans le processus de sécurité de son organisation.

Prérequis de la Formation

- Connaissances de base dans le fonctionnement des systèmes d'information et en cyber sécurité.

Audience Ciblée

- RSSI,
- SOC Manager,
- Analystes SOC,
- Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise.

Programme

Jour 1

- Matin : Introduction à la CTI / Concepts & modèles (MITRE ATT&CK, Diamond, Kill Chain) / Typologies de menaces
- Après-midi :CTI dans l'organisation (SOC, CERT, RSSI) / Cas pratiques & classification des menaces

Jour 2

- Matin : Collecte (OSINT, Dark Web, SIEM, EDR) / IoC & IoA
- Après-midi : Analyse des TTP / Outils CTI (MISP, YARA, Sigma) / Atelier pratique

Jour 3

- Matin : Automatisation & IA / Transformation des données / Rapports CTI (RSSI, COMEX, SOC)
- Après-midi : Mise en place d'un service CTI / Simulation & restitution / Clôture & attestations

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBERSÉCURITÉ

Référent Cybersécurité en TPE/PME

Objectifs

- Comprendre les enjeux et menaces liés à la cybersécurité dans le contexte TPE/PME.
- Savoir identifier les risques spécifiques et y répondre avec des mesures pragmatiques.
- Être capable de structurer une politique de sécurité (PSSI) adaptée à la taille de l'organisation.
- Développer des réflexes opérationnels en cas d'incident de sécurité.
- Intégrer la cybersécurité dans les processus métier, la gouvernance et la culture d'entreprise.
- Être autonome dans la mise en œuvre de la conformité réglementaire (RGPD, NIS2, etc.).
- Constituer une boîte à outils de veille et de réponse aux menaces.

Prérequis de la Formation

- Maîtrise de l'environnement numérique d'entreprise
- Connaissances de base en réseaux et systèmes (niveau utilisateur averti)
- Appétence pour les enjeux technico-réglementaires

Audience Ciblée

- Référents cybersécurité / SSI
- DSI, RSI, RSSI en environnement PME
- Responsables informatiques
- Responsables conformité ou RGPD
- Dirigeants techniques ou chefs d'entreprise

Programme

Jour 1

- Fondamentaux, enjeux, cadre juridique

Jour 2

- Hygiène numérique & sécurité de base

Jour 3

- Analyse de risque et PSSI PME

Jour 4

- Externalisation, innovation, crise

Jour 5

- Sécurité web, boîte à outils du référent cybersécurité & Projet de synthèse

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB CERTIFIED ISO 22301 Foundation

Objectifs

- Décrire les concepts, principes et définitions du management de la continuité d'activité
- Expliquer les principales exigences d'ISO 22301 pour un système de management de la continuité d'activité (SMCA)
- Identifier les approches et les techniques utilisées pour la mise en œuvre et la gestion d'un SMCA

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne impliquée dans le management de la continuité d'activité
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus d'un Système de management de la continuité d'activité
- Personnes souhaitant poursuivre une carrière dans le management de la continuité d'activité

Programme

Jour 1

- Introduction au Système de management de la continuité d'activité (SMCA) et à la norme ISO 22301

Jour 2

- Système de management de la continuité d'activité
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB

PECB CERTIFIED ISO 22301 Lead Implementer

Objectifs

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

Prérequis de la Formation

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

Audience Ciblée

- Les responsables de projets et les consultants impliqués dans la continuité d'activité
- Les conseillers experts cherchant à maîtriser la mise en œuvre du système de management de la continuité d'activité
- Les personnes chargées de maintenir la conformité aux exigences du SMCA au sein d'un organisme

Programme

Jour 1

- Introduction à l'ISO 22301 et déclanchement d'un SMCA

Jour 2

- Plan de mise en œuvre d'un SMCA

Jour 3

- Mise en œuvre d'un SMCA

Jour 4

- Suivi du SMCA, amélioration continue et préparation à l'audit de certification

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB

PECB CERTIFIED ISO 22301 Lead Auditor

Objectifs

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

Prérequis de la Formation

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

Audience Ciblée

- Auditeurs cherchant à réaliser et à mener des audits de systèmes de management de la continuité d'activité (SMCA)
- Gestionnaires ou consultants cherchant à maîtriser le processus d'audit du système de management de la continuité d'activité
- Personnes chargées de maintenir la conformité aux exigences du SMCA dans une entreprise.
- Experts techniques cherchant à se préparer à l'audit du système de management de la continuité d'activité
- Conseillers experts en management de la continuité d'activité

Programme

Jour 1

- Introduction au système de management de la continuité d'activité (SMCA) et à ISO 22301

Jour 2

- Principes d'audit, préparation et déclenchement d'un audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB CERTIFIED Disaster Recovery Manager

Objectifs

- Connaître la corrélation entre la reprise d'activité après sinistre et d'autres normes, cadres réglementaires et domaines des TI
- Comprendre les concepts, les approches, les méthodes et les techniques utilisées pour la mise en œuvre et la gestion efficace d'un plan de reprise d'activité après sinistre
- Savoir interpréter les stratégies de reprise d'activité après sinistre des TIC dans le contexte spécifique d'une organisation
- Développer l'expertise pour soutenir une organisation afin de planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement les services de reprise après sinistre en conformité avec les meilleures pratiques

Prérequis de la Formation

- Une compréhension fondamentale des services de reprise d'activité après sinistre et une connaissance approfondie des principes de gestion.

Audience Ciblée

- Professionnels de reprise d'activité après sinistre souhaitant acquérir une connaissance approfondie des meilleures pratiques en matière de reprise d'activité après sinistre
- Personnes responsables de la mise en œuvre et la gestion continue d'un plan de reprise d'activité après sinistre dans une organisation
- Membres de l'équipe chargée de la reprise d'activité après sinistre

Programme

Jour 1

- Introduction à la reprise d'activité après sinistre et lancement d'un plan de reprise d'activité après sinistre

Jour 2

- Stratégies d'atténuation des risques et planification de la reprise d'activité après sinistre

Jour 3

- Services sous-traités de reprise d'activité après sinistre, réponse et activation, formation et test

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB

PECB CERTIFIED Lead Disaster Recovery Manager

Objectifs

- Expliquer les concepts fondamentaux de la reprise après sinistre et de ses différents aspects
- Lancer le projet de planification de la reprise après sinistre selon les meilleures pratiques
- Effectuer une évaluation des risques et une analyse d'impact sur l'activité et concevoir des stratégies d'atténuation
- Élaborer un plan de reprise après sinistre et analyser le plan de réponse aux incidents, le plan d'urgence et le plan de gestion de crise
- Effectuer des tests de reprise après sinistre et prendre des mesures de performance nécessaires

Prérequis de la Formation

- La principale condition pour participer à cette formation est d'avoir une connaissance générale des concepts et stratégies de reprise après sinistre.

Audience Ciblée

- Professionnels ou consultants souhaitant apprendre à mettre en œuvre des projets de planification de la reprise après sinistre, à réaliser des évaluations des risques et des AIA, ainsi qu'à effectuer des tests de reprise après sinistre et à prendre des mesures de performance nécessaires
- Responsables de l'établissement d'un plan de reprise après sinistre dans une organisation
- Personnes chargées de maintenir l'infrastructure informatique d'une organisation
- Membres d'une équipe de reprise après sinistre

Programme

Jour 1

- Introduction à la planification de la reprise après sinistre et à l'évaluation des risques

Jour 2

- Analyse d'impact sur l'activité et élaboration du plan de reprise après sinistre (PRS)

Jour 3

- Sous-composants du PRS, sites de reprise et activation du plan de reprise après sinistre

Jour 4

- Test de reprise après sinistre, mesure des performances et amélioration continue

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB

PECB CERTIFIED Lead Crisis Manager

Objectifs

- Expliquer les concepts fondamentaux et les principes de la gestion des crises sur la base de la norme ISO 22361
- Établir, maintenir et améliorer en permanence un cadre de gestion des crises comprenant le leadership, la structure, la culture et les compétences.
- Anticiper, évaluer, prévenir et préparer les crises
- Réagir aux crises, s'en remettre et en tirer des enseignements afin d'améliorer la capacité de gestion des crises de l'organisation.

Prérequis de la Formation

- Les participants qui souhaitent suivre cette formation doivent avoir une compréhension fondamentale des concepts, du cadre et du processus de gestion de crise.

Audience Ciblée

- Personnes responsables de la mise en place d'une capacité de gestion des crises au sein d'une organisation
- Personnes responsables de la mise en œuvre d'un plan et d'une structure de gestion des crises au sein de l'organisation
- Le(s) responsable(s) de crise
- Les membres des équipes de gestion de crise
- Personnes cherchant à comprendre en profondeur la gestion de crise
- Les personnes souhaitant démarrer ou faire progresser leur carrière dans le domaine de la gestion de crise
- Consultants, conseillers et professionnels souhaitant acquérir une connaissance approfondie des lignes directrices de l'ISO 22361 sur la gestion de crise

Programme

Jour 1

- Introduction à l'ISO 22361 et à la gestion de crise

Jour 2

- Framework de gestion de crises

Jour 3

- Prévention et préparation aux crises

Jour 4

- Réponse aux crises et rétablissement

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CONTINUITÉ ET REPRISE D'ACTIVITÉ PCA ET PRA

PECB CERTIFIED DORA Lead Manager

Objectifs

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

Prérequis de la Formation

- La principale exigence pour participer à cette formation est d'avoir une compréhension fondamentale des concepts de la sécurité de l'information et de la cybersécurité et de se familiariser avec les principes de gestion des risques liés aux TIC.

Audience Ciblée

- Cadres supérieurs et décideurs des institutions financières
- Responsables de la conformité et gestionnaires de risques
- Professionnels des TI
- Personnel des affaires juridiques et réglementaires
- Consultants et conseillers spécialisés dans la règlementation financière et la cybersécurité

Programme

Jour 1

- Introduction des concepts et exigences de DORA

Jour 2

- Gestion des risques et incidents liés aux TIC

Jour 3

- Gestion des risques liés aux prestataires tiers et partage des informations

Jour 4

- Réévaluation et amélioration continuelle

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

EC-Council

EC-Council – Web Application Hacking and Security (WAHS)

Objectifs

The EC-Council Web Application Hacking and Security (WAHS) course equips participants with hands-on skills to identify, exploit, and secure against critical web vulnerabilities such as SQL Injection, XSS, CSRF, SSRF, authentication bypass, IDOR, file inclusion, command injection, and privilege escalation. Delivered through challenge-based, CTF-style labs, it prepares learners to conduct realistic penetration tests under pressure while strengthening their ability to secure web applications. Successful candidates earn certification at three levels — Associate, Professional, or Expert — based on exam performance.

Prérequis de la Formation

- Basic web/app knowledge, Linux/OS familiarity, scripting skills, for security professionals.

Audience Ciblée

- If you are tasked with implementing, managing, or protecting web applications, then this course is for you. If you are a cyber or tech professional who is interested in learning or recommending mitigation methods to a myriad of web security issues and want a pure hands-on program, then this is the course you have been waiting for.

Programme

You will learn about application vulnerabilities and web application hacking. Even though this will prove useful for other CTF contests, and in cracking VVMs, it will be even more useful to your career as you learn to defend your applications and progress to Web Application Hacking and Security.

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) – GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with
- Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning
- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

W|AHS Web Application Hacking & Security

EC-Council – Disaster Recovery Professional (EDRP)

Objectifs

The EC-Council Disaster Recovery Professional (E|DRP) certification is designed to educate and validate a candidate's ability to plan, strategize, implement, and maintain a business continuity and disaster recovery plan.

Prérequis de la Formation

- Some experience in the IT BC/DR domain

Audience Ciblée

- IT Professionals in the BC/DR or System Administration domain
- Business Continuity and Disaster Recovery Consultants
- Individuals wanting to establish themselves in the field of IT Business Continuity and Disaster Recovery
- IT Risk Managers and Consultants
- CISOs and IT Directors

Programme

Module 1
- Introduction to Disaster Recovery and Business Continuity

Module 2
- Business Continuity Management (BCM)

Module 3
- Risk Assessment

Module 4
- Business Impact Analysis (BIA)

Module 5
- Business Continuity Planning (BCP)

Module 6
- Data Backup Strategies

Module 7
- Data Recovery Strategies

Module 8
- Virtualization-Based Disaster Recovery

Module 9
- System Recovery

Module 10
- Centralized and Decentralized System Recovery

Module 11
- Disaster Recovery Planning Process

Module 12
- BCP Testing, Maintenance, and Training

Informations Pratiques

E-LEARNING

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **EC-Council**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

EC-Council Disaster Recovery Professional™

DORA (Digital Operational Resilience Act), mettre en place une stratégie de résilience numérique

Objectifs

- Comprendre les principaux objectifs et concepts clés du règlement DORA
- Connaître les différents types de cyber-risques
- Identifier les obligations en matière de sécurité des données et de conformité réglementaire
- Appréhender les bonnes pratiques de sécurité numérique et sensibiliser les collaborateurs
- Mettre en place et établir une stratégie de résilience numérique

Prérequis de la Formation

- Connaissances de base en cybersécurité et sécurité des systèmes d'information.

Audience Ciblée

- RSSI et référents sécurité, architectes sécurité, directeurs et responsables informatiques, ingénieurs IT, chefs de projet (MOE, MOA), auditeurs de sécurité et juristes réglementaires IT.

Programme

Module 1

- Gestion des risques liés aux technologies de l'information et de la communication (TIC)

Module 2

- Gestion, classification et déclaration des incidents liés aux TIC

Module 3

- Les tests de résilience opérationnelle numérique

Module 4

- Gestion des risques liés aux prestataires tiers de services

Module 5

- Dispositions relatives à l'échange d'informations

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

GOUVERNANCE, RISQUE ET CONFORMITÉ

PECB ISO 37001 Foundation

Objectifs

- Décrire les concepts, principes et définitions du management anti-corruption
- Expliquer les principales exigences d'ISO 37001 pour un système de management anti-corruption
- Identifier les actions et approches potentielles que les organisations peuvent utiliser pour atteindre la conformité à ISO 37001

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Managers et consultants souhaitant se familiariser avec les exigences d'ISO 37001 pour un système de management anti-corruption (SMAC).
- Responsables chargés de pratiquer la diligence raisonnable à l'égard des risques de corruption
- Les personnes souhaitant contribuer au maintien de l'intégrité de l'organisation en soutenant un comportement éthique.
- Les responsables et les membres des équipes de gouvernance, de management des risques et de conformité
- Les personnes aspirant à devenir des consultants anti-corruption

Programme

Jour 1

- Introduction au système de management anticorruption (SMAC) et aux articles 4-6 d'ISO 37001

Jour 2

- Articles 7-10 d'ISO 37001
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

PECB CERTIFIED ISO/IEC 38500 Foundation

Objectifs

- Comprendre les éléments fondamentaux de la gouvernance des technologies de l'information pour l'entreprise
- Comprendre les principes de bonne gouvernance des TI
- Connaître les approches, les méthodes et les techniques permettant de gouverner efficacement l'utilisation des TI

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne impliquée dans la gouvernance des technologies de l'information pour l'entreprise
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus de la gouvernance des technologies de l'information
- Personnes souhaitant poursuivre une carrière dans la gouvernance des technologies de l'information pour l'entreprise

Programme

Jour 1

- Introduction aux pratiques de gouvernance des TI selon la norme ISO /IEC 38500

Jour 2

- Principes de la gouvernance des TI
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

PECB CERTIFIED ISO/IEC 38500 IT Governance Manager

Objectifs

- Comprendre les principes fondamentaux de l'ISO/IEC 38500 et apprendre à les interpréter
- Connaître le modèle ISO/IEC 38500 Évaluer – Diriger - Surveiller
- Acquérir les connaissances nécessaires pour évaluer, diriger et surveiller l'utilisation des technologies de l'information dans une organisation
- Comprendre COBIT 5 et CGEIT

Prérequis de la Formation

- Suivre la formation ISO/IEC 38500 IT Corporate Governance Manager ne nécessite aucun prérequis.

Audience Ciblée

- Gestionnaires ou consultants chargés d'assurer une bonne gouvernance des technologies de l'information au sein d'une organisation
- Personnes souhaitant acquérir une connaissance approfondie des principes fondamentaux de la gouvernance des technologies de l'information
- Membres d'une équipe de gouvernance des technologies de l'information
- Conseillers spécialisés impliqués dans la gouvernance des technologies de l'information

Programme

Jour 1

- Introduction à la gouvernance des TI et à la norme ISO/IEC 38500

Jour 2

- Principes pour l'utilisation des technologies de l'information de manière efficace, efficiente et acceptable

Jour 3

- Résultats, techniques de mesure de la performance et examen de certification

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

PECB

PECB CERTIFIED ISO/IEC 38500 Lead IT Governance Manager

Objectifs

- Maîtriser les principes fondamentaux de l'ISO/IEC 38500, leurs avantages ainsi que leur application dans une organisation
- Comprendre le modèle ISO/IEC 38500 Évaluer-Diriger-Surveiller et apprendre à l'intégrer au sein d'une organisation
- Comprendre COBIT 5 et CGEIT et comment ils complètent l'ISO/IEC 38500
- Savoir appliquer, gérer et surveiller efficacement la gouvernance des TI au sein de l'organisation
- Acquérir l'expertise pour conseiller une organisation sur les meilleures pratiques de la Gouvernance TI en conformité avec l'ISO/IEC 38500, COBIT 5 et CGEIT afin d'assurer une bonne gouvernance des technologies de l'information

Prérequis de la Formation

- Une compréhension fondamentale de l'ISO/IEC 38500 et une connaissance approfondie de la gouvernance des TI..

Audience Ciblée

- Gestionnaires ou consultants chargés d'assurer une bonne gouvernance des TI au sein d'une organisation et une gestion efficace de ses risques
- Conseillers spécialisés souhaitant acquérir une connaissance approfondie des principaux concepts et principes de la gouvernance des TI
- Experts techniques désirant formaliser, modifier et / ou étendre les objectifs liés à la technologie de l'information d'une organisation
- Membres de groupes de surveillance des ressources au sein d'une organisation
- Membres de l'équipe de gouvernance des technologies de l'information et / ou de la sécurité de l'information

Programme

Jour 1

- Introduction à la gouvernance des TI et à la norme ISO/IEC 38500

Jour 2

- Stratégie des technologies de l'information et acquisition

Jour 3

- Performance et gestion des risques

Jour 4

- Gestion des ressources, conformité et comportement humain

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED NIS 2 Directive Lead Implementer

Objectifs

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

Prérequis de la Formation

Les principales exigences pour participer à cette formation sont d'avoir une compréhension fondamentale de la cybersécurité.

Audience Ciblée

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

Programme

Jour 1

- Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2

Jour 2

- Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques

Jour 3

- Contrôles de cybersécurité, gestion des incidents et gestion de crise

Jour 4

- Communication, tests, contrôle et amélioration continue de la cybersécurité

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

ISACA CERTIFIED COBIT 2019 Foundation

Objectifs

- COBIT® is a framework for the enterprise governance and management of information and technology (I&T) that supports enterprise goal achievement. Certificate holders gain a deeper understanding of governance and management objectives, how to align IT with business goals, and how to map and create customized I&T governance frameworks.

Prérequis de la Formation

- Having solid practical experience in the field of information systems management is highly recommended.

Audience Ciblée

Current COBIT 5 Foundation certificate holders as well as those new to COBIT who are interested in achieving the latest foundation certificate. It can be beneficial for strategic roles in GRC and IT Governance, including:

- Senior Manager
- Business Manager
- IT Manager
- Assurance Providers
- Risk Management
- Regulator
- GRC Manager
- Consultant
- Solutions Architect
- Program Manager
- Security and Compliance Advisors

Programme

Domain 1

- COBIT Framework Introduction

Domain 2

- Principles

Domain 3

- Business Case

Domain 4

- Governance Systems and Components

Domain 5

- Designing a Tailored Governance System

Domain 6

- Governance and Management Objectives

Domain 7

- Implementation

Domain 8

- Performance Management

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

COBIT
An ISACA® Framework

GOUVERNANCE, RISQUE ET CONFORMITÉ

ISACA CERTIFIED in the Governance of Enterprise IT

Objectifs

- Apprendre à définir, établir et administrer un cadre de gouvernance de l'informatique d'entreprise.
- Apprendre à vous assurer que les investissements activés par l'informatique sont administrés pour fournir des avantages commerciaux optimisés.
- Apprendre à soutenir et à permettre la réalisation des objectifs de l'entreprise.

Prérequis de la Formation

- Vous devez avoir au moins cinq ans d'expérience dans la gestion, le rôle consultatif ou de supervision, et/ou le soutien de la gouvernance des contributions liées à l'informatique au sein d'une entreprise.

Audience Ciblée

- Professionnels ayant 5 ans d'expérience ou plus dans l'établissement et la gestion d'un cadre de gouvernance de l'informatique et de la technologie (I&T), ainsi que dans des rôles consultatifs ou de supervision, et/ou soutenant d'une autre manière la gouvernance des contributions liées à l'informatique. Cela inclut :
    - SVP, VP, Directeurs
    - Professionnels informatiques soutenant la haute direction : Consultants, Cadres supérieurs, Gestionnaires, Ingénieurs seniors
- La gouvernance relève en fin de compte de la responsabilité de la haute direction et du conseil d'administration. Par conséquent, une compréhension de haut niveau de la gouvernance de l'I&T est essentielle à ce niveau pour qu'ils puissent habiliter les praticiens de la gouvernance et parrainer les bonnes initiatives.

Programme

Domain 1

- Gouvernance de l'informatique d'entreprise

Domain 2

- Ressources informatiques

Domain 3

- Réalisation des avantages

Domain 4

- Optimisation des risques

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

ISC2 CERTIFIED in Governance, Risk and Compliance

Objectifs

- Identify and describe the steps and tasks within the NIST Risk Management Framework (RMF).
- Apply common elements of other risk management frameworks using the RMF as a guide.
- Describe the roles associated with the RMF and how they are assigned to tasks within the RMF.
- Execute tasks within the RMF process based on assignment to one or more RMF roles.
- Explain organizational risk management and how it is supported by the RMF.

Prérequis de la Formation

- To qualify for the CGRC, candidates must have at least two years of cumulative, paid work experience in one or more of the seven domains of the current ISC2 CGRC Exam Outline.
- If you don't yet have the required experience, you may become an Associate of ISC2 after successfully passing the CGRC exam. The Associate of ISC2 will then have three years to earn the experience needed for the CGRC certification

Audience Ciblée

This course is for individuals planning to pursue the CGRC certification. The CGRC is ideal for IT, information security and information assurance practitioners and contractors who use the RMF in federal government, military, civilian roles, local governments and private sector organizations. Roles include:

- ISSOs, ISSMs and other infosec/information assurance practitioners who are focused on security assessment and authorization (traditional C&A) and continuous monitoring issues.
- Executives who must « sign off » on Authority to Operate (ATO).
- Inspector generals (IGs) and auditors who perform independent reviews.
- Program managers who develop or maintain IT systems.
- IT professionals interested in improving cybersecurity and learning more about the importance of lifecycle cybersecurity risk management.

Programme

Domain 1

- Information Security Risk Management Program

Domain 2

- Scope of the Information System

Domain 3

- Selection and Approval of Security and Privacy Controls

Domain 4

- Implementation of Security and Privacy Controls

Domain 5

- Assessment/Audit of Security and Privacy Controls

Domain 6

- Authorization/Approval of Information System

Domain 7

- Continuous Monitoring

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CGRC®

GOUVERNANCE, RISQUE ET CONFORMITÉ

EBIOS RM Piloter la cybersécurité par la maîtrise du risque numérique

Objectifs

- Mettre en œuvre la méthode EBIOS Risk Manager sur un cas réel ou simulé
- Comprendre les concepts fondamentaux : risque, menace, vulnérabilité, gravité
- Identifier les biens supports, objectifs visés et sources de risque
- Élaborer des scénarios stratégiques et opérationnels, orientés sur les menaces
- Choisir et planifier des mesures de traitement des risques
- Consolider une démarche complète de management des risques SSI
- Accompagner une organisation vers une cybersécurité raisonnée, pilotée et documentée

Prérequis de la Formation

- Connaissances générales en sécurité des systèmes d'information
- Familiarité avec les SI, les notions de gouvernance ou d'audit
- Appétence pour les démarches méthodologiques & collaboratives

Audience Ciblée

- Risk Managers / Responsables SSI
- RSSI / DSI / MOA / Directeurs projets
- Consultants en sécurité des SI
- Auditeurs SI & SMSI/ homologateurs SSI
- Responsables conformité (NIS2, RGPD, ISO 27001)
- Chefs de projets numériques

Programme

Jour 1

- Fondamentaux & Atelier 1 : Cadrage et socle

Jour 2

- Ateliers 2 à 4 : Menaces & scénarios

Jour 3

- Atelier 5 & Étude de cas finale

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GOUVERNANCE, RISQUE ET CONFORMITÉ

NIS 2

Objectifs

- Connaître la législation NIS2
- Intégrer les exigences de la législation NIS2 dans son organisation.

Prérequis de la Formation

- Connaissances de base en cybersécurité et sécurité des systèmes d'information.

Audience Ciblée

- RSSI,
- DSI,
- Ingénieurs IT,
- Chefs de projet,
- Auditeurs de sécurité et juristes règlementaires IT ou tout autre personne implique e dans la sécurité de son organisation.

Programme

Jour 1

- Matin : Introduction à la directive NIS2 et son contexte
- Après-midi : Exigences organisationnelles et techniques

Jour 2

- Matin : Gestion des incidents et reporting
- Après-midi : Mise en conformité et intégration opérationnelle

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RISK MANAGEMENT

RISK MANAGEMENT

PECB

PECB ISO/IEC 27005 Foundation

Objectifs

- Décrire les principaux concepts, principes et définitions de la gestion des risques
- Interpréter les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information
- Identifier les approches, les méthodes et les techniques utilisées pour la mise en œuvre et la gestion d'un programme de gestion des risques liés à la sécurité de l'information

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Professionnels de la gestion des risques
- Professionnels souhaitant se familiariser avec les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information
- Personnel chargé de la gestion des risques liés à la sécurité de l'information dans son domaine de responsabilité
- Personnes intéressées par une carrière dans la gestion des risques liés à la sécurité de l'information

Programme

Jour 1

- Introduction à la norme ISO/IEC 27005 et aux concepts fondamentaux de la gestion des risques liés à la sécurité de l'information

Jour 2

- Gestion des risques liés à la sécurité de l'information
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/CEI 27005 Risk Manager

Objectifs

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

Prérequis de la Formation

- La formation Les fondamentaux du management du risque constitue le prérequis idéal pour suivre ce cours.

Audience Ciblée

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

Programme

Jour 1

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

Jour 2

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

Jour 3

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

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/IEC 27005 Lead Risk Manager

Objectifs

- Expliquer les concepts et principes de gestion des risques définis par les normes ISO/IEC 27005 et ISO 31000
- Mettre en place, maintenir et améliorer un cadre de gestion des risques liés à la sécurité de l'information conformément aux lignes directrices de la norme/IEC 27005
- Appliquer les processus de gestion des risques liés à la sécurité de l'information conformément aux lignes directrices de la norme/IEC 27005
- Planifier et mettre en place des activités de communication et de consultation sur les risques
- Surveiller, réviser et améliorer le cadre et le processus de gestion des risques liés à la sécurité de l'information en fonction des résultats des activités de gestion de ces risques

Prérequis de la Formation

- La participation à cette formation requiert une compréhension fondamentale de la norme/IEC 27005 et des connaissances approfondies de la gestion des risques et de la sécurité de l'information.

Audience Ciblée

- Responsables ou consultants impliqués ou responsables de la sécurité de l'information dans une organisation
- Personnes responsables de la gestion des risques liés à la sécurité de l'information
- Membres des équipes de sécurité de l'information, professionnels de l'informatique et responsables de la protection de la vie privée
- Personnes responsables du maintien de la conformité aux exigences de sécurité de l'information de la norme/IEC 27001 au sein d'une organisation
- Gestionnaire de projet, consultants ou conseillers experts cherchant à maîtriser la gestion des risques liés à la sécurité de l'information

Programme

Jour 1

- Introduction à la norme ISO/IEC 27005 et à la gestion des risques

Jour 2

- Identification, évaluation et traitement des risques conformément à la norme ISO/IEC 27005

Jour 3

- Acceptation, communication, consultation, surveillance et révision des risques liés à la sécurité de l'information

Jour 4

- Méthodes d'évaluation des risques

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/IEC 27005 AVEC MEHARI

Objectifs

- Comprendre les concepts, les approches, les méthodes et les techniques permettant une gestion efficace du risque selon la norme ISO/IEC 27005
- Interpréter les exigences de la norme ISO/IEC 27001 pour le management de la sécurité de l'information
- Acquérir les compétences nécessaires pour conduire une appréciation du risque avec la méthode MEHARI
- Maîtriser les démarches pour conduire une appréciation du risque avec la méthode MEHARI
- Comprendre la relation entre le management du risque de la sécurité de l'information, les mesures de sécurité et la conformité avec les autres exigences de différentes parties prenantes dans une organisation
- Acquérir les compétences pour la mise en œuvre, le maintien et la gestion d'un programme de gestion du risque de la sécurité de l'information selon la norme ISO/IEC 27005
- Acquérir les compétences pour conseiller de manière efficace les organisations sur les meilleures pratiques de management du risque de la sécurité de l'information

Prérequis de la Formation

- Connaissance des principes fondamentaux de la cybersécurité.
- Compréhension des concepts de base des systèmes d'information.
- Expérience professionnelle dans le domaine de la sécurité de l'information est un plus, bien que ce ne soit pas obligatoire.
- Une familiarité avec les normes ISO/IEC 27001 et ISO/IEC 27005 est utile, mais pas indispensable.

Audience Ciblée

- Les managers des risques
- Les personnes responsables de la sécurité de l'information ou de la conformité dans une organisation
- Les membres d'une équipe chargée de la sécurité de l'information
- Les consultants des TI
- Le personnel chargé de la mise en œuvre ou souhaitant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de gestion des risques, conforme à la méthode MEHARI

Programme

Jour 1

- Introduction, programme de gestion du risque selon la norme ISO/IEC 27005

Jour 2

- Identification, appréciation, évaluation, traitement, acceptation, communication et surveillance relatives au risque selon l'ISO/IEC 27005

Jour 3

- Examen et déclenchement de l'appréciation du risque avec MEHARI

Jour 4

- Appréciation des vulnérabilités et du risque, selon MEHARI

Jour 5

- Planification de la sécurité selon MEHARI et examen

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RISK MANAGEMENT

PECB

PECB CERTIFIED EBIOS Risk Manager

Objectifs

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

Prérequis de la Formation

- Une connaissance en gestion du risque est recommandée.

Audience Ciblée

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnes 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

Programme

Jour 1

- Introduction à la méthode EBIOS et ateliers 1 & 2

Jour 2

- Ateliers 3, 4 et 5 – Scénarios et traitement du risque

Jour 3

- Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité.

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB Certified NIST Cybersecurity Professional

Objectifs

- Discuter des principes et concepts fondamentaux de la cybersécurité
- Soutenir la conformité aux principales publications du NIST, y compris le NIST 800-12, le NIST 800-53, le NIST RMF, le NIST 800-171 et le NIST CSF
- Évaluer les contrôles de sécurité et prodiguer des conseils à cet égard, en conformité avec les lignes directrices du NIST
- Fournir des orientations sur la gestion des risques en cybersécurité et les stratégies de gestion des incidents
- Guider les organisations dans le développement et l'optimisation de leurs programmes de cybersécurité

Prérequis de la Formation

- La formation PECB Certified NIST Cybersecurity Professional nécessite une connaissance de base en cybersécurité. Pour l'obtention de la certification professionnelle, le candidat doit justifier de 5 ans d'expérience, dont 2 ans en cybersécurité, ainsi qu'au moins 300 heures d'implication dans un programme de cybersécurité, et accepter le Code d'éthique PECB

Audience Ciblée

- Dirigeants ou administrateurs responsables de la supervision des initiatives de cybersécurité au sein de leur organisation
- Administrateurs systèmes et ingénieurs réseaux souhaitant approfondir leur compréhension des contrôles de sécurité et des processus de gestion des risques afin de se conformer aux normes de sécurité du NIST
- Professionnels impliqués dans le développement et la mise en œuvre de programmes de cybersécurité
- Professionnels et conseillers qui fournissent des services de cybersécurité et de conformité, en veillant à rester informés des derniers cadres et bonnes pratiques du NIST
- Enquêteurs en criminalistique numérique et en cybercriminalité qui doivent comprendre les aspects techniques et réglementaires des cadres de cybersécurité afin d'enquêter sur les incidents de sécurité et d'y répondre de manière complète
- Personnes travaillant en cybersécurité ou en sécurité de l'information qui visent à approfondir leur compréhension des lignes directrices du NIST et à développer des compétences pratiques en gestion des risques liés à la cybersécurité

Programme

Jour 1

- Introduction aux normes et principes de cybersécurité du NIST

Jour 2

- Stratégie de gestion des risques et gestion des risques liés à la chaîne d'approvisionnement

Jour 3

- Sélection des contrôles de sécurité, sensibilisation et formation, et surveillance continue

Jour 4

- Gestion des incidents de cybersécurité

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB Certified ISO 21502 Lead Project Manager

Objectifs

- Expliquer les concepts fondamentaux, les approches et les méthodologies en matière de management de projet
- Mettre en œuvre des pratiques de management de projet intégrées basées sur ISO 21502 lors de la réalisation d'un projet
- Mettre en œuvre des pratiques individuelles de management de projet basées sur ISO 21502 lors de la réalisation d'activités de projet

Prérequis de la Formation

- Les participants doivent avoir des connaissances de base en gestion de projet et une compréhension générale des normes ISO

Audience Ciblée

- Responsables de projet
- Commanditaires du projet
- Conseillers experts
- Membres de l'équipe de projet
- Cadres, managers et directeurs impliqués dans la gouvernance, la direction et les audits de projets.
- Personnes cherchant à comprendre en profondeur le management de projet.
- Personnes souhaitant démarrer ou faire progresser leur carrière dans le management de projet

Programme

Jour 1

- Introduction à ISO 21502 et au management de projet

Jour 2

- Pratiques pour le management intégré de projet

Jour 3

- Pratiques du management d'un projet

Jour 4

- Pratiques de management d'un projet

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB ISO 31000 Foundation

Objectifs

- Résumer les principaux concepts et principes du management du risque tels qu'ils sont définis dans la norme ISO 31000.
- Expliquer les lignes directrices d'ISO 31000 pour l'établissement du cadre de management du risque
- Décrire l'application du processus de management du risque conformément aux lignes directrices d'ISO 31000

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Professionnels du management du risque
- Les personnes souhaitant acquérir des connaissances sur les lignes directrices ISO 31000 relatives aux principes, au cadre et au processus de management du risque
- Personnes responsables de la création et de la protection de la valeur au sein d'une organisation
- Personnel chargé du management du risque et des opportunités dans son domaine de responsabilité
- Les personnes intéressées par une carrière de manager

Programme

Jour 1

- Introduction à la gestion des risques, aux composantes de la norme ISO 31000 et initiation au processus de gestion des risques

Jour 2

- L'évaluation des risques, le traitement du risque, enregistrement et élaboration de rapports, suivi et revue, communication et consultation selon la norme ISO 31000
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO 31000 Risk Manager

Objectifs

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

Prérequis de la Formation

- Des connaissances fondamentales de la normes ISO 31000 et des connaissances approfondies sur le management du risque.

Audience Ciblée

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

Programme

Jour 1

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

Jour 2

- Processus de management du risque conforme à la norme ISO 31000

Jour 3

- Techniques d'appréciation du risque conformes à la norme ISO/IEC 31010 et examen de certification

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RISK MANAGEMENT

PECB

PECB CERTIFIED ISO 31000 Lead Risk Manager

Objectifs

- Démontrer leur compréhension des principes de management du risque, tels que formulés dans ISO 31000
- Établir, maintenir et améliorer continuellement un cadre de management du risque, conformément aux lignes directrices d'ISO 31000
- Appliquer le processus de management du risque, conformément aux lignes directrices d'ISO 31000
- Planifier les processus d'enregistrement et d'élaboration des rapports sur les risques, ainsi que les activités de communication sur les risques
- Surveiller, passer en revue et améliorer le cadre et le processus de management du risque en fonction des résultats des activités de management du risque

Prérequis de la Formation

- Avoir une bonne compréhension de la norme ISO 31000:2018 et de disposer de compétences avancées dans la gestion du risque.

Audience Ciblée

- Responsables ou consultants désirant maîtriser les compétences pour accompagner un organisme pendant la mise en œuvre d'un cadre organisationnel et d'un processus de management du risque conforme à la norme ISO 31000
- Professionnels responsables de la création et de la préservation de la valeur dans les organismes grâce au management efficace des risques
- Conseillers spécialisés désirant acquérir des connaissances approfondies liées aux principaux concepts, processus et stratégies de management du risque
- Membres d'une équipe chargée du management du risque

Programme

Jour 1

- Introduction à la norme ISO 31000 et aux processus de management du risque

Jour 2

- Établissement du contexte, appréciation et traitement du risque selon la norme ISO 31000

Jour 3

- Acceptation, communication et concertation, enregistrement et rapports, surveillance et revue du risque selon la norme ISO 31000

Jour 4

- Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RISK MANAGEMENT

ISACA CERTIFIED in Risk and Information System Control

Objectifs

- La désignation CRISC ne certifiera pas seulement les professionnels possédant des connaissances et une expérience dans l'identification et l'évaluation des risques spécifiques à une entité, mais elle les aidera également à assister les entreprises dans l'accomplissement de leurs objectifs commerciaux en concevant, mettant en œuvre, surveillant et maintenant des contrôles de sécurité de l'information efficaces et efficients, basés sur les risques.

Prérequis de la Formation

- Pour obtenir la certification CRISC, un minimum de trois ans d'expérience professionnelle cumulative est requis, au cours desquelles vous avez effectué les tâches d'un professionnel CRISC dans au moins deux des quatre domaines CRISC. Parmi ces deux domaines requis, l'un doit être soit le Domaine 1, soit le Domaine 2.

Audience Ciblée

- Professionnels de la gestion des risques informatiques ayant au moins 3 ans d'expérience professionnelle pertinente en matière de risques informatiques et de contrôle des systèmes d'information, y compris :
- Responsables informatiques
- Analystes de risques informatiques
- Consultants en informatique
- Responsables consultatifs en risques/sécurité informatique
- Responsables de la conformité informatique
- Spécialistes de l'évaluation des risques informatiques

Programme

Domain 1

- Gouvernance

Domain 2

- Évaluation des risques

Domain 3

- Réponse et Rapport sur les Risques

Domain 4

- Technologies de l'information et Sécurité

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

Risk Manager – Méthode EBIOS

Objectifs

- Comprendre les concepts et les principes relatifs à la gestion des risques de la méthode EBIOS
- Maîtriser les étapes de la méthode EBIOS pour la réalisation complète d'une étude
- Gérer les risques de sécurité de l'information en utilisant la méthode EBIOS
- Analyser et communiquer les résultats d'une étude EBIOS.

Prérequis de la Formation

- Connaître le guide sécurité de l'ANSSI,
- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes sur la sécurité des systèmes d'information.

Audience Ciblée

- Consultants,
- Responsables sécurité des SI,
- Gestionnaires des risques, toute personne impliquée dans des activités d'appréciation des risques informatique.

Programme

Jour 1

- Introduction à la méthode EBIOS Risk Manager

Jour 2

- Scénarios stratégiques, opérationnels et traitement

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

PECB CERTIFIED ISO/IEC 27701 Lead Implementer

Objectifs

- Expliquer les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS
- Comprendre la corrélation entre les normes ISO/IEC 27701, ISO/IEC 27001 ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le fonctionnement d'un PIMS basé sur la norme ISO/IEC 27701 et ses principaux processus.
- Apprendre à interpréter et à mettre en œuvre les exigences de la norme ISO/EC 27701 dans le contexte spécifique d'un organisme
- Développer l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, contrôler et maintenir efficacement un PIMS

Prérequis de la Formation

- Une compréhension fondamentale en matière de management de la protection de la vie privée et une connaissance approfondie des principes de mise en œuvre du PIMS.

Audience Ciblée

- Responsables et consultants impliqués dans la gestion de la vie privée et des données
- Conseillers experts cherchant à maîtriser la mise en place d'un système de management de la protection de la vie privée
- Personnes responsables des données à caractère personnel (DCP) au sein des organismes
- Personnes chargées de veiller au respect des exigences des régimes de protection de la vie privée
- Membres de l'équipe PIMS

Programme

Jour 1

- Introduction à l'ISO/IEC 27701 et initiation au PIMS

Jour 2

- Planification de la mise en œuvre d'un PIMS

Jour 3

- Mise en œuvre d'un PIMS

Jour 4

- Suivi, amélioration continue et préparation à l'audit de certification du PIMS

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

PECB CERTIFIED ISO/IEC 27701 Lead Auditor

Objectifs

- Comprendre un système de management de la protection de la vie privée (PIMS) et ses processus basés sur ISO/IEC 27701
- Identifier la relation entre ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et les autres normes et cadres réglementaires
- Comprendre le rôle de l'auditeur dans la planification, la direction et le suivi d'un audit de système de management selon ISO 19011
- Apprendre à interpréter les exigences de la norme ISO/IEC 27701 dans le contexte d'un audit du PIMS

Prérequis de la Formation

- Une compréhension fondamentale de la sécurité de l'information et de la protection de la vie privée, ainsi qu'une connaissance approfondie des principes d'audit.

Audience Ciblée

- Auditeurs cherchant à réaliser et à diriger des audits de certification du système de management de la protection de la vie privée (PIMS)
- Gestionnaires ou consultants souhaitant maîtriser un processus d'audit du PIMS
- Personnes responsables du maintien de la conformité aux exigences du PIMS
- Experts techniques souhaitant se préparer à un audit du PIMS.
- Experts-conseils en matière de protection des informations d'identification personnelle (IIP)

Programme

Jour 1

- Introduction au système de management de la protection de la vie privée (PIMS) et à la norme ISO/IEC 27701

Jour 2

- Principes d'audit, préparation et ouverture d'un audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

PECB GDPR CERTIFIED Data Protection Officer

Objectifs

- Comprendre les concepts du RGPD et interpréter ses exigences
- Comprendre le contenu et la corrélation entre le Règlement général sur la protection des données et d'autres cadres réglementaires et normes applicables, telles qu'ISO/IEC 27 701 et ISO/IEC 29 134
- Acquérir la compétence nécessaire pour remplir le rôle et les tâches quotidiennes du délégué à la protection des données au sein d'un organisme
- Développer la capacité à informer, conseiller et surveiller la conformité au RGPD et à coopérer avec l'autorité de surveillance

Prérequis de la Formation

- Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données.

Audience Ciblée

- Gestionnaires ou consultants souhaitant préparer et soutenir un organisme dans la planification, la mise en œuvre et le maintien d'un programme de conformité basé sur le RGPD
- DPO et personnes responsables du maintien de la conformité aux exigences du RGPD
- Membres d'une équipe de sécurité de l'information, de gestion des incidents et de continuité d'activité
- Experts techniques et experts de la conformité envisageant un poste de délégué à la protection des données
- Conseillers experts en sécurité des données à caractère personnel

Programme

Jour 1

- Introduction au RGPD et mise en œuvre de la conformité au RGPD

Jour 2

- Désignation du DPO et analyse du programme de conformité au RGPD

Jour 3

- Responsabilités opérationnelles du DPP

Jour 4

- Suivi et amélioration continue de la conformité au RGPD

Jour 5

- Toolkit RGPD (Pratique et analyse) et Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

ISACA CERTIFIED Data Privacy Solutions Engineer

Objectifs

- Dans ce cours d'ingénieur en solutions de protection des données personnelles, les participants apprendront comment créer des solutions protégeant la vie privée et seront responsables des stratégies de protection des renseignements personnels de leur entreprise pour soutenir sa croissance sans entrave.
- Les participants acquerront l'ensemble des compétences techniques requises de conceptions avancées en matière de protection de la vie privée afin de développer une compréhension commune des meilleures pratiques dans toute votre organisation. Les participants apprendront également à mettre en œuvre l'évaluation de l'impact sur la vie privée (PIA), les stratégies contre les menaces, les attaques et les vulnérabilités liées à la confidentialité – y compris le cryptage, le hachage et la désidentification, l'inventaire des données et la classification (par exemple, marquage, suivi, SOR).

Prérequis de la Formation

- Vous devez avoir un minimum de 3 années d'expérience cumulée à accomplir les tâches d'un professionnel CDPSE. L'expérience professionnelle pour la certification CDPSE doit être acquise dans les 10 années précédant la date de demande de certification. Les candidats ont 5 ans à compter de la date de réussite pour faire leur demande.

Audience Ciblée

- Professionnels de l'informatique qui mettent en œuvre la première ligne de défense contre les violations de données et fournissent des solutions techniques de protection de la vie privée, notamment :
- Ingénieur logiciel principal – Protection des données et des systèmes
- Architecte de domaine (Conformité aux soins juridiques, confidentialité)
- Ingénieur en sécurité et confidentialité
- Architecte de solutions de confidentialité
- Chef de projet informatique
- Data scientist spécialisé en confidentialité
- Analyste de confidentialité
- Responsable de la confidentialité principal

Programme

Domain 1

- Gouvernance de la confidentialité

Domain 2

- Architecture de la confidentialité

Domain 3

- Cycle de vie des données

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ISACA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CDPSE

QUALITÉ MANAGEMENT

QUALITÉ MANAGEMENT

PECB CERTIFIED ISO 9001 Foundation

Objectifs

- Décrire les concepts, principes et définitions du management qualité
- Expliquer les principales exigences de la norme ISO 9001 relatives à un système de management de la qualité
- Identifier les éventuelles actions et approches que les organisations peuvent utiliser pour se conformer à la norme ISO 9001

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Responsables et consultants souhaitant acquérir des connaissances sur les concepts fondamentaux du management de la qualité
- Professionnels souhaitant se familiariser avec les exigences de la norme ISO 9001 relatives à un SMQ
- Personnel responsable du maintien et de l'amélioration de la qualité des produits et services de son organisation
- Personnes souhaitant faire carrière dans le management de la qualité

Programme

Jour 1

- Introduction à la norme ISO/CEI 27002 et au Système de management de la sécurité de l'information.

Jour 2

- Lancement de la phase de reconnaissance.
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

QUALITÉ MANAGEMENT

PECB CERTIFIED ISO 9001 Lead Implementer

Objectifs

- Comprendre la corrélation entre la norme ISO 9001 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMQ
- Savoir interpréter les exigences de la norme ISO 9001 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 SMQ
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la qualité

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 9001 et des connaissances approfondies des principes de mise en œuvre.

Audience Ciblée

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

Programme

Jour 1

- Introduction à la norme ISO 9001 et initialisation d'un SMQ

Jour 2

- Planification de la mise en œuvre d'un SMQ

Jour 3

- Mise en œuvre d'un SMQ

Jour 4

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

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

QUALITÉ MANAGEMENT

PECB

PECB CERTIFIED ISO 9001 Lead Auditor

Objectifs

- Comprendre le fonctionnement d'un Système de management de la qualité (SMQ) conforme à la norme ISO 9001
- Expliquer la corrélation entre la norme ISO 9001 et la norme ISO 9004, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO 9001 dans le contexte d'un audit du SMQ
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 9001 et des connaissances approfondies sur les principes de l'audit.

Audience Ciblée

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

Programme

Jour 1

- Introduction au Système de management de la qualité et à la norme ISO 9001

Jour 2

- Principes, préparation et déclenchement de l'audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INFORMATIQUE JUDICIAIRE

INFORMATIQUE JUDICIAIRE

PECB CERTIFIED Computer Forensics Foundation

Objectifs

- Comprendre les concepts fondamentaux relatifs à l'investigation judiciaire
- Comprendre les processus fondamentaux relatifs à l'investigation judiciaire
- Comprendre les approches, les méthodes et les techniques permettant de gérer efficacement les processus d'investigation judiciaire

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Aux individus intéressés par les processus de l'investigation judicaire
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus de l'investigation judicaire
- Personnes souhaitant poursuivre une carrière dans l'investigation judicaire

Programme

Jour 1

- Introduction aux processus d'investigation judiciaire

Jour 2

- Processus d'investigation judiciaire
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INFORMATIQUE JUDICIAIRE

PECB CERTIFIED PECB Certified Lead Computer Forensics Examiner

Objectifs

- Comprendre les rôles et les responsabilités d'un Lead Computer Forensics Examiner au cours de l'enquête judiciaire informatique
- Comprendre le but de l'examen des médias électroniques et sa relation avec les normes et méthodologies communes
- Comprendre la séquence correcte des étapes d'une enquête sur un incident informatique et d'une opération d'investigation légale numérique
- Comprendre les outils communs et les outils libres qui peuvent être utilisés lors d'une enquête d'incident et d'une opération judiciaire numérique
- Acquérir les compétences nécessaires pour planifier et exécuter une opération informatique judiciaire, mettre en œuvre et maintenir un réseau de sécurité pour protéger les preuves

Prérequis de la Formation

La formation PECB Certified Lead Computer Forensics Examiner nécessite des connaissances de base en informatique (systèmes, réseaux, fichiers), une familiarité avec la cybersécurité, et idéalement une expérience en informatique légale ou sécurité de l'information. Bien que non obligatoires, ces compétences sont fortement recommandées pour suivre efficacement la formation et réussir l'examen. La compréhension de l'anglais technique peut également être utile.

Audience Ciblée

- Spécialistes en informatique judiciaire
- Consultants en informatique judiciaire
- Professionnels de cybersécurité
- Analystes de Cyber intelligence
- Analystes de données électroniques.
- Spécialistes en récupération des preuves informatiques
- Professionnels qui travaillent ou qui s'intéressent à l'application de la loi
- Professionnels souhaitant approfondir leurs connaissances en analyse des investigations informatiques
- Membres de l'équipe chargée de la sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Personnes responsables de l'examen des médias pour en extraire et divulguer des données
- Spécialistes des TI

Programme

Jour 1

- Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique

Jour 2

- Préparer et diriger une enquête informatique judiciaire

Jour 3

- Analyse et gestion des artefacts numériques

Jour 4

- Présentation du cas et jeux de simulation

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

DURABILITÉ

PECB

PECB CERTIFIED ISO/IEC 14001 Foundation

Objectifs

- Comprendre les éléments et le fonctionnement d'un Système de management environnemental et ses principaux processus
- Connaître la corrélation entre la norme ISO 14001 et les autres normes et cadres règlementaires
- Comprendre les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management environnemental

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation

Audience Ciblée

- Toute personne impliquée dans le management environnemental
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management environnemental
- Personnes souhaitant poursuivre une carrière dans le management environnemental

Programme

Jour 1

- Introduction aux concepts du Système de management environnemental, tels que définis par l'ISO 14001

Jour 2

- Exigences relatives au Système de management environnemental
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/IEC 14001 Lead Implementer

Objectifs

- Comprendre la corrélation entre la norme ISO 14001 et la norme ISO 14040, 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 SME
- Savoir interpréter les exigences de la norme ISO 14001 dans un contexte spécifique de l'organisme
- Savoir soutenir un organisme dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SME
- Acquérir l'expertise nécessaire pour conseiller un organisme sur la mise en œuvre des meilleures pratiques relatives au Système de management environnemental

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre

Audience Ciblée

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

Programme

Jour 1

- Introduction à la norme ISO 14001 et initialisation d'un SME

Jour 2

- Planification de la mise en œuvre d'un SME

Jour 3

- Mise en œuvre d'un SME

Jour 4

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

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/IEC 14001 Lead Auditor

Objectifs

- Comprendre le fonctionnement d'un Système de management environnemental (SME) conforme à la norme ISO 14001
- Expliquer la corrélation entre la norme ISO 14001 et la norme ISO 14040, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO 14001 dans le contexte d'un audit du SME
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de l'audit

Audience Ciblée

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

Programme

Jour 1

- Introduction au Système de management environnemental et à la norme ISO 14001

Jour 2

- Principes, préparation et déclenchement de l'audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/IEC 50001 Foundation

Objectifs

- Comprendre les éléments et le fonctionnement d'un Système de management de l'énergie et ses principaux processus
- Comprendre la corrélation entre la norme ISO 50001 et les autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en oeuvre et de gérer un Système de management de l'énergie

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne impliquée dans le management de l'énergie
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de l'énergie
- Personnes souhaitant poursuivre une carrière dans le management de l'énergie

Programme

Jour 1

- Introduction aux concepts du Système de management de l'énergie, tels que définis par l'ISO 50001

Jour 2

- Exigences relatives au Système de management de l'énergie
- Examen de certification.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/IEC 50001 Lead Implementer

Objectifs

- Comprendre la corrélation entre la norme ISO 50001 et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMÉ
- Savoir interpréter les exigences de la norme ISO 50001 dans un contexte spécifique de l'organisme
- Savoir accompagner un organisme dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMÉ
- Acquérir l'expertise nécessaire pour conseiller un organisme sur la mise en œuvre des meilleures pratiques relatives au Système de management de l'énergie

Prérequis de la Formation

- Une bonne connaissance préalable de la norme ISO 50001 et des connaissances approfondies des principes de mise en œuvre sont nécessaires.

Audience Ciblée

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

Programme

Jour 1

- Introduction à la norme ISO 50001 et initialisation d'un SMÉ

Jour 2

- Planification de la mise en œuvre d'un SMÉ

Jour 3

- Mise en œuvre d'un SMÉ

Jour 4

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

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/IEC 50001 Lead Auditor

Objectifs

- Comprendre le fonctionnement d'un Système de management de l'énergie (SMÉ) conforme à la norme ISO 50001
- Expliquer la corrélation entre la norme ISO 50001 et les autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO 50001 dans le contexte d'un audit du SMÉ
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 50001 et des connaissances approfondies sur les principes de l'audit.

Audience Ciblée

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

Programme

Jour 1

- Introduction au Système de management de l'énergie et à la norme ISO 50001

Jour 2

- Principes, préparation et déclenchement de l'audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO/CEI 26000 Foundation

Objectifs

- Understand the principles of Social Responsibility
- Learn how to integrate social responsibility behaviour within your organization
- Understand the approaches, methods and techniques used by organizations to contribute to sustainable development

Prérequis de la Formation

- The PECB Certified ISO 26000 Foundation training course does not require prior expertise in social responsibility or related standards, making it accessible to professionals from various backgrounds. However, it is recommended that participants have a general understanding of organizational practices and a basic interest in sustainability, ethics, and corporate social responsibility to better benefit from the course

Audience Ciblée

- Individuals concerned with and committed to Social Responsibility
- Individuals seeking to gain knowledge about Social Responsibility Programs (SRP)
- Individuals interested in Social Responsibility

Programme

Jour 1

- Introduction to Social Responsibility Program (SRP) concepts as specified in ISO 26000

Jour 2

- Social Responsibility Programs
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO 26000 Lead Manager

Objectifs

- Explain the fundamental concepts of and principles for social responsibility based on ISO 26000
- Comprehend and identify the social responsibility core subjects and issues within an organization
- Apply practices on integrating social responsibility in an organization
- Review, assess, and continually improve social responsibility within an organization

Prérequis de la Formation

- The PECB Certified ISO 26000 Lead Manager course has no strict prerequisites, but prior knowledge of ISO 26000 or experience in social responsibility and sustainability is recommended. This helps participants better apply and manage social responsibility initiatives effectively.

Audience Ciblée

- Managers or consultants involved in or concerned with social responsibility efforts
- Project managers, consultants, and expert advisors seeking to learn more about social responsibility and sustainable development
- Individuals responsible for ensuring that the organization adheres to relevant laws and regulations related to social responsibility
- Individuals responsible for integrating and promoting social responsibility behavior within an organization

Programme

Jour 1

- Introduction to ISO 26000 and social responsibility

Jour 2

- Social Responsibility core subjects

Jour 3

- Social responsibility core subjects (cont'd) and integrating practices for social responsibility

Jour 4

- Improving social responsibility performance

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SANTÉ ET SÉCURITÉ

PECB CERTIFIED ISO/IEC 45001 Foundation

Objectifs

- Comprendre les concepts, définitions et approches de base en matière de santé et de sécurité au travail
- Se familiariser avec les exigences de la norme ISO 45001 relatives à un système de management de la santé et de la sécurité au travail
- Développer une compréhension générale de la façon dont les exigences de la norme ISO 45001 pourraient être appliquées dans un organisme

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation

Audience Ciblée

- Managers/consultants cherchant à se familiariser avec les concepts de base de la santé et de la sécurité au travail
- Personnes souhaitant créer des lieux de travail plus sûrs et plus sains au sein de leur organisation
- Personnes souhaitant se familiariser avec les principales exigences de la norme ISO 45001 pour un système de management de la santé et de la sécurité au travail
- Personnes souhaitant poursuivre une carrière en santé et sécurité au travail

Programme

Jour 1

- Introduction au management de la santé et de la sécurité au travail, au SMSST et aux articles 4 à 6 d'ISO 45001

Jour 2

- Articles 7 à 10 de la norme ISO 45001
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB

PECB CERTIFIED ISO 45001 Lead Implementer

Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de la santé et de la sécurité au travail (SMSST) conformément à la norme ISO 45001
- Interpréter les exigences de la norme ISO 45001 pour un SMSST du point de vue d'un auditeur
- Initier et planifier la mise en œuvre d'un SMSST conformément à la norme ISO 45001, en utilisant la méthodologie IMS2 de PECB et d'autres meilleures pratiques
- Accompagner une organisation dans le fonctionnement, le maintien et l'amélioration continue d'un SMSST conformément à la norme ISO 45001
- Préparer une organisation à se soumettre à un audit de certification par un tiers

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre

Audience Ciblée

- Personnes chargées du maintien et de l'amélioration de la sécurité sur le lieu de travail
- Agents, consultants et conseillers en matière de santé et de sécurité au travail
- Professionnels souhaitant se familiariser avec la méthodologie IMS2 de PECB pour la mise en œuvre d'un SMSST
- Personnes chargées de maintenir la conformité du SMSST aux exigences de la norme ISO 45001
- Membres des équipes de santé et sécurité au travail
- Personnes aspirant faire carrière en tant que responsables de la mise en œuvre d'un SMSST, consultants ou agents

Programme

Jour 1

- Introduction à la norme ISO 45001 et lancement de la mise en œuvre d'un SMSST

Jour 2

- Plan de mise en œuvre d'un SMSST

Jour 3

- Mise en œuvre d'un SMSST

Jour 4

- Évaluation des performances du SMSST, amélioration continue et préparation à l'audit de certification

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO 45001 Lead Auditor

Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management de la santé et de la sécurité au travail (SMSST) conformément à la norme ISO 45001
- Interpréter les exigences de la norme ISO 45001 pour un SMSST du point de vue d'un auditeur
- Évaluer la conformité du SMSST aux exigences de la norme ISO 45001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à la norme ISO 45001, conformément aux exigences de la norme ISO/ IEC 17021-1, aux lignes directrices de la norme ISO 19011 et aux autres meilleures pratiques d'audit
- Gérer un programme d'audit conformément à la norme ISO 45001

Prérequis de la Formation

- Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de l'audit

Audience Ciblée

- Auditeurs intéressés par la réalisation et la direction d'audits de certification de SMSST
- Responsables ou consultants désireux d'approfondir leurs connaissances du processus d'audit de SMSST
- Auditeurs internes et personnes responsables du maintien de la conformité aux exigences de la norme ISO 45001
- Experts techniques souhaitant se préparer à un audit de SMSST
- Conseillers experts en management de la santé et de la sécurité au travail

Programme

Jour 1

- Introduction au SMSST et à la norme ISO 45001

Jour 2

- Principes d'audit, préparation et lancement d'un audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

TRANSFORMATION NUMÉRIQUE

TRANSFORMATION NUMÉRIQUE

PECB

PECB CERTIFIED Digital Transformation Officer

Objectifs

- Expliquer les concepts fondamentaux de la transformation numérique et des technologies de transformation numérique, y compris l'intelligence artificielle. l'intelligence artificielle, l'informatique en nuage, le big data, l'apprentissage automatique, l'IdO et la blockchain
- Adopter les approches et les méthodologies utilisées pour la mise en œuvre des stratégies de transformation numérique dans une organisation.
- Soutenir une organisation dans la conception, la mise en œuvre, le suivi et l'amélioration efficaces d'une stratégie de transformation numérique.
- Contrôler et mesurer les résultats de la stratégie de transformation numérique.
- Expliquer et appliquer les approches et les techniques utilisées pour établir une culture numérique et communiquer la stratégie de transformation numérique

Prérequis de la Formation

- Les principales exigences pour participer à cette formation sont d'avoir une compréhension fondamentale des concepts des technologies de l'information et une connaissance générale de la transformation numérique

Audience Ciblée

- Les managers et les dirigeants qui cherchent à prospérer dans l'économie numérique
- Les personnes chargées de transformer les opérations de l'organisation grâce aux technologies numériques
- Les professionnels de l'informatique ou les consultants qui cherchent à améliorer leurs connaissances en matière de conception et de stratégie numériques afin de soutenir les initiatives de transformation numérique de l'organisation les initiatives de transformation numérique de l'organisation
- Les cadres supérieurs des secteurs du numérique, de l'information, du marketing et de l'informatique qui cherchent à comprendre comment les technologies numériques peuvent être utilisées pour transformer les processus des entreprises.

Programme

Jour 1

- Introduction à la transformation numérique

Jour 2

- Technologies, approches et méthodologies de la transformation numérique et planification de la stratégie de transformation numérique

Jour 3

- Gestion des risques liés à la transformation numérique et mise en œuvre de la stratégie de transformation numérique

Jour 4

- Communication et suivi de la stratégie de transformation numérique

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

INTELLIGENCE ARTIFICIELLE

PECB

PECB CERTIFIED ISO/IEC 42001 Foundation

Objectifs

- Expliquer les concepts et principes de la gestion de l'intelligence artificielle
- Décrire les principales exigences de la norme ISO/IEC 42001 pour un système de management de l'intelligence artificielle (SMIA)
- Identifier des approches, méthodes et techniques utilisées pour mettre en œuvre, gérer et améliorer un SMIA

Prérequis de la Formation

- Il n'y a pas de prérequis pour s'inscrire à cette formation.

Audience Ciblée

- Professionnels désireux d'avoir une compréhension fondamentale des exigences de la norme ISO/IEC 42001
- Managers et consultants désireux d'en savoir plus sur la gestion de l'intelligence artificielle
- Personnes impliquées dans la gestion ou la mise en œuvre de systèmes d'IA
- Personnes chargées de la supervision des projets liés à l'IA

Programme

Jour 1

- Introduction au système de management de l'intelligence artificielle (SMIA) et à ISO/IEC 42001

Jour 2

- Système de management de l'intelligence artificielle (SMIA)
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

PECB

PECB CERTIFIED ISO/IEC 42001 Lead Implementer

Objectifs

- Expliquer les concepts et principes fondamentaux d'un SMIA conformément à la norme ISO/IEC 42001
- Interpréter les exigences de la norme ISO/IEC 42001 applicables à un SMIA du point de vue d'un Implementer (responsable de la mise en œuvre)
- Lancer et planifier la mise en œuvre d'un SMIA conformément à la norme ISO/IEC 42001 en utilisant la méthodologie IMS2 de PECB et d'autres meilleures pratiques
- Soutenir une organisation dans l'exploitation, la maintenance et l'amélioration continue d'un SMIA conformément à la norme ISO/IEC 42001
- Préparer une organisation à faire l'objet d'un audit de certification effectué par une tierce partie

Prérequis de la Formation

- Avoir des connaissances de base sur la norme ISO 42001 et sur le fonctionnement de l'intelligence artificielle.
- Savoir lire et comprendre l'anglais pour pouvoir consulter le support de cours et passer l'examen de certification.

Audience Ciblée

- Professionnels chargés de superviser et de gérer les projets d'IA
- Consultants des stratégies de mise en œuvre de l'IA
- Conseillers experts et spécialistes désirant maîtriser la mise en œuvre pratique d'un SMIA conformément à la norme ISO/IEC 42001
- Personnes chargées de veiller à ce que les projets d'IA soient conformes aux exigences en la matière au sein d'une organisation
- Membres des équipes de mise en œuvre d'un SMIA participant à la mise en œuvre des systèmes d'IA
- Cadres et dirigeants souhaitant prendre des décisions éclairées concernant la mise en œuvre de l'IA et sa conformité à la norme ISO/IEC 42001

Programme

Jour 1

- Introduction à l'ISO/IEC 42001 et au lancement de la mise en œuvre d'un SMIA

Jour 2

- Planification de la mise en œuvre d'un SMIA

Jour 3

- Mise en œuvre d'un SMIA

Jour 4

- Suivi d'un SMIA, amélioration continue et préparation de l'audit de certification

Jour 5

- Examen de certification

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

PECB

PECB CERTIFIED ISO/IEC 42001 Lead Auditor

Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management de la santé et de la sécurité au travail (SMSST) conformément à la norme ISO 45001
- Interpréter les exigences de la norme ISO 45001 pour un SMSST du point de vue d'un auditeur
- Évaluer la conformité du SMSST aux exigences de la norme ISO 45001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à la norme ISO 45001, conformément aux exigences de la norme ISO/ IEC 17021-1, aux lignes directrices de la norme ISO 19011 et aux autres meilleures pratiques d'audit
- Gérer un programme d'audit conformément à la norme ISO 45001

Prérequis de la Formation

- Avoir des connaissances de base sur la norme ISO 42001 et sur le fonctionnement de l'intelligence artificielle
- Savoir lire et comprendre l'anglais pour pouvoir consulter le support de cours et passer l'examen de certification

Audience Ciblée

- Personnes ayant une expérience en matière d'audit, interne ou externe, désirant se spécialiser dans l'audit des systèmes de management de l'IA
- Gestionnaires ou consultants souhaitant maîtriser le processus d'audit des systèmes de management de l'IA
- Personnes responsables du maintien de la conformité aux exigences du système de management de l'IA au sein d'une organisation
- Conseillers experts en management de l'IA
- Professionnels chargés d'analyser et de comprendre les besoins des entreprises pour la mise en œuvre de l'IA
- Personnes impliquées dans le développement et la mise en œuvre de solutions d'IA et dans la conception de l'architecture des systèmes d'IA

Programme

Jour 1

- Introduction au système de management de l'intelligence artificielle et à la norme ISO/IEC 42001

Jour 2

- Principes d'audit, préparation et lancement d'un audit

Jour 3

- Activités d'audit sur place

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

PECB

PECB CERTIFIED Artificial Intelligence Professional

Objectifs

- Explain the foundational principles of AI and its various applications.
- Conduct data analysis and create meaningful visualizations to support AI projects.
- Apply machine learning techniques to real-world problems, including supervised, unsupervised, and reinforcement learning.
- Implement simple neural network and advanced deep learning architectures such as CNNs.
- Understand NLP systems and Computer Vision methodologies.
- Understand robotics and expert systems for AI-driven automation.
- Identify and mitigate AI risks while ensuring compliance with regulations.
- Develop ethical AI strategies aligned with organizational values and societal needs.

Prérequis de la Formation

- A basic understanding of artificial intelligence concepts, data management, and information security is recommended to successfully follow this training course

Audience Ciblée

- AI Professionals actively involved in the development and implementation of AI technologies
- Experienced AI Practitioners seeking to enhance their knowledge, stay updated with the latest trends, and refine their leadership skills
- Data Scientists responsible for developing and optimizing AI models h IT Managers overseeing AI projects and initiatives within their organizations
- AI Enthusiasts who aspire to advance into leadership roles, such as AI project managers or AI strategists
- Risk and Compliance Officers responsible for managing AI-related risks and ensuring compliance with regulations
- Executives, including CIOs, CEOs, and COOs, who play a crucial role in decision-making processes related to AI
- Professionals aiming for executive-level AI roles who need a comprehensive understanding of AI technologies and their applications

Programme

Jour 1

- Foundations of AI and Data Analysis

Jour 2

- Machine Learning

Jour 3

- Deep Learning and Natural Language Processing

Jour 4

- Computer Vision, Robotics, AI Strategy, Governance, and Risk Manager

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

PECB

PECB CERTIFIED Lead AI Risk Manager

Objectifs

- Understand AI risk management fundamentals, including key concepts, approaches, and techniques for identifying, assessing, and mitigating AI-related risks
- Identify, analyze, evaluate, and treat AI risks, such as bias, security vulnerabilities, transparency issues, and ethical concerns
- Develop and implement risk mitigation strategies and incident response measures to address AI-related threats and vulnerabilities
- Apply established AI risk management frameworks, such as the NIST AI Risk Management Framework and the EU AI Act, to ensure governance, compliance, and ethical AI use

Prérequis de la Formation

- A basic understanding of artificial intelligence concepts, risk management principles, and information security is recommended to successfully follow this training course.

Audience Ciblée

- Professionals responsible for identifying, assessing, and managing AI-related risks within their organizations
- IT and security professionals seeking expertise in AI risk management
- Data scientists, data engineers, and AI developers working on AI system design, deployment, and maintenance
- Consultants advising organizations on AI risk management and mitigation strategies
- Legal and ethical advisors specializing in AI regulations, compliance, and societal impacts
- Managers and leaders overseeing AI implementation projects and ensuring responsible AI adoption
- Executives and decision-makers aiming to understand and address AI-related risks at a strategic level

Programme

Jour 1

- Introduction to AI risk management

Jour 2

- Organizational context, AI risk governance, and AI risk identification

Jour 3

- Analysis, evaluation, and treatment of AI risks

Jour 4

- AI risk monitoring and reporting, training and awareness, and optimizing AI risk performance

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

CompTIA AI Essentials

Objectifs

- Learn what defines artificial intelligence from other types of intelligence and computing
- Practice communicating about AI effectively
- Explore AI tools and the ways they can support your organization
- Craft AI prompts
- Navigate the privacy and security concerns AI technology presents
- Prepare for AI's effect on the future of technology

Programme

Lesson 1

- AI Unveiled

Lesson 2

- Generative AI Frontiers

Lesson 3

- Engineering Effective Prompts

Lesson 4

- Balancing Innovation and Privacy

Lesson 5

- Future Trends and Innovations in A

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

CompTIA AI Prompting Essentials

Objectifs

- AI task identification: Decide when and how to use AI for different workplace tasks based on complexity, risk, and desired outcomes.
- Prompt crafting: Learn to write clear, effective prompts for AI chatbots to achieve better, more accurate responses.
- Moving beyond transactional interactions: Improve outcomes by engaging with and refining AI responses to get more targeted, relevant results.
- Ethical AI use: Apply AI ethically and securely, understanding issues around privacy, transparency, and copyright.
- Task automation: Use AI to automate routine and repetitive tasks, freeing up your time for more critical projects.
- Workplace integration: Leverage AI in multi-step projects and common workplace functions to drive collaboration and productivity.

Programme

Lesson 1

- Course Intro

Lesson 2

- Foundations of AI Prompting

Lesson 3

- AI Prompting Basics

Lesson 4

- Advanced AI Prompting Skills

Lesson 5

- Apply AI Skills in Real World Contexts

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

Appréhender le fonctionnement des IA génératives et maîtriser l'art du prompt

Objectifs

- Comprendre le fonctionnement des intelligences artificielles génératives (IAG) et les différentes familles de solutions d'IA existantes.
- Utiliser les principales fonctionnalités des outils d'IAG et formuler des prompts adaptés aux objectifs visés.
- Développer un regard critique sur les résultats produits par l'IA afin d'en évaluer la pertinence, les limites et les biais.

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Toute personne souhaitant apprendre à prompter.

Programme

Jour 1

- Matin : Comprendre les fondamentaux des IA génératives
- Après-midi : Maîtriser l'art du prompt

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

Déjouer les biais de l'IA par la pensée critique

Objectifs

- Identifier les fondements de l'esprit critique.
- Comprendre les biais cognitifs et algorithmiques.
- Adopter une posture critique, éthique et stratégique face à l'Intelligence Artificielle Générative (IAG)

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Toute personne souhaitant renforcer son esprit critique face à l'IA.

Programme

Jour 1

- Matin : Fondements de l'esprit critique et découverte des biais
- Après-midi : Biais algorithmiques et posture critique face à l'IA

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

Les enjeux de l'intelligence Artificielle (IA) pour les dirigeants

Objectifs

- Comprendre les enjeux stratégiques, éthiques et réglementaires de l'intelligence artificielle dans le contexte de l'entreprise.
- Identifier les opportunités et les risques de l'IA pour l'organisation, les métiers et les parties prenantes.
- Outiller les dirigeants pour piloter une démarche responsable d'intégration de l'IA dans leur entreprise.
- Coconstruire les grandes lignes d'une charte d'entreprise sur l'usage de l'IA, adaptée à leur secteur et à leurs valeurs.

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Membres de COMEX,
- CODIR,
- Dirigeants d'entreprises.

Programme

Jour 1

- Matin : Compréhension des enjeux stratégiques de l'IA
- Après-midi : Opportunités, risques et gouvernance de l'IA

Jour 2

- Matin : IA responsable et charte d'entreprise

Informations Pratiques

1,5 JOUR

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

Développeurs : Boostez vos performances grâce à l'IA

Objectifs

- Intégrer des outils d'intelligence artificielle (IA) dans leur workflow de développement
- Automatiser certaines tâches de développement grâce à des assistants IA
- Évaluer les risques liés à l'usage de l'IA générative (IA) dans un contexte de développement sécurisé
- Appliquer des bonnes pratiques de cybersécurité dans l'utilisation d'outils d'IA (données sensibles, confidentialité du code).

Prérequis de la Formation

- Connaissances de base en programmation et conception d'applications.

Audience Ciblée

- Développeurs,
- RSSI
- Toute personne en charge de projets SI.

Programme

Jour 1

- Matin : Introduction et fondamentaux de l'IA pour les développeurs
- Après-midi : Intégrer l'IA dans le workflow de développement

Jour 2

- Matin : Cybersécurité et risques liés à l'IA générative
- Après-midi : Approfondissement et cas pratiques avancés

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INTELLIGENCE ARTIFICIELLE

Accompagner ses équipes dans l'intégration de l'IA

Objectifs

- Comprendre les fondamentaux de l'intelligence artificielle et ses implications pour les entreprises.
- Identifier les opportunités, les limites et les enjeux éthiques, juridiques et organisationnels liés à l'usage de l'IA.
- Adopter une posture de leadership éclairée pour piloter des projets intégrant l'IA, même sans expertise technique.
- Renforcer la confiance numérique en intégrant les questions de sécurité, de confidentialité des données et de détection des manipulations.

Prérequis de la Formation

- Cette formation ne nécessite pas de prérequis.

Audience Ciblée

- Managers,
- Responsables
- Dirigeants.

Programme

Jour 1

- Matin : Comprendre les fondamentaux de l'IA et ses implications
- Après-midi : Opportunités, limites et enjeux de l'IA

Jour 2

- Matin : Leadership et pilotage des projets IA
- Après-midi : Sécurité, confiance et adoption

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

AUDIT

PECB CERTIFIED ISO/CEI 20000 Foundation

Objectifs

- Comprendre les éléments et le fonctionnement d'un Système de management de services des TI et ses principaux processus
- Comprendre la corrélation entre la norme ISO/CEI 20000 et les autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en oeuvre et de gérer un Système de management de services des TI

Prérequis de la Formation

- Aucun prérequis n'est nécessaire pour participer à cette formation.

Audience Ciblée

- Toute personne impliquée dans le management de services des TI
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de services des TI
- Personnes souhaitant poursuivre une carrière dans le management de services des TI

Programme

Jour 1

- Introduction aux concepts du Système de management de services des TI, tels que définis par la norme ISO/CEI 20000

Jour 2

- Exigences relatives au Système de management de services des TI
- Examen de certification

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/CEI 20000 Lead Implementer

Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 20000-1 et la norme ISO/CEI 20000-2, ainsi qu'avec d'autres normes et cadres réglementaires
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en oeuvre et gérer efficacement un SMSTI
- Savoir interpréter les exigences de la norme ISO/CEI 20000-1 dans un contexte spécifique de l'organisme
- Savoir accompagner un organisme dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour d'un SMSTI
- Acquérir l'expertise nécessaire pour conseiller un organisme sur la mise en œuvre des meilleures pratiques relatives au Système de management des services des TI

Prérequis de la Formation

- Les participants doivent avoir des connaissances de base en gestion des services informatiques ainsi qu'une compréhension générale de la norme ISO/IEC 20000.

Audience Ciblée

- Responsables ou consultants impliqués dans le management des services des TI
- Conseillers spécialisés désirant maîtriser la mise en oeuvre d'un Système de Management des services des TI
- Toute personne responsable du maintien de la conformité aux exigences du SMSTI
- Membres d'une équipe du SMSTI

Programme

Jour 1

- Introduction à la norme ISO/CEI 20000 et initialisation d'un SMSTI

Jour 2

- Planification de la mise en œuvre d'un SMSTI

Jour 3

- Mise en œuvre d'un SMSTI

Jour 4

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

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PECB CERTIFIED ISO/CEI 20000 Lead Auditor

Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management des services (SMS) conformément à la norme ISO 20000-1
- Interpréter les exigences de la norme ISO/IEC 20000-1 pour un SMS du point de vue d'un auditeur
- Évaluer la conformité du SMS aux exigences de la norme ISO 20000-1, conformément aux concepts et principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de la norme ISO 20000-1, conformément aux exigences de la norme ISO/IEC 17021-1, aux lignes directrices de la norme ISO 19011 et aux autres meilleures pratiques d'audit
- Gérer un programme d'audit de la norme ISO/IEC 20000-1

Prérequis de la Formation

- Participants should have basic knowledge of IT service management and a general understanding of the ISO/IEC A

Audience Ciblée

- Auditeurs souhaitant réaliser et diriger des audits de SMS
- Managers ou consultants souhaitant maîtriser le processus d'audit du SMS
- Personnes responsables de maintenir la conformité aux exigences de la norme ISO/IEC 20000-1 dans une organisation
- Experts techniques souhaitant préparer les organisations à un audit de SMS
- Conseillers experts en management des services

Programme

Jour 1

- Introduction au SMS et à la famille de normes ISO/IEC 20000

Jour 2

- Principes d'audit et préparation pour le lancement d'un audit

Jour 3

- Activités d'audit sur site

Jour 4

- Clôture de l'audit

Jour 5

- Examen de certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

PECB CERTIFIED ISA/IEC 62443 Lead Implementer

Objectifs

- Explain the fundamental concepts and principles of an industrial automation and control systems (IACS) security program based on the ISA/IEC 62443 series of standards
- Interpret the ISA/IEC 62443 requirements, recommendations, and technical reports from the perspective of an implementer
- Manage threats by implementing security controls, assessing maturity, securing assets and supply chains, and plan patching
- Design and maintain an IACS security program aligned with ISA/IEC 62443, assess and manage risks, and define clear security roles and responsibilities

Provide ongoing security awareness and training, monitor IACS environments for threats, conduct regular security testing, and respond swiftly to incidents

Prérequis de la Formation

- A basic understanding of cybersecurity concepts, industrial control systems (OT), and information security management principles is recommended to successfully follow this training course.

Audience Ciblée

- Managers, engineers, and consultants seeking to develop or enhance their competence in implementing IACS security programs
- Professionals responsible for or involved in IACS security activities who wish to deepen their understanding of the ISA/IEC 62443 series of standards
- Security practitioners and risk managers looking to strengthen their skills in applying industrial cybersecurity controls, assessing maturity, and managing IACS security
- Individuals pursuing a career in IACS cybersecurity who want to learn a comprehensive methodology for designing, implementing, and maintaining security programs aligned with ISA/IEC 62443

Programme

Day 1

- Foundations of ISA/IEC 62443 and IACS security

Day 2

- Security requirements, maturity models, and threat landscape

Day 3

- Establishing and managing an IACS security program

Day 4

- Training, incident response, and sector-specific standards

Day 5

- Certification exam

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Audit sécurité d'applications mobiles Android – Introduction

Objectifs

- Maîtrisez les bases nécessaires pour la réalisation d'audits de sécurité avancés sur les applications Android.

Prérequis de la Formation

- Aucun prérequis nécessaire pour participer à cette formation.

Audience Ciblée

- Consultant en sécurité
- Administrateurs système ou réseau
- Développeurs

Programme

Jour 1

- Tests d'intrusion mobiles, concepts et mise en place, analyse statique

Jour 2

- Analyse réseau, analyse dynamique

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Audit sécurité d'applications mobiles Android – Advanced

Objectifs

- Maîtrisez les dernières techniques d'exploitation pour les applications mobiles Android.

Prérequis de la Formation

- Aucun prérequis nécessaire pour participer à cette formation.

Audience Ciblée

- Consultant en sécurité
- Administrateurs système ou réseau
- Développeurs

Programme

Jour 1

- Analyse statique avancée, analyse réseau avancée, analyse dynamique avancée.

Jour 2

- Signature et reverse d'application, Frida / Objection, Metasploit, Forensic.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Audit sécurité d'applications mobiles iOS

Objectifs

- Obtenez les bases nécessaires pour la réalisation d'audits de sécurité avancés sur les applications iOS.

Prérequis de la Formation

- Aucun prérequis nécessaire pour participer à cette formation.

Audience Ciblée

- Consultant en sécurité
- Administrateurs système ou réseau
- Développeurs

Programme

Jour 1

- Tests d'intrusion mobiles, concepts et mise en place, analyse statique.

Jour 2

- Analyse réseau, analyse dynamique.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Test D'intrusion des Serveurs et des Application Web

Objectifs

- Obtenez les bases nécessaires pour la compréhension des applications Web et des vulnérabilités associées.

Prérequis de la Formation

- Aucun prérequis nécessaire pour participer à cette formation.

Audience Ciblée

- Consultant en sécurité
- Administrateurs système ou réseau
- Développeurs

Programme

Jour 1

- Connaissance des applications web et infrastructure, collecte d'information, contournement d'autorisation, Cross-Site Scripting (XSS).

Jour 2

- Injection, téléchargement non sécurisé, attaques sur les tokens JWT, faille de type CSRF.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Audit Sécurité sur Réseaux Wifi Moderne

Objectifs

- Obtenez les bases nécessaires pour la compréhension des applications Web et des vulnérabilités associées.

Prérequis de la Formation

- Aucun prérequis nécessaire pour participer à cette formation.

Audience Ciblée

- Consultant en sécurité
- Administrateurs système ou réseau

Programme

Jour 1

- Connaissance des réseaux Wi-Fi, Identification des réseaux, WPS.

Jour 2

- La sécurité des réseaux Wi-Fi (Filtrage MAC / WEP / WPA{1/2/3}), WPA Entreprise.

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

Maîtriser l'analyse des journaux systèmes avec Splunk : Visualisation, Corrélation et Surveillance Active

Objectifs

- Obtenez les bases nécessaires pour la réalisation d'audits de sécurité avancés sur les applications iOS.

Prérequis de la Formation

- Connaissances de base des systèmes (Windows/Linux) et des réseaux.
- Expérience en exploitation ou supervision IT (niveau intermédiaire).

Audience Ciblée

- Administrateurs systèmes, ingénieurs réseaux, analystes sécurité.
- Toute personne impliquée dans la surveillance ou l'exploitation des infrastructures IT.
- Techniciens souhaitant monter en compétence sur un outil SIEM accessible et puissant.

Programme

Jour 1

- Fondamentaux et premières analyses

Jour 2

- Visualisation, corrélation, alertes

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Préparation Offensive Security Certified Professional (OSCP)

Objectifs

- Maîtriser les méthodologies et techniques de tests d'intrusion en environnement réel.
- Utiliser efficacement les outils de Kali Linux pour identifier et exploiter des vulnérabilités.

Découvrez tous les détails de cette formation en ligne.

Prérequis de la Formation

- Connaissances de base en réseaux et systèmes d'exploitation (Windows et Linux).
- Familiarité avec la ligne de commande et les scripts.
- Compréhension des concepts fondamentaux de la cybersécurité.
- Aucune certification préalable requise, mais une expérience en IT est recommandée.

Audience Ciblée

- Professionnels de la cybersécurité souhaitant acquérir des compétences pratiques en tests d'intrusion.
- Administrateurs systèmes et réseaux désireux de comprendre les techniques d'attaque.
- Développeurs souhaitant renforcer la sécurité de leurs applications.
- Toute personne aspirant à une carrière en sécurité offensive.

Programme

Module 1
- Introduction à la cybersécurité

Module 2
- Stratégies d'apprentissage efficaces

Module 3
- Rédaction de rapports pour les testeurs d'intrusion

Module 4
- Collecte d'informations

Module 5
- Analyse de vulnérabilités

Module 6
- Attaques sur applications web

Module 7
- Injection SQL

Module 8
- Attaques côté client

Module 9
- Utilisation d'exploits publics

Module 10
- Évasion des antivirus

Module 11
- Attaques par mot de passe

Module 12
- Élévation de privilèges Windows

Module 13
- Élévation de privilèges Linux

Module 14
- Redirection de ports et tunneling SSH

Module 15
- Framework Metasploit

Module 16
- Active Directory

Module 17
- Laboratoires de challenge

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Préparation Offensive Security Exploit Developer (OSED)

Objectifs

- Maîtriser le développement d'exploits Windows en mode utilisateur sur architecture x86.
- Contourner les mécanismes de sécurité modernes tels que DEP et ASLR.
- Développer des chaînes ROP personnalisées et écrire du shellcode sur mesure.
- Appliquer des techniques avancées de reverse engineering pour identifier des vulnérabilités.
- Préparer et réussir l'examen de certification OSED.

Prérequis de la Formation

- Familiarité avec les débogueurs tels que WinDbg, ImmunityDBG ou OllyDBG.
- Connaissances de base en exploitation sur architecture 32 bits.
- Compétences en programmation, notamment en Python 3.

Audience Ciblée

- Professionnels de la cybersécurité souhaitant approfondir leurs compétences en développement d'exploits.
- Pentesters expérimentés désirant se spécialiser dans l'exploitation de vulnérabilités binaires.
- Chercheurs en sécurité et analystes de logiciels malveillants.
- Développeurs souhaitant comprendre les techniques d'exploitation pour renforcer la sécurité de leurs applications.

Programme

- Introduction à WinDbg
- Débordements de tampon (Stack Buffer Overflows)
- Exploitation des SEH Overflows
- Introduction à IDA Pro (version gratuite)
- Contournement des restrictions d'espace : Egghunters
- Création de shellcode personnalisé
- Reverse engineering de bugs
- Bypass des protections DEP/ASLR avec des chaînes ROP
- Attaques de type format string

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Préparation Offensive Security Web Expert (OSWE)

Objectifs

- Maîtriser les techniques avancées d'audit de sécurité des applications web en environnement « white-box ».
- Identifier et exploiter des vulnérabilités complexes via l'analyse de code source.
- Développer des scripts d'exploitation personnalisés pour des applications web.
- Préparer et réussir l'examen de certification OSWE.

Prérequis de la Formation

- Confort dans la lecture et l'écriture d'au moins un langage de programmation (PHP, Java, C#, JavaScript).
- Familiarité avec Linux.
- Capacité à écrire des scripts simples en Python, Perl, PHP ou Bash.
- Expérience avec des proxys web (ex. Burp Suite).
- Compréhension générale des vecteurs d'attaque des applications web.

Audience Ciblée

- Testeurs d'intrusion expérimentés souhaitant approfondir l'audit de sécurité des applications web.
- Spécialistes en sécurité des applications web.
- Développeurs web souhaitant renforcer leurs compétences en sécurité

Programme

- Introduction et méthodologie
- Outils et méthodologies
- Études de cas pratiques

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU INTERMÉDIAIRE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Préparation Offensive Security Experienced Penetration Tester (OSEP)

Objectifs

- Maîtriser les techniques avancées de tests d'intrusion contre des systèmes durcis.
- Apprendre à contourner les mécanismes de défense tels que les antivirus, les listes blanches d'applications et les filtres réseau.
- Développer des compétences en post-exploitation sur des environnements Windows et Linux.
- Acquérir une expertise en exploitation d'Active Directory et en mouvements latéraux au sein d'un réseau.

Prérequis de la Formation

- Avoir suivi la formation Offensive Security Certified Professional (OSCP) ou posséder une expérience équivalente en tests d'intrusion.
- Maîtrise de l'environnement Kali Linux.
- Connaissances solides en réseaux et systèmes d'exploitation

Audience Ciblée

- Professionnels de la cybersécurité souhaitant approfondir leurs compétences en tests d'intrusion avancés.
- Pentesters expérimentés désirant se spécialiser dans l'évasion des défenses et les attaques furtives.
- Membres d'équipes Red Team cherchant à renforcer leurs techniques d'attaque.

Programme

- Théorie des systèmes d'exploitation et de la programmation.
- Exécution de code côté client avec Office.
- Exécution de code côté client avec JScript.
- Injection et migration de processus.
- Introduction à l'évasion des antivirus.
- Évasion avancée des antivirus.
- Listes blanches d'applications.
- Contournement des filtres réseau.
- Post-exploitation sur Linux.
- Post-exploitation sur Windows.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ TECHNIQUE

Pentesting – Réaliser des tests d'intrusion

Objectifs

- Comprendre les fondamentaux et le cadre juridique du pentesting.
- Connaître les différentes phases d'un test d'intrusion.
- Utiliser les outils et techniques d'analyse de pentesting.
- Simuler des attaques.
- Rédiger un rapport d'audit professionnel.

Prérequis de la Formation

- Des notions en informatique et sécurité des systèmes d'information.

Audience Ciblée

- RSSI,
- Techniciens,
- Auditeurs amenés à faire du pentest, Administrateurs systèmes et réseaux.

Programme

Jour 1

- Matin : Objectifs de la formation / Définitions (pentest vs audit) / Cadre légal & principes de la sécurité / Quiz de validation
- Après-midi : Méthodologies et approches de pentest / Planification & périmètre / Cycle de vie d'un test / Étude de cas / Quiz

Jour 2

- Matin : Reconnaissance passive (OSINT) / Cartographie des actifs / Outils comme Whois, Shodan, Maltego / Quiz
- Après-midi : Reconnaissance active / Scans réseau & vulnérabilités (Nmap, Nessus, OpenVAS…) / Exercices pratiques de détection de failles / Quiz

Jour 3

- Matin : Tests d'exploitation des vulnérabilités / Exploitation manuelle vs automatisée / Introduction à Metasploit et autres frameworks / Quiz
- Après-midi : Tests sur infrastructures systèmes & réseau / Applications web (SQLi, XSS, CSRF, LFI/RFI) / Applications mobiles / Labs pratiques / Quiz

Jour 4

- Matin : Techniques avancées : élévation de privilèges, pivoting, persistance / Ingénierie sociale / Sécurité physique / Quiz
- Après-midi : Post-intrusion : exploitation, validation, collecte de preuves / Exercices de type Capture The Flag (CTF) / Qui

Jour 5

- Matin : Analyse et documentation des résultats / Rédaction de rapport d'audit professionnel / Restitution aux décideurs et techniciens / Quiz
- Après-midi : Plans d'action correctifs et suivi / Mise en situation et évaluation des compétences / Bonnes pratiques pour pérenniser un processus de pentesting /Clôture et évaluation finale / Remise des attestations

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

FOUNDATIONS CERTIFICATION

FOUNDATIONS CERTIFICATION

CompTIA Tech+ (FC0-U71)

Objectifs

CompTIA Tech+ is the foundational certification program designed to build essential tech knowledge across a range of essential domains and provide instructors with the tools they need to guide learners toward a successful career in tech.

CompTIA Tech+ gives learners the knowledge and skills required to:

- Understand and manage tech infrastructure and computing concepts.
- Troubleshoot and resolve common hardware and software issues.
- Recognize and address basic cybersecurity threats.
- Understand the increasing relevance of emerging technologies.
- Pursue a more advanced certification, such as CompTIA A+.

With hands-on simulations for tasks like setting up a computer and securing a small wireless network, learners can gain a solid foundation in tech fundamentals. The course also introduces emerging technologies, including artificial intelligence, Internet of Things (IoT), robotics, quantum computing, and more.

Prérequis de la Formation

- CompTIA Tech+ is the only pre-career certification that helps students and career changers determine if they have competency in tech, and if it's the right career path for them.

Programme

Lesson 1
- Understanding Tech Basics

Lesson 2
- Data and Privacy

Lesson 3
- Internet Technologies

Lesson 4
- Cybersecurity

Lesson 5
- Networking

Lesson 6
- Applications and Software

Lesson 7
- Operating Systems

Lesson 8
- Hardware

Lesson 9
- Databases

Lesson 10
- Coding

Lesson 11
- The Future of Tech

- CompTIA Tech+ FC0-U71 Exam Practice

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

C)SA1+2: Certified Security Awareness 1 + 2

Objectifs

- Upon completion, the Certified Security Awareness 1 + 2 candidate will be able to competently take the C)SA1 + 2 exams as well as be able to understand basic cybersecurity principles to keep companies' IP and IT infrastructure safe.

Prérequis de la Formation

- None.

Audience Ciblée

- Everyone
- End Users
- Employees
- Managers

Programme

Module 1

- Basic Security Awareness What is it and why it's needed? End User Risk Trends

Module 2

- Social Engineering Phishing Mail, via phone, social websites are common Spear Phishing

Module 3

- Data Classification and corporate use (Safe Guarding) Corporate Sensitive, internal or public classification

Module 4

- End User Best Practices Hot spots, public places & roaming risks Safe Web Site surfing

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

FOUNDATIONS CERTIFICATION

MILE2 CERTIFIED Network Principles

Objectifs

- Upon completion, the Certified Network Principles candidate will be able to competently take the C)NP exams well as the Comp TIA Network+ exam. You will have the knowledge to keep a companies' IP network infrastructure secure.

Prérequis de la Formation

- (Any of the following Mile2 Courses)
- C)HT/C)OST or equivalent knowledge

Audience Ciblée

- Everyone
- End Users
- Employees
- Managers

Programme

Module 1
- Introduction to Network Fundamentals

Module 2
- The Physical Networking Fundamentals

Module 3
- TCP/IP Primer

Module 4
- Connecting Networks with Switches and Routers

Module 5
- Wireless Networking

Module 6
- Security Principles

Module 7
- Defending the Network

Module 8
- Network Technology Boom

Module 9
- Day to Day Networking

Module 10
- Network Planning

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

FOUNDATIONS CERTIFICATION

MILE2 CERTIFIED Information Technology Principles

Objectifs

- Upon completion, the Certified Internet Technology Principles (CITP) candidate will be able to competently take the C)ITP exams as well as be able to understand basic IT principles to provide individuals with the fundamentals of computer and network security concepts.

Prérequis de la Formation

- None.

Audience Ciblée

- Everyone
- Employees
- IT Starters
- Career Changers
- Secondary Students
- Post-secondary Students

Programme

Module 1

- Utilizing Computers

Module 2

- Utilizing Databases and Applications

Module 3

- Utilizing Computer Hardware

Module 4

- Utilizing Networks

Module 5

- Introduction to Security Concepts

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

FOUNDATIONS CERTIFICATION

C)HT/C)OST: Certified Hardware Technician & Operating Systems Technician

Objectifs

- Upon completion, the Certified Hardware Technician and Certified Operating Systems Technician candidate will be able to competently take the C)OST & C)HT exams well as the CompTIAA+ 220-1002 exam.

Prérequis de la Formation

- None.

Audience Ciblée

- Anyone

Programme

Chapter 1

C)HT Detailed Outline

Module 1
- Troubleshooting

Module 2
- Motherboards and CPUs

Module 3
- Power Supplies

Module 4
- Memory

Module 5
- Computer Expansion

Module 6
- Physical Storage

Module 7
- Input-Output Devices

Module 8
- Display Devices

Module 9

Network Cables and Connectors

Module 10

Printers and Multifunction Print Devices

Module 11

TCP/IP and Transport Protocols

Module 12

Custom Computers

Module 13

Operational Procedures

Chapter 2

C)OST Detailed Outline

Module 1
- Operating Systems

Module 2
- Windows Management

Module 3
- Network Basics

Module 4
- Network Protocols

Module 5
- Wireless Networking

Module 6
- Windows Networking

Module 7
- Virtualization and Cloud Computing

Module 8
- Security Principles

Module 9
- Security Technologies

Module 10
- Securing Devices and Data

Module 11

SOHO Network Configurations

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

FOUNDATIONS CERTIFICATION

MILE2 Foundational Course path

Objectifs

- After completing this series of training courses, the student will have broad knowledge at foundational IT level. After this, you can further specialize in one of the roles defined on the Mile2 roadmap or in another IT direction with certifications from alternative vendors such as Microsoft, ISTQB, etc.

Prérequis de la Formation

- None.

Audience Ciblée

- Anyone

Programme

This package includes the courses CSA 1+2, CITP, CHT+COST and CNP. For a detailed overview of the content of these courses, see the content of the individual course on this site.

- **Security Awareness 1**
- **Security Awareness 2**
- **IT Principles**
- **Hardware Technician**
- **Operating Systems Technician**
- **Network Principles**

Informations Pratiques

16 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CORE

CORE

CompTIA Security+ (701)

Objectifs

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and is the first security certification a candidate should earn. Security+ establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions;
- Monitor and secure hybrid environments, including cloud, mobile, and IoT;
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance;
- Identify, analyze, and respond to security events and incidents.

Prérequis de la Formation

- CompTIA Network+ and a minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts.

Audience Ciblée

This course is designed for an early-career IT Professional looking to open the door to a career in cybersecurity.

- Security Specialist
- Security Administrator
- Systems Administrator
- Help Desk Analyst
- Security Analyst
- Security Engineer

Programme

Lesson 1
- Summarize Fundamental Security Concepts

Lesson 2
- Compare Threat Types

Lesson 3
- Explain Cryptographic Solutions

Lesson 4
- Implement Identity and Access Management

Lesson 5
- Secure Enterprise Network Architecture

Lesson 6
- Secure Cloud Network Architecture

Lesson 7
- Explain Resiliency and Site Security Concepts

Lesson 8
- Explain Vulnerability Management

Lesson 9
- Evaluate Network Security Capabilities

Lesson 10
- Assess Endpoint Security Capabilities

Lesson 11
- Enhance Application Security Capabilities

Lesson 12
- Explain Incident Response and Monitoring Concepts

Lesson 13
- Analyze Indicators of Malicious Activity

Lesson 14
- Summarize Security Governance Concepts

Lesson 15
- Explain Risk Management Processes

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

EARLY CAREER

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CORE

CompTIA a+ Network

Objectifs

The CompTIA a+ Network course serves as an ideal starting point for individuals looking to launch a career in networking, providing the foundational knowledge and skills necessary to succeed. This program prepares learners to understand and manage network configurations, troubleshoot connectivity issues, and secure network environments, laying the groundwork for advanced training courses like CompTIA Network+. By building a strong baseline in networking concepts, CompTIA a+ Network empowers learners to pursue industry-recognized certifications and unlock opportunities in the dynamic and evolving field of IT networking. CompTIA a+ Network is designed to fast track learners to a career in IT Networking.

- Learn how to install networks in different places, like homes and offices
- Get to know how to keep networks running well and fix them when they have problems
- Discover the basics of helping apps work, managing servers, setting up network users, storing data, and making tasks automatic
- Gain the essentials to progress to CompTIA Network+ certification training

Programme

Lesson 1
- Network Client Fundamentals

Module 2
- Local Network Types

Module 3
- Other Network Types

Module 4
- Enterprise Network Application Support

Module 5
- Network Operations Support Fundamentals

Module 6
- Network Troubleshooting Fundamentals

Module 7
- Linux App Server Fundamentals

Module 8
- Automation Scripting Fundamentals

Module 9
- Data Management Fundamentals

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CORE

CompTIA Network+ (N10-009)

Objectifs

CompTIA Network+ is a global certification that validates the baseline skills necessary to establish, maintain, troubleshoot and secure networks in any environment, preparing you for a rewarding career in networking and cybersecurity.

The CompTIA Network+ certification exam will certify the successful candidate has the knowledge and skills required to:

- Establish network connectivity by deploying wired and wireless devices.
- Explain the purpose of documentation and maintain network documentation.
- Configure common network services.
- Explain basic data center, cloud, and virtual-networking concepts.
- Monitor network activity and troubleshoot performance and availability issues.
- Implement network security hardening techniques.
- Manage, configure, and troubleshoot network infrastructure.

Audience Ciblée

This course is designed for people who are seeking to launch a career in networking and cybersecurity.

- Junior Network Administrator
- NOC Technician
- Systems Administrator
- Datacenter Support Technician
- Telecommunications Technician
- IT Support Manager
- Tier II Support Technician

Programme

Lesson 1
- Explaining Network Topologies

Lesson 2
- Supporting Cabling and Physical Installations

Lesson 3
- Configuring Interfaces and Switches

Lesson 4
- Configuring Network Addressing

Lesson 5
- Configuring Routing and Advanced Switching

Lesson 6
- Implementing Network Services

Lesson 7
- Explaining Application Services

Lesson 8
- Supporting Network Management

Lesson 9
- Explaining Network Security Concepts

Lesson 10
- Applying Network Security Features

Lesson 11
- Supporting Network Security Design

Lesson 12
- Configuring Wireless Networks

Lesson 13
- Comparing Remote Access Methods

Lesson 14
- Summarizing Cloud Concepts

- A.0 Network Sandbox
- B.0 CompTIA Network+ N10-009 Practice Exams

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

EARLY CAREER

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CORE

CompTIA A+(220-1201 & 220-1202)

Objectifs

- Install, configure, and maintain computer equipment, mobile devices, and software for end users
- Service components based on customer requirements
- Understand networking basics and apply basic cybersecurity methods to mitigate threats
- Properly and safely diagnose, resolve, and document common hardware and software issues
- Apply troubleshooting skills and provide customer support using appropriate communication skills
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments

Prérequis de la Formation

- 12 months of hands-on experience in an IT support specialist job role.

Programme

Lesson 1
- What Does an IT Specialist Do?

Lesson 2
- Installing Motherboards and Connectors

Lesson 3
- Installing System Devices

Lesson 4
- Troubleshooting PC Hardware

Lesson 5
- Comparing Local Networking Hardware

Lesson 6
- Configuring Network Addressing and Internet Connections

Lesson 7
- Supporting Network Services

Lesson 8
- Summarizing Virtualization and Cloud Concepts

Lesson 9
- Supporting Mobile Devices

Lesson 10
- Supporting Print Devices

Lesson 11
- Managing Support Procedures

Lesson 12
- Configuring Windows

Lesson 13
- Managing Windows

Lesson 14
- Supporting Windows

Lesson 15
- Securing Windows

Lesson 16
- Installing Operating Systems

Lesson 17
- Supporting Other OS

Lesson 18
- Configuring SOHO Network Security

Lesson 19
- Managing Security Settings

Lesson 20
- Supporting Mobile Software

Lesson 21
- Using Data Security

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

INFRASTRUCTURE

CompTIA Cloud+ CV0-004

Objectifs

- Understand cloud architecture and design concepts Implement and maintain a secure cloud environment
- Successfully provision and configure cloud resources
- Demonstrate the ability to manage operations throughout the cloud environment life cycle using observability, scaling and automation
- Understand fundamental DevOps concepts related to deployment and integration
- Troubleshoot common issues related to cloud management

Prérequis de la Formation

- Learners should possess 5 years of tech experience. Ideally 2-3 years of that experience would include networking or systems administration.

Programme

Lesson 1
- Understanding Cloud Architecture Concepts

Lesson 2
- Planning Cloud Services

Lesson 3
- Provisioning and Migrating Cloud Resources

Lesson 4
- Comparing Cloud Storage

Lesson 5
- Troubleshooting Deployment Issues and Cost

Lesson 6
- Using Virtualization and Databases

Lesson 7
- Comprehending Cloud Networking

Lesson 8
- Automating Cloud Resources

Lesson 9
- Implementing Security Management

Lesson 10
- Comprehending Security Compliance and Troubleshooting

Lesson 11
- Implementing Performance and Monitoring

Lesson 12
- Managing Disaster Recovery and Business Continuity

- A.0 CompTIA Cloud+ CV0-004 Practice Test

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

Collecte et analyse des Logs avec Splunk

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

Prérequis de la Formation

- Connaissances de base des réseaux et des systèmes

Audience Ciblée

- Administrateurs systèmes et réseaux

Programme

Module 1

- Installer Splunk ; récupérer/injecter les données

Module 2

- Exploration de données

Module 3

- Tableaux de bord (Base)

Module 4

- Tableaux de bord (Avancé)

Module 5

- Installation d'application

Module 6

- Modèles de données

Module 7

- Enrichissement de données

Module 8

- Alertes

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION NON CERTIFIANTE

NIVEAU FONDAMENTAL

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **ACG CYBERSECURITY**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : CLOUD SECURITY ENGINEER

PREVENTION : CLOUD SECURITY ENGINEER

MILE2 CERTIFIED Cloud Security Officer

Objectifs

- Upon completion, Certified Cloud Security Officer students will understand Cloud security from a real-world viewpoint and comprehend the industry security standards. The student will also be prepared to take the C)CSO exam.

Prérequis de la Formation

- (Any of the following Mile2 Courses)
- 12 months experience with virtualization technology or equivalent knowledge.
- General understanding of cloud architectures
- Minimum 12 months experience with general security

Audience Ciblée

- Virtualization Admins
- Cloud Security Officers
- CIO
- Virtualization and Cloud Auditors
- Virtualization and Cloud Compliance Officers

Programme

Module 1
- Introduction to Cloud Computing and Architecture

Module 2
- Cloud Risks

Module 3
- ERM and Governance

Module 4
- Legal Issues

Module 5
- Virtualization

Module 6
- Data Security

Module 7
- Data Center Operations

Module 8
- Interoperability and Portablility

Module 9
- Traditional Security

Module 10
- BCM and DR

Module 11
- Incident Response

Module 12
- Application Security

Module 13
- Encryption and Key Management

Module 14
- Identity, Entitlement and Access Management

Module 15
- Auditing and Compliance

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

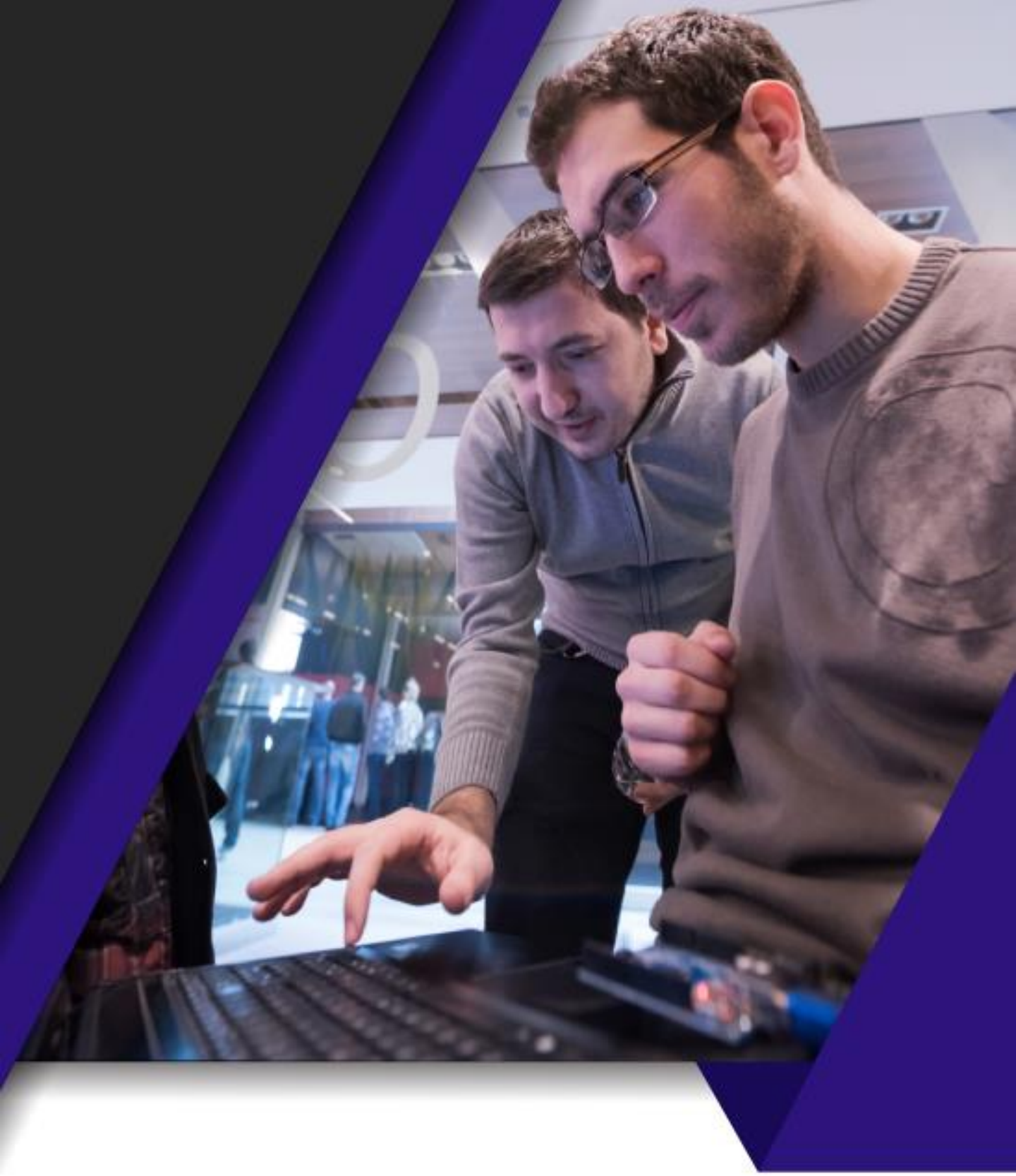
LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures



SÉCURITÉ DE L'INFORMATION

SÉCURITÉ DE L'INFORMATION

PECB

PECB CERTIFIED ISO/IEC 27400 Lead Manager

Objectifs

- Explain the fundamental concepts and principles of IoT security and privacy
- Evaluate the organization's context and alignment of IoT with business processes, and define the roles and responsibilities in ensuring IoT security and privacy
- Implement asset management practices specific to IoT devices, systems, and components
- Identify, assess, and manage risks associated with IoT systems
- Implement security and privacy controls specific to IoT service providers, developers, and users
- Implement procedures for detecting, reporting, and responding to IoT-related incidents

Prérequis de la Formation

A basic understanding of cybersecurity, Internet of Things (IoT) technologies, and information security management principles is recommended to successfully follow this training course.

Audience Ciblée

- Individuals seeking to gain a thorough understanding of IoT security and privacy principles and best practices
- Professionals responsible for ensuring security, privacy, and compliance in IoT environments
- Managers overseeing IoT infrastructure and managing risks associated with IoT deployments
- Consultants advising organizations on IoT security, privacy, and risk management
- Individuals looking to advance their careers in the rapidly growing IoT security industry
- IoT service providers, IoT service developers, and IoT users who are involved in defining security and privacy requirements or implementing controls throughout the IoT systems life cycle, as described in ISO/IEC 30141 and ISO/IEC 27400

Programme

Day 1

- IoT concepts, principles, and lifecycle

Day 2

- Security roles and responsibilities, asset management, and risk management

Day 3

- IoT security and privacy controls, blockchain and integrated technologies, and training

Day 4

- IoT security monitoring, incident management, internal audit and management review, and continual improvement

Day 5

- Certification exam

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **PECB**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SÉCURITÉ DE L'INFORMATION

ISC2 Systems Security Certified Practitioner

Objectifs

- Discuss the foundational concepts of cybersecurity principles.
- Recognize foundational security concepts of information assurance.
- Define risk management terminology and summarize the process.
- Relate risk management to personal or professional practices.
- Classify types of security controls.
- Distinguish between policies, procedures, standards, regulations and laws.
- Demonstrate the relationship among governance elements.
- Analyze appropriate outcomes according to the canons of the ISC2 Code of Ethics when given examples.
- Practice the terminology of and review security policies.
- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions.
- Recall the terms and components of incident response.

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

- None. No prior work experience or formal degree required. You only need to become an ISC2 Candidate.

Audience Ciblée

This training course is intended for practitioners who have at least one year of cumulative, paid work experience in one or more of the seven domains of the ISC2 SSCP CBK and are pursuing SSCP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those with technical skills and practical, hand-on security knowledge working in operational IT positions.

such as, but not limited to:

- Network Security Engineer
- Systems/Network Administrator
- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

Programme

Chapter 1

- Introducing Security and Aligning Asset Management to Risk Management

Chapter 2

- Understanding Risk Management Options and the Use of Access Controls to Protect Assets

Chapter 3

- Cryptography

Chapter 4

- Securing Software, Data, and Endpoints

Chapter 5

- Network and Communications Security

Chapter 6

- Cloud and Wireless Security

Chapter 7

- Incident Detection and Response

Chapter 8

- Maturing Risk Management

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SSCP®

ELECTIVES

MILE2 CERTIFIED ISMS Lead Auditor/Implementer

Objectifs

- Upon completion, the Certified Information Security Management Systems – Lead Auditor candidate will be able to competently take the C)ISMS-LA exam and acquire the necessary knowledge to manage an ISMS audit.

Prérequis de la Formation

- Experience with Information Systems
- Interest in Auditing

Audience Ciblée

- Internal Auditor
- IT Auditor and Lead Auditor
- It Consultant
- Chief Information Officer
- Security Consultant

Programme

Module 1

- Lead Auditor Intro

Module 2

- The ISO/27001:2013

Module 3

- Information Security and Key Controls

Module 4

- Risk Management

Module 5

- Risk Treatment

Module 6

- Audits and Auditors

Module 7

- Auditing the Information Security Management System

Module 8

- Planning and Conducting an Audit

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Healthcare Information Systems Security

Objectifs

- Upon completion, Certified Healthcare Information Systems Security Practitioner students will be versed with best practices in the healthcare industry and will be able to establish a framework with current best practices in respects to privacy, regulation and risk management.

Prérequis de la Formation

- 12 Months of Healthcare Information Systems Management

Audience Ciblée

- IS Security Officers, Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security Managers
- Compliance and Privacy Officers

Programme

Module 1

- Intro to the Healthcare Industry

Module 2

- Regulatory Environment

Module 3

- Healthcare Privacy and Security Policies

Module 4

- Information Governance

Module 5

- Risk Managment

Module 6

- Thrid-Party Management

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

ELECTIVES

MILE2 IS18 Controls

Objectifs

- Upon completion, the IS18 Security Controls candidate will be able to competently take the IS18 Controls exam and understand how to implement the top 18 most critical controls in the workplace.

Prérequis de la Formation

- Broad Understanding of Multiple Networking and Security Technologies

Audience Ciblée

- Information Assurance Managers/Auditors
- System Implementers
- IT Administrators
- Auditors
- Federal Agencies
- Security Vendors and Consulting Groups

Programme

Module 1

- Introduction

Module 2

- Inventory and Control

Module 3

- Inventory and Control of Software Assets

Module 4

- Data Protection

Module 5

- Secure Configuration of Enterprise Assets and Software Concept

Module 6

- Account Management

Module 7

- Access Control Management

Module 8

- Continuous Vulnerability Management

Module 9

- Audit Log Management

Module 10

- Email and Browser Protection

Module 11

- Malware Defenses

Module 12

- Data Recovery

Module 13

- Network Infrastructure Management

Module 14

- Network Monitoring and Defense

Module 15

- Security Awareness and Skills Training

Module 16

- Service Provider Management

Module 17

- Applications Software Security

Module 18

- Incident Response Mgmt

Module 19

- Penetration Testing

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Wireless Security Engineer

Objectifs

- Upon completion, Certified Wireless Security Engineer students will not only be able to establish industry acceptable Cyber Security & IS management standards with current best practices but also be prepared to competently take the C)WSE exam.

Prérequis de la Formation

- Mile2's C)SP
- 12 months of Information Systems Management Experience

Audience Ciblée

- Coders
- Application Engineers
- IS Managers
- Developers
- Programmers

Programme

Module 1

- Business and Technical Logistics

Module 2

- Wireless Security Fundamentals

Module 3

- Authentication

Module 4

- Encryption

Module 5

- WLAN Encryption Implementations

Module 7

- Reconnaissance and Enumeration

Module 8

- Network Assessment and Exploitation Techniques

Module 9

- Evasion Techniques

- CYBER RANGE - WIRELESS LABS

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : APPLICATION SECURITY CODER

PREVENTION : APPLICATION SECURITY CODER

ISC2 CERTIFIED Secure Software Lifecycle Professional

Objectifs

- Discuss the core concepts of software security and the foundational principles that drive construction of resilient software.
- Discuss the security design principles as essential elements for building secure software.
- Discuss software security standards and frameworks, roadmaps and strategies and risk management.
- Explain security in software development methodologies, security metrics and security culture in software development.
- Identify and analyze software requirements pertaining to data privacy, security and compliance with laws and regulations.
- Describe requirement specification and tractability, misuse and abuse cases and flow down of security requirements to supplier.
- Explain secure architecture and design elements and patterns, architectural risk assessment, threat modeling, threat intelligence and attack surface evaluation.
- Explain security architecture and control identification, prioritization and positioning.
- Apply secure coding practices, analyze code for security risks and implement security controls.
- Discuss third-party code and libraries, software composition analysis and security of the build process.

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

To qualify for the CSSLP, candidates must have a minimum of four years of cumulative paid work experience in one or more of the eight domains of the current ISC² CSSLP Exam Outline. If you don't yet have the required experience to become a CSSLP, you may become an Associate of ISC² after successfully passing the CSSLP exam. The Associate of ISC² will then have five years to earn the experience needed for the CSSLP certification.

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Audience Ciblée

This training course is intended for professionals who have at least four years of cumulative, paid work experience as a software development lifecycle professional in one or more of the eight domains of the ISC2 CSSLP CBK. The course builds on and brings together the holistic view of the topics covered in the everyday environment of an information assurance professional. Experience in the following professions will greatly enhance the learning environment:

- Software developers
- Engineers and architects
- Product managers
- Project managers
- Software QA
- Business analysts
- Professionals who manage these stakeholders

Programme

Chapter 1

- Secure Software Concepts

Chapter 2

- Secure Software Lifecycle and Risk Management Domain

Chapter 3

- Secure Software Requirements Domain

Chapter 4

- Secure Software Architecture and Design Domain

Chapter 5

- Secure Software Implementation Domain

Chapter 6

- Secure Software Testing Domain

Chapter 7

- Secure Software Deployment, Operations and Maintenance Domain Learning Objectives

Chapter 8

- Secure Software Supply Chain Domain

Chapter 9

- Applied Scenario Activities

Les Plus

- Cours animé par un formateur certifié ISC2
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CSSLP®

PREVENTION : APPLICATION SECURITY CODER

MILE2 CERTIFIED Vulnerability Assessor

Objectifs

- Upon completion, the Certified Vulnerability Assessor candidate will be able to competently take the C)VA exam.

Prérequis de la Formation

- Basic Networking Understanding
- Mile2's CNP

Audience Ciblée

- Information System Owners
- Analysts
- Ethical Hackers
- ISSOs
- IT Engineers
- Cyber Security Managers

Programme

Module 1

- Why Vulnerability Assessment

Module 2

- Vulnerability Types

Module 3

- Assessing the Network

Module 4

- Assessing Web Servers and Applications

Module 5

- Assessing Remote and VPN Services

Module 6

- Vulnerability Assessments & Tools of the Trade

Module 7

- Output Analysis

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 200

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : APPLICATION SECURITY CODER

MILE2 CERTIFIED Secure Web Application Engineer

Objectifs

- Upon completion, Certified Secure Web Application Engineer students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the C)SWAE exam.

Prérequis de la Formation

- Sound knowledge of networking
- At least one coding language
- Linux understanding
- Open shell Or 24 months experience in software technologies and security.

Audience Ciblée

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Programme

Module 1
- Web Application Security

Module 2
- Secure SDLC

Module 3
- OWASP Top 10

Module 4
- Risk Management

Module 5
- Threat Modeling

Module 6
- Authentication and Authorization Attacks

Module 7
- Session Management

Module 8
- Security Architecture

Module 9
- Data Validation

Module 10
- AJAX Security

Module 11
- Insecurity Code Review and Mitigation

Module 12
- Application Mapping Analysis

Module 13
- Cryptography

Module 14
- Web Application Penetration Testing

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : INTRUSION PREVENTION SPECIALIST

PREVENTION : INTRUSION PREVENTION SPECIALIST

MILE2 CERTIFIED Penetration Testing Engineer

Objectifs

- Upon completion, the Certified Penetration Testing Engineer, C)PTE, candidate will have solid knowledge of testing and reporting procedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTE exam.

Prérequis de la Formation

- Mile2 C)PEH or equivalent knowledge
- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security experience

Audience Ciblée

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Programme

Module 1

- Business & Technical Logistics of Pen Testing

Module 2

- Information Gathering

Module 3

- Detecting Live Systems

Module 4

- Banner Grabbing and Enumeration

Module 5

- Automated Vulnerability Assessment

Module 6

- Hacking an OS

Module 7

- Advanced Assessment and Exploitation Techniques

Module 8

- Evasion Technique

Module 9

- Hacking with PowerShell

Module 10

- Networks and Sniffing

Module 11

- Hacking Web Tech

Module 12

- Mobile and IoT Hacking

Module 13

- Report Writing Basics

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : INTRUSION PREVENTION SPECIALIST

MILE2 CERTIFIED Penetration Testing Consultant

Objectifs

- Upon completion, the Certified Penetration Testing Consultant, C)PTC, candidate will have solid knowledge of testing and reporting proceedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTC exam.

Prérequis de la Formation

- Mile2 C)PEH and C)PTE or equivalent knowledge
- 2 years of experience in Networking Technologies
- Sound Knowledge of TCP/IP
- Computer Hardware Knowledge

Audience Ciblée

- IS Security Officers
- Cybersecurity Managers/Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Programme

Module 1

- Pentesting Team Foundation

Module 2

- NMAP Automation

Module 3

- Exploitation Process

Module 4

- Fuzzing with Spike

Module 5

- Simple Buffer Overflow

Module 6,

- Stack Based Windows Buffer Overflow

Module 7

- Web Application Security and Exploitation

Module 8

- Linux Stack Smashing & Scanning

Module 9

- Linux Address Space Layout Randomization

Module 10

- Windows Exploit Protection

Module 11

- Getting Around SEH ASLR

Module 12

- Penetration Testing Report Writing

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

AUDITING : INFORMATION SYSTEMS SECURITY AUDITOR

AUDITING : INFORMATION SYSTEMS SECURITY AUDITOR

MILE2 CERTIFIED Cybersecurity Systems Manager

Objectifs

- Upon completion, Certified Cybersecurity Systems Manager students will have a strong foundation in Cyber Security & IS management standards with current best practices and will be prepared to competently take the C)CSSM exam.

Prérequis de la Formation

- Mile2's C)SP
- 12 months of Information Systems Experience

Audience Ciblée

- Penetration Testers
- Microsoft Administrators
- Security Administrators
- Active Directory Admins

Programme

Module 1

- Introduction

Module 2

- Architectural Frameworks and Compliance

Module 3

- Risk Management and Controls

Module 4

- Evaluating Systems and Management Strategies

Module 5

- Incident Management, Law, and Ethics

Module 6

- Business Continuity and Disaster Recovery Processes

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

AUDITING : INFORMATION SYSTEMS SECURITY AUDITOR

MILE2 CERTIFIED Cybersecurity Systems Auditor

Objectifs

- Upon completion, Certified Cybersecurity Systems Auditor students will be able to establish industry acceptable Cyber Security & IS management standards with current best practices and be prepared to competently take the C)CSSA exam.

Prérequis de la Formation

- Mile2's C)SP
- 12 months of IT experience

Audience Ciblée

- IS Security Officers
- Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security managers
- Government employees

Programme

Module 1

- The Process of Auditing Information Systems

Module 2

- Risk-Based Auditing

Module 3

- Audit Planning and Performance

Module 4

- IS Systems Reports

Module 5

- IT Governance and Management

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

AUDITING : INFORMATION SYSTEMS SECURITY AUDITOR

MILE2 CERTIFIED Information System Security Officer

Objectifs

- Upon completion, Certified Information Systems Security Officer students be able to establish industry acceptable Cyber Security and Information Systems management standards with current best practices.

Prérequis de la Formation

- Mile2's C)SP
- Mile2's C)ISSM
- 12 months of Information Systems Management Experience

Audience Ciblée

- IS Security Officers
- IS Managers
- Risk Managers
- Auditors
- Info Systems Owners
- IS Control Assessors
- System Managers
- Government Employees

Programme

Module 1
- Risk Management

Module 2
- Security Management

Module 3
- Identification and Authentication

Module 4
- Access Control

Module 5
- Security Models and Evaluation Criteria

Module 6
- Operations Security

Module 7
- Symmetric Cryptography and Hashing

Module 8
- Asymmetric Cryptography and PKI

Module 9
- Network Connections

Module 10
- Network Protocols and Devices

Module 11
- Telephony, VPNs and Wireless

Module 12
- Security Architecture and Attacks

Module 13
- Software Development Security

Module 14
- Database Security

Module 15
- Malware and Attacks XVI

Module 16
- Business Continuity

Module 17
- Incident Management, Law and Ethics

Module 18
- Physical Security

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 300

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

AUDITING : INFORMATION SYSTEMS SECURITY AUDITOR

MILE2 CERTIFIED Security Principles

Objectifs

- Upon completion, the Certified Security Principles candidate will not only be able to competently take the C)SP exam but will also understand the principal security knowledge to keep companies' IP and IT infrastructure safe.

Prérequis de la Formation

- 12 Months of experience with server administration
- Mile2 C)SA1, C)SA2, C)HT, C)OST and C)NP
- Equivalent Knowledge

Audience Ciblée

- IT Professionals
- Server Administrators
- Virtualization and Cloud Administrators

Programme

Module 1
- Introduction to IT Security

Module 2
- Risk Management

Module 3
- Audit Planning and Performance

Module 4
- Understanding Identity and Access Management

Module 5
- Managing Data Security

Module 6
- Data Security

Module 7
- Managing Server/Host Security

Module 8
- Application Security for Non-Developers

Module 9
- Understanding Mobile Device Security (IoT)

Module 10
- Managing Day to Day Security

Module 11
- Understating Compliance and Auditing

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 200

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RESPONSE & RECOVERY :
DISASTER RECOVERY ENGINEER

RESPONSE & RECOVERY : DISASTER RECOVERY ENGINEER

MILE2 CERTIFIED Disaster Recovery Engineer

Objectifs

- Upon completion, Certified Disaster Recovery Engineer students will be able to establish industry acceptable DR & BCP standards with current best practices and policies. Students will also be prepared to competently take the C)DRE exam.

Prérequis de la Formation

- 12 Months in Information Systems
- 12 Months in Information Systems Management
- Mile2's C)ISSO Course

Audience Ciblée

- IS Security Officers
- IS Managers
- Risk Managers
- DR and BCP Engineers
- Info Systems Owners
- IS Control Assessors
- System Managers
- Government workers

Programme

Module 1

- Introduction

Module 2

- Business Impact Analysis

Module 3

- BCP and DRP Design

Module 4

- IT Recovery Strategies

Module 5

- IT Resiliency

Module 6

- Implementation Phase

Module 7

- Testing and Exercise

Module 8

- Maintenance and Execution

Module 9

- Pandemics

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RESPONSE & RECOVERY :
CYBER FORENSIC INVESTIGATOR

RESPONSE & RECOVERY : CYBER FORENSIC INVESTIGATOR

MILE2 CERTIFIED Network Forensics Examiner

Objectifs

- Upon completion, Certified Network Forensics Examiner students will have knowledge to perform network forensic examinations. Be able to accurately report on their findings, and be ready to sit for the C)NFE exam.

Prérequis de la Formation

- 2 years networking experience
- 2 years in IT Secuirty – Working knowledge of TCPIP

Audience Ciblée

- Digital and Network Forensics Examiners
- IS Managers
- Network Auditors
- IT Managers

Programme

Module 1
- Digital Evidence Concepts

Module 2
- Network Evidence Challenges

Module 3
- Network Forensics Investigative Methodology

Module 4
- Network-Based Evidence

Module 5
- Network Principles

Module 6
- Internet Protocol Suite

Module 7
- Physical Interception

Module 8
- Traffic Acquisition Software

Module 9
- Live Acquisition

Module 10
- Analysis

Module 11
- Layer 2 Protocol

Module 12
- Wireless Access Points

Module 13
- Wireless Capture Traffic and Analysis

Module 14
- Wireless Attacks

Module 15
- NIDS/Snort

Module 16
- Centralized Logging and Syslog

Module 17
- Investigating Network Devices

Module 18
- Web Proxies and Encryption

Module 19
- Network Tunneling

Module 20
- Malware Forensics

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RESPONSE & RECOVERY : CYBER FORENSIC INVESTIGATOR

MILE2 CERTIFIED Digital Forensics Examiner

Objectifs

- Upon completion, Certified Digital Forensics Examiner students will be able to establish industry acceptable digital forensics standards with current best practices and policies. Students will also be prepared to competently take the C)DFE exam.

Prérequis de la Formation

- 1 YR experience in computers
- Mile2's C)SP course
- Mile2's Foundational Course Pack

Audience Ciblée

- Virtualization Admins
- Cloud Security Officers
- CIO
- Virtualization and Cloud Auditors
- Virtualization and Cloud Compliance Officers

Programme

Module 1
- Computer Forensics Incidents

Module 2
- Investigative Theory

Module 3
- Investigative Process

Module 4
- Digital Acquisition and Analysis Tools

Module 5
- Disks and Storages

Module 6
- Live Acquisitions

Module 7
- Windows Forensics

Module 8
- Linux Forensics

Module 9
- Mac Forensics

Module 10
- Examination Protocols

Module 11
- Digital Evidence Protocols

Module 12
- Digital Evidence Presentation

Module 13
- Laboratory Protocols

Module 14
- Artifact Recovery

Module 15
- Advanced Search Strings

Module 16
- eDiscovery and ESI

Module 17
- Mobile Forensics

Module 18
- Incident Handling

Module 19
- Reporting

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 300

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CYBER WARFARE

CYBER WARFARE

MILE2 Ultimate Red vs Blue Team

Objectifs

- Provide hands-on experience in both offensive and defensive cybersecurity. Participants engage in simulated cyber battles, allowing them to sharpen their skills in real-world scenarios using Red Team (attack) and Blue Team (defense) tactics. The goal is to enhance detection, response, and mitigation capabilities through practical collaboration.

Prérequis de la Formation

- Participants are recommended to have prior cybersecurity experience, including familiarity with Red Team and Blue Team concepts, network analysis, incident response, and malware analysis

Audience Ciblée

- IS Security Officers
- Cybersecurity Managers/Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Programme

Module 1

- Kali vs Proximo and Graccus

Module 2

- Kali vs Priscus and Verus

Module 3

- Kali vs Maximus and Quintus

Module 4

- Kali vs Tetraites and Commodus

Informations Pratiques

2 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT ROLES : DOD CYBERSECURITY MANAGER

MILE2 CERTIFIED Cybersecurity Framework Officer

Objectifs

- Upon completion, the Certified Cybersecurity Framework Officer candidate will be able to competently take the C)CSFO Exam. They will also be ready to prepare an organization for proactive defense against today's hackers.

Prérequis de la Formation

- Any of the following Mile2 Courses)
- Certified Security Principles
- Certified Information Systems Security Officer
- Certified Vulnerability Assessor
- Or Equivalent Knowledge

Audience Ciblée

- DoD Security Professionals
- Anyone required to comply with the Cybersecurity Enhancement Act of 2014
- Anyone in a Security Operations Center • Cybersecurity Analysts

Programme

Module 1

- CSF Introduction

Module 2

- NIST CSF

Module 3

- NIST CSF Basics

Module 4

- NIST CSF Usage

Module 5

- NIST CSF SelfAssessment Process

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MILE2 CERTIFIED Risk Manager Framework Analyst

Objectifs

- Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the exam.

Prérequis de la Formation

- (Any one of the following) This is an advanced look into how the RMF applies to government systems.
- 4-5 years of information systems security management is suggested (or equivalent education).

Audience Ciblée

- IS Security Owners
- Security Officers
- Ethical Hackers
- Information Owners
- Penetration Testers
- System Owners and Managers
- Cyber Security Engineers

Programme

Module 0

- Introduction

Module 1

- Introduction to the RMF

Module 2

- The Software Development Life Cycle

Module 3

- RMF Step 1

Module 4

- RMF Step 2

Module 5

- RMF Step 3

Module 6

- RMF Step 4

Module 7

- RMF Step 5

Informations Pratiques

3 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT ROLES : INFORMATION SYSTEMS RISK MANAGER

MANAGEMENT ROLES : INFORMATION SYSTEMS RISK MANAGER

MILE2 CERTIFIED Information Systems Risk Manager

Objectifs

- Upon completion, Certified Information Systems Risk Manager students will be prepared to pass the C)ISRM exam.

Prérequis de la Formation

- Mile2's C)SP
- 12 months of IT experience

Audience Ciblée

- IS Security Officers
- Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security Managers
- Government Employees

Programme

Module 1

- The Big Picture

Module 2

- Domain 1 – Risk Identification

Module 3

- Domain 2 – Risk Response

Module 4

- Domain 3 – Risk Monitor

Module 5

- Domain 4 – IS Control Design and Implementation

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

PREVENTION : CYBER THREAT ANALYST

PREVENTION : CYBER THREAT ANALYST

MILE2 CERTIFIED Threat Intelligence Analyst

Objectifs

- Upon completion, Certified Threat Intelligence Analyst course students will have knowledge to perform thorough threat analysis on any information system. Be able to accurately report on their findings, and be ready to sit for the C)TIA exam.

Prérequis de la Formation

- 12 months vulnerability testing
- Mile2's C)VA and C)PEH

Audience Ciblée

- Penetration Testers
- Microsoft Administrator
- Security Administrators
- Active Directory Administrators
- Anyone looking to learn more about security

Programme

Module 1

- Threat Intelligence Basics

Module 2

- Cyber Threats

Module 3

- Threat Actors

Module 4

- Case Studies

Module 5

- Threat Identification

Module 6

- Proactive Approach

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

MANAGEMENT ROLES : INFORMATION SYSTEMS SECURITY OFFICER

MANAGEMENT ROLES : INFORMATION SYSTEMS SECURITY OFFICER

MILE2 CERTIFIED Security Leadership Officer

Objectifs

- Upon completion, the Certified Security Leadership Officer candidate be able to competently take the C)SLO exam. You will be versed in implementing strong security controls and managing an organization with an industry acceptable security posture.

Prérequis de la Formation

- 12 months professional experience in IT or
- 12 months professional experience in systems management

Audience Ciblée

- C – Level Managers
- IT Managers
- Cyber Security Personelle
- Engineers
- Information Systems Owners
- ISSO's
- CISSP Students
- ISO's

Programme

Module 1

- Security Management

Module 2

- Risk Management

Module 3

- Encryption

Module 4

- Information Security Access Control Concepts

Module 5

- Incident Handling and Evidence

Module 6

- Operations Security

Module 7

- Network Security

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RESPONSE & RECOVERY : INCIDENT HANDLER

RESPONSE & RECOVERY : INCIDENT HANDLER

MILE2 CERTIFIED Cybersecurity Analyst

Objectifs

- Upon completion, the Certified Cybersecurity Analyst candidate will be able to competently take the C)CSA Exam. They will also be ready to prepare an organization for proactive defense against today's hackers.

Prérequis de la Formation

- Certified Security Principles
- Certified Digital Forensics Examiner
- Certified Incident Handling Engineer
- Certified Professional Ethical Hacker

Audience Ciblée

- Security Professionals
- Incident Handling Professionals
- Anyone in a Security Operations Center
- Forensics Experts
- Cybersecurity Analysts

Programme

Chapter 1

- Blue Team Principles

Chapter 2

- Digital Forensics

Chapter 2

- Labs: Digital Forensics

Chapter 3

- Malware Analysis

Chapter 3

- Labs: Malware Analysis

Chapter 4

- Traffic Analysis

Chapter 4

- Labs: Traffic Analysis

Chapter 5

- Assessing the Current State of Defense with the Organization

Chapter 5

- Labs: Assessing the Current State of Defense within the Organization

Chapter 6

- Leveraging SIEM for Advanced Analytics

Chapter 6

- Labs: Leveraging SIEM for Advanced Analytics

Chapter 7

- Defeating the Red Team with Purple Team tactics

Chapter 7

- Labs: Defeating the Red Team with Purple Team Tactics

Informations Pratiques

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

RESPONSE & RECOVERY : INCIDENT HANDLER

MILE2 CERTIFIED Incident Handler Engineer

Objectifs

- Upon completion, Certified Incident Handling Engineer students will know NIST's 800-61 four incident handling phases, be able to accurately report on their findings, and be ready to sit for the C)IHE exam.

Prérequis de la Formation

- 12 months network technologies
- Sound knowledge of networking and TCP/IP
- Linux knowledge is essential

Audience Ciblée

- Penetration Testers
- Microsoft Administrator
- Security Administrators
- Active Directory Administrators
- Anyone looking to learn more about security

Programme

Module 1

- Incident Handling Explained

Module 2

- Incident Response Policy, Plan and Procedure Creation

Module 3

- Incident Response Team Structure

Module 4

- Incident Response Team Services

Module 5

- Incident Response Recommendations

Module 6

- Preparation

Module 7

- Detection and Analysis

Module 8

- Containment, Eradication and Recovery

Module 9

- Post Incident Activity

Module 10

- Incident Handling Checklist

Module 11

- Incident Handling Recommendations

Module 12

- Coordination and Information Sharing

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **Mile2**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

BUSINESS & IT

CompTIA Business Essentials

Objectifs

- Understand the core goals and functions of a business.
- Interpret financial statements and assess financial health.
- Create and implement effective business strategies.
- Analyze how businesses create value for stakeholders.
- Use financial data to optimize performance.
- Explore ways to achieve competitive advantages.
- Practice strategic thinking to align business goals.

Programme

Lesson 1

- Business Fundamentals

Lesson 2

- Business Strategy

Lesson 3

- Business Finance

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CLOUD

CompTIA Cloud Essentials

Objectifs

- Understand the fundamental concepts of cloud computing, including service and deployment models.
- Learn how to align cloud strategies with business objectives.
- Explore cloud migration strategies and the use of cloud-native applications.
- Gain insights into cloud governance, including risk management and compliance.
- Develop the ability to communicate effectively with technical teams about cloud initiatives.
- Prepare for the future of cloud technology and its impact on business operations.

Programme

Lesson 1

- Identifying Cloud Concepts

Lesson 2

- Applying Cloud Business Principles

Lesson 3

- Advising a Cloud Design

Lesson 4

- Operating in the Cloud

Lesson 5

- Managing Cloud Governance

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

CLOUD & INFRASTRUCTURE

CompTIA CloudNetX (CNX-001)

Objectifs

- CloudNetX helps professionals develop the expertise to design, implement, and manage secure, scalable networks that integrate both on-premises and cloud systems. With a focus on practical skills like automation, monitoring, troubleshooting, and modern security practices such as Zero Trust, this vendor-neutral certification ensures candidates are ready to tackle real-world challenges. Whether you're aiming to advance into roles like Network Architect or Enterprise Architect, or simply want to stay ahead with emerging technologies like container networking and generative AI, CloudNetX provides the tools and recognition to help you succeed. It's a certification that not only validates your technical skills but also helps you align them with business goals, making you a valuable asset in today's IT landscape.

Prérequis de la Formation

- A minimum of ten years of experience in the IT field and five years of experience in a network architect role, with experience in the hybrid cloud environment. Network+, Security+, and Cloud+ or equivalent experience.

Audience Ciblée

- Network Architect
- Cloud Architect•
- Architect
- Enterprise Architect
- Cloud Architect
- Systems Architect

Programme

Lesson 1

- Preassessment

Lesson 2

- Designing and Analyzing Networks

Lesson 3

- Troubleshooting Methodology

Lesson 4

- Comparing Network Security Principles

Lesson 5

- Planning Campus Networks

Lesson 6

- Monitoring Network Performance

Lesson 7

- Configuring Network Access and Security

Lesson 8

- 8.0 Describing Network Operations

- A.0 CloudNetX CNX- 001 Practice Exams

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

DATA

DATA

CompTIA Data+ V2

Objectifs

- Build a foundation in modern data concepts so you can confidently navigate analytics tools and data sources in any organization.
- Transform, clean, and organize raw data to make it reliable and useful for analysis.
- Apply statistical methods to extract trends, uncover insights, and support business decisions.

Discover all the details of this training by viewing its full online course page

Prérequis de la Formation

- Recommended to have 18–24 months of experience in a report/business analyst job role.

Audience Ciblée

- Data Analyst
- Reporting Analyst
- Service Desk Analyst
- Business Intelligence Analyst
- Marketing Analyst
- Financial Analyst
- Research Analyst

Programme

Lesson 1
- Summarizing Database Concepts

Lesson 2
- Comparing and Contrasting Different Data Systems

Lesson 3
- Recognizing AI's Impact on Data Project

Lesson 4
- Distinguishing Markup Languages and Data Analytics Tools

Lesson 5
- Using Data Acquisition Methods

Lesson 6
- Applying Quality Control to Data

Lesson 7
- Profiling and Cleansing Data

Lesson 8
- Executing Data Manipulation Techniques

Lesson 9
- Building Queries to Model Data

Lesson 10
- Preparing for Data Analysis

Lesson 11
- Applying Descriptive Statistical Methods

Lesson 12
- Illustrating Different Statistical Methods

Lesson 13
- Summarizing Business Requirements in a Report Format

Lesson 14
- Using the Appropriate Type of Visualization

Lesson 15
- Designing Components for Reports and Dashboards

Lesson 16
- Preparing for the Delivery and Consumption of Reports

Lesson 17
- Summarizing the Importance of Data Governance

Lesson 18

Explaining Data Management Concepts

Lesson 19
- Troubleshooting Issues and Measuring Performance

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

SYSTÈMES ET RÉSEAUX

SYSTÈMES ET RÉSEAUX

CompTIA Linux+

Objectifs

- CompTIA Linux+ validates the competencies required of an early career systems administrator supporting Linux systems.
- It certifies the successful candidate has the knowledge and skills required to configure, manage, operate, and troubleshoot Linux server environments while using security best practices, scripting, containerization, virtualization, and automation.
- Critical to help secure and manage diverse Linux systems, coupled with other certifications/experience, Linux+ sets a foundation for future professional roles such as Linux systems administrator, Cloud Administrator, DevOps Engineer, and Cybersecurity analyst.

Prérequis de la Formation

- 12 months of hands-on experience working with Linux servers. CompTIA A+, Network+, and Server+ recommended.

Audience Ciblée

This certification is designed for an early-career systems administrator supporting Linux systems.

- Job roles that Linux+ maps to:
- System Administrator
- Cybersecurity Analyst
- DevOps Engineer

Programme

Lesson 1

- Identifying Basic Linux Concepts

Lesson 2

- Administering Users and Groups

Lesson 3

- Configuring Permissions

Lesson 4

- Implementing File Management

Lesson 5

- Authoring Text Files

Lesson 6

- Deploying Software

Lesson 7

- Administering Storage

Lesson 8

- Managing the Linux Kernel and Devices

Lesson 9

- Maintaining Services

Lesson 10

- Configuring Network Settings

Lesson 11

- Securing a Linux System

Lesson 12

- Installing Linux

Lesson 13

- Scripting with Bash and Python

Lesson 14

- Managing Containers in Linux

Lesson 15

- Automating Infrastructure Management

- A.0 Linux+ XK0-006 Practice Exams

Informations Pratiques

5 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

GESTION DE PROJET

GESTION DE PROJET

CompTIA Project Management Essentials

Objectifs

- Understand the project life cycle: Explore the phases of a project and the core concepts of project management.
- Project initiation: Learn how to define a project and identify key stakeholders.
- Planning basics: Discover techniques to break down a project into tasks, estimate time and effort, create a timeline, and prepare for risks.
- Execution skills: Assign responsibilities, communicate effectively, monitor progress, and resolve issues as they arise.Project completion: Evaluate results, perform project reviews, and successfully close a project.

Programme

Lesson 1

- Introduction to Project Management

Lesson 2

- Initiating a Project

Lesson 3

- Planning a Project

Lesson 4

- Executing a Project

Lesson 5

- Monitoring and Closing a Project

Informations Pratiques

1 JOUR

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Plus

- Cours animé par un formateur certifié **CompTIA**
- Consultez Programme, l'agenda de prochaines sessions et téléchargez les brochures

EXECUTIVE MBAS

EXECUTIVE MBAs

Cours en ligne, synchrones
Et asynchrones

48 CRÉDITS

12 - 36 MOIS

Anglais & français

Cybersecurity

Audience

Designed for candidates seeking managerial or executive positions in Information Security.

Business Continuity Management

Audience

Designed for candidates seeking managerial or executive positions in Business Continuity.

Governance, Risk and Compliance

Audience

Designed for candidates seeking managerial or executive positions in Risk Management.

Work Experience

A minimum of 2 years of relevant working experience. Although you are not required to have previous experience in business administration, you are expected to have a background on the field in which you are pursuing the Executive MBA program.

ACG | Cybersecurity

ACADEMIC PARTNER

PECB UNIVERSITY
EXISTIMATIO PER VERITATEM

ACG | Cybersecurity

EXPLOREZ LES FORMATIONS D'ACG CYBER ACADEMY POUR TRANSFORMER VOTRE AVENIR

Découvrez l'ensemble de nos formations !

acgcyberacademy.fr

+33 1 89 62 34 30

acgcyberacademy.fr

formation@acgcybersecurity.fr