Catalogue des formations

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

FORMIND

formind
ACADEMY

Sommaire

Bienvenue à la Formind academy

Formind est un cabinet de conseil et d'intégration en Cybersécurité, créé en 2010, dont la mission est simple et belle : protéger ses clients. Nous sommes près de 200 experts, passionnés, animés par des valeurs de rigueur, d'exigence, de partage et d'écoute.

Nous sommes ravis de partager nos connaissances et notre expérience en créant Formind Academy, centre de formation Cybersécurité. Nos formateurs sont enthousiastes, passionnés, expérimentés, certifiés et accrédités !

Avec Formind Academy, nous nous engageons :

RIEN QUE LA CYBERSÉCURITÉ, TOUTE LA CYBERSÉCURITÉ

Tout le monde est concerné ! Ce qui est passionnant avec la cybersécurité, c'est que vous travaillez avec tous les métiers. C'est pour ça que nous proposons une offre complète : de la gouvernance pour la direction et les managers, du juridique pour la protection des données personnelles, et de la technique pour les administrateurs et les spécialistes.

LE PARFAIT DOSAGE ENTRE THÉORIE ET RETOURS D'EXPÉRIENCES PRATIQUES

Halte aux cours standards et insipides ! Bien que nous dispensions des formations certifiantes, nous enrichissons les contenus de nos cours par nos propres études de cas et de nos retours d'expérience. Nous pouvons aller jusqu'à la création d'un cours ex nihilo, 100% adapté à vos besoins spécifiques. Nous comptons de très nombreuses références client.

DES FORMATEURS DE TRÈS HAUT NIVEAU

Ne comptez-pas sur nous pour lire les diapos Powerpoint en cours ! Nos formateurs sont certifiés (ils ont passé le même examen que vous) et accrédités (ils ont été audités et ont obtenu l'autorisation d'enseigner un cours). Leurs capacités pédagogiques sont validées, ainsi que leur maîtrise du contenu et leur capacité à illustrer chaque point par des anecdotes et des exemples réels.

UNE EXPÉRIENCE STIMULANTE

Nos experts parlent à vos experts ! Nous proposons des formations avant-gardistes, surtout en cyber sécurité, où tout retard se paie très cher, ainsi qu'une pédagogie innovante en s'appuyant par exemple sur la réalité Virtuelle. Nos formateurs sont formés aux techniques pédagogiques (inductive, déductive, interactive), pour favoriser la transmission des connaissances et des compétences.
Et nos salles sont très agréables : vous apprécierez nos canapés Chesterfield !

Nous animons des formations partout en France, dans nos locaux ou bien les vôtres !

A bientôt,

Hervé Morizot, Associé

POURQUOI FORMIND ACADEMY ?

Formind Consulting dispose de son propre centre de formation : Formind Academy. L'objectif est double :

- **Former nos propres équipes.** Chez Formind, la formation est essentielle car elle permet à nos équipes d'être toujours à jour, aussi bien sur les techniques ou les produits d'éditeurs, les aspects juridiques que sur les aspects de gouvernance des systèmes d'information.
- **Former vos équipes** ! Nous disposons d'un catalogue très riche de formations en cybersécurité.
  - Nous proposons des formations certifiantes (PECB, ISC2, Isaca), ainsi que des formations sur mesure, complètement adaptées à vos besoins.
  - Notre catalogue compte une soixantaine de références de formation en sécurité de l'information.
  - Nous pouvons inscrire vos collaborateurs dans nos sessions ouvertes à tous, ou bien organiser un cours selon vos disponibilités, en France ou à l'étranger, en français ou en anglais.
  - Nos formateurs sont certifiés (ils ont passé le même examen que vous) et accrédités (ils ont été audités et ont le droit d'enseigner).
  - Nos salles de cours sont accueillantes. Nous avons mis l'accent sur la décoration des salles, chaleureuses et confortables.

95%

des brèches de cybersécurité sont liées à une erreur humaine

Source : Gartner. Why Cloud Security Is Everyone's Business - Smarter With Gartner

80%

des entreprises dans le monde ont été victime de phishing

Source : Baromètre Cesin 6ème édition du baromètre annuel du CESIN - CESIN

60%

La gouvernance est le premier enjeu de demain (60%), suivi par celui de la formation et de la sensibilisation des utilisateurs (56%).

Source : EC Council - 2020

214 jours

en moyenne pour réaliser qu'un malware infecte un système d'information d'entreprise, et 77 jours sont nécessaires pour se remettre complètement d'une attaque informatique

NOTRE OFFRE DE FORMATION

SENSIBILISATION

- Changer les comportements
- Quelques heures

FONDAMENTAUX

- Acquérir les connaissances de base
- 1 ou 2 jours

EXPERT

- Acquérir des compétences
- 3 à 5 jours

NOS ATOUTS

Des formateurs certifiés ET accrédités (audités et autorisés à enseigner)

Nous sommes spécialisés dans la cybersécurité et nous ne nous éparpillons pas !

Des cours enrichis par nos études de cas et expériences terrain

D'une offre standard certifiante à des cours 100% sur mesure

100% de réussite, aux examens sur l'ensemble de nos équipes que nous avons formées (60 candidats en 2020)

Des partenariats avec les leaders : PECB, (ISC)2, Isaca, etc.

NOTRE APPROCHE : UNE DÉMARCHE 100% QUALITÉ

La qualité dans l'analyse et anticipation du besoin

- la bonne formation au bon moment pour répondre aux besoins de l'organisation
- connaître, écouter, comprendre le client
- formuler de manière explicite

La qualité dans la conception

- l'équilibre entre la créativité et les compétences organisationnelles et techniques
- définir les spécifications et spécificités de la formation
- définir et choisir la solution pédagogique : format, workhops, Réalité Virtuelle, etc.

La qualité dans la réalisation

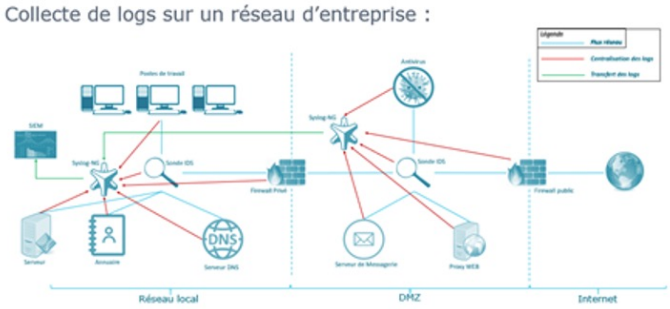
- la maîtrise du contenu et des outils, les retours d'expérience du formateur, son savoir-faire pédagogique
- la performance de la formation
- la maîtrise des coûts et des délais

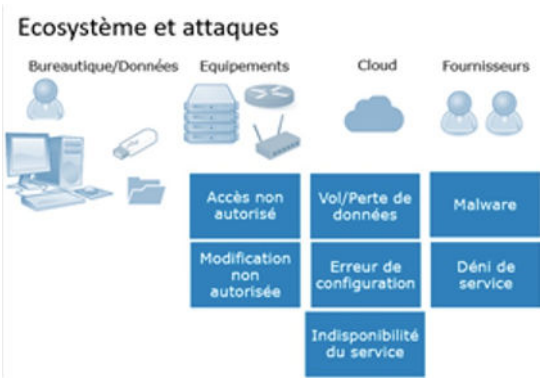
La qualité du feed-back

- service et création de valeur pour l'apprenant
- l'accompagnement, la maintenance et le suivi post formation
- l'épanouissement personnel et professionnel

EXEMPLES DE SUPPORTS

Les stagiaires disposent de supports afin de suivre les présentations, démonstrations, TP, TD et études de cas. Les supports présentent les notions, les démarches, de façon synthétiques et accompagnés de schémas permettant d'avoir une vue de l'ensemble des notions abordées en animation.



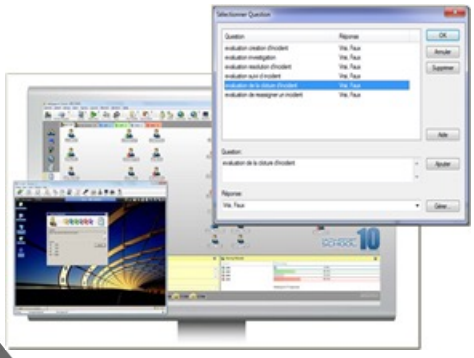


Le pilotage de la qualité

Le pilotage de la qualité s'effectue en 2 temps : l'évaluation à chaud puis à froid. La première relève d'un bilan général, du point de vue sur les évaluations, des remarques sur les moyens mis en œuvre et enfin des suggestions d'amélioration. La seconde vise à évaluer la qualité de l'animation et des supports, l'organisation et les moyens et enfin l'apport de la formation.

Plus particulièrement, l'évaluation à chaud valide l'acquis des connaissances tout au long de la session sur la base d'un questionnaire en ligne personnel :

- En s'appuyant sur le Module de création de QCM d'évaluations d'un outil tel que Net Support School
- Collecte automatique des travaux réalisés par les stagiaires
- A chaque fin de module, l'animateur vérifie que les manipulations ont correctement générées les résultats attendus dans le dossier stagiaire de chaque poste



L'évaluation à froid prend la forme d'un questionnaire envoyé au stagiaire une semaine après avoir commencé à utiliser les connaissances abordées en formation :

- Pour chaque fonction présentée en stage, un QCM sous forme d'images est proposé au stagiaire
- Le principe : retrouver les fonctionnalités, démarches, notions abordées durant la session

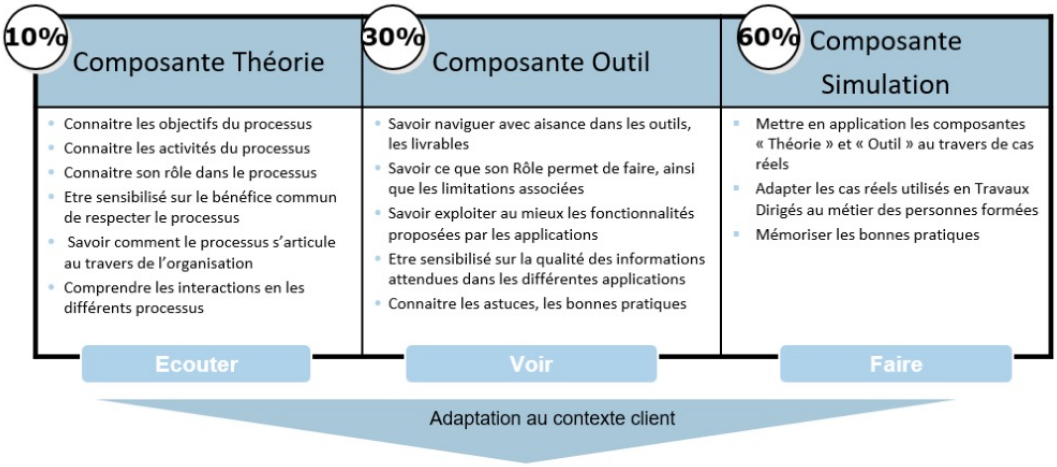
Pour chaque fin de session, **une évaluation à chaud est réalisée** afin de recueillir les éléments de qualité et d'amélioration de la prestation pour les sessions suivantes :

Evaluation de la session par le stagiaire

Evaluation de la session par le formateur

NOTRE APPROCHE PÉDAGOGIQUE

La journée se découpe en 3 temps avec 3 objectifs distincts :



Support de cours formateur

Support à disposition sur clé USB et document imprimé :
- Support identique au stagiaire plus des annotations sur les questions réponses, le timing, les recommandations d'animation

Support stagiaire
(remis en début de session)

Support à disposition sur clé USB et document imprimé :
- Vidéos de démonstration de chacune des fonctions
- Support complet de la journée

Cahier exercice avec corrigé
(remis en fin de session)

Support à disposition sur clé USB et document imprimé :
- Vidéos de démonstration de chacun des exercices
- Support de chacun des exercices avec les corrections

Aide mémoire
(remis en début de session)

Support à disposition sur clé USB et document imprimé :
- Rappel des principales fonctionnalités
- Lexique

NOTRE MÉTHODOLOGIE PÉDAGOGIQUE

Au sein de FORMIND ACADEMY, l'apprenant est le cœur du système. Notre centre de formation propose une démarche inductive à travers laquelle l'apprenant participe activement à des mises en situation, et à des démonstrations animées par des formateurs accrédités.

Nos formateurs sont formés aux techniques pédagogiques (inductive, déductive, interactive), pour favoriser la transmission des connaissances et des compétences. Cette méthodologie positionne l'apprenant dans une pédagogie participative et collaborative. Nous nous appuyons sur des exposés théoriques, des exercices pratiques, l'application des concepts au sein de logiciels du marché, ou des matrices de type Excel. Nous créons également nos propres méthodes et outils pédagogiques lors de formations sur mesure (workshops, Capture the Flag, etc.)

Modalités et délais d'accès

L'accès à nos formations peut été initié, soit par l'employeur, soit à l'initiative du salarié avec l'accord de ce dernier, soit à l'initiative propre du salarié.

- Pour chaque demande de formation, notre service réalise sous 8 j un entretien téléphonique afin d'établir une formation personnalisée qui prend en compte les attentes, les préférences et les contraintes du prospect. Une politique de prévention de la violence dans leur(s) établissement(s) peut-être également proposée. Lors de cet entretien, les modalités de déroulement et de sanction de la formation, le ou les objectifs, les connaissances et les compétences acquises, les sources de financement, etc..., sont précisés.
- Une proposition commerciale (hors subrogation OPCO) est transmise sous 8 jours, un programme adapté ainsi qu'une fiche client, qui permet de faciliter les échanges administratifs.
- A réception du devis signé l'organisation logistique, technique, pédagogique et financière est établie lors des divers échanges avec notre service formation et le commanditaire. Le devis est valable 30 jours.
- Le délai d'accès aux formations, tient compte de ces différentes formalités afin d'être accessible dans un temps minimum d'un mois avant le début de l'action.

Modalité d'accès pour les PSH

Modalité d'accès pour les personnes en situation de handicap (PSH) .

Nous veillons au respect des conditions d'accueil des Publics concernés et étudions au cas par cas toutes les situations de handicap afin d'envisager une intégration dans la formation. Si vous êtes en situation de handicap, nous trouverons des solutions pour vous accueillir. Nos formations peuvent être adaptées aux différentes situations de handicap (cf. procédure d'accueil des personnes en situation de handicap). Nous sommes à votre disposition pour étudier les adaptations nécessaires à votre besoin.
Merci de nous écrire à formation@formind.fr

Contact Référent handicap :
Laurence PERTUIS
Laurence.pertuis@formind.fr

NOTRE MÉTHODOLOGIE D'EVALUATION

1. Avant la formation

Tout d'abord, avant même d'entamer le processus de formation, il s'agit d'évaluer vos besoins spécifiques. D'ailleurs, les entretiens annuels ou entretiens professionnels (qui eux ont lieu tous les deux ans) aideront à mettre en avant vos besoins prioritaires.

Ensuite une évaluation des prérequis est effectuée dans le but d'avoir à l'esprit sa marge de progrès et ainsi faciliter la mesure du chemin parcouru avant et après la formation.

Pour ce faire, rien de plus efficace qu'un test de connaissances en amont ou bien un entretien avec le formateur.

2. Pendant la formation

Tout au long de la formation et ce, quelle qu'en soit la durée, le formateur valide la compréhension de même que l'acquisition de vos connaissances. La plupart des formateurs utilisent dans ce contexte des tests ou des jeux de mise en situation. Ils confirment donc, la compréhension et facilitent la mémorisation de l'apprentissage sur le long terme.

3. A l'issue de la formation

A la fin de chaque formation, il est crucial de prévoir un outil de mesure de la satisfaction des participants sur tous les éléments du dispositif tels que le contenu, la méthode du formateur, ses compétences pédagogiques, l'organisation du cursus...

En effet, ce retour d'expérience peut être fait de façon orale, en prévoyant un tour de table par exemple, ou bien de façon individuelle et écrite, notamment en distribuant des questionnaires en fin de formation).

Les outils les plus fréquemment utilisés restent les quizz, les questionnaires vrai-faux, ou encore les questionnaires d'auto-évaluation avant-après.

4. Quelques mois après avoir terminé la formation

Trois à six mois après la formation, il est nécessaire de mesurer son impact en situation professionnelle de l'apprenant. On parle d'évaluation à froid.

Plusieurs méthodes peuvent être utilisées pour évaluer cette étape :

- Une grille d'analyse de l'évolution des comportements à la suite de la formation
- Une analyse de l'évolution des objectifs individuels
- De l'efficacité et de l'efficience du salarié à son poste
- Une analyse de l'évolution des indicateurs de performance.

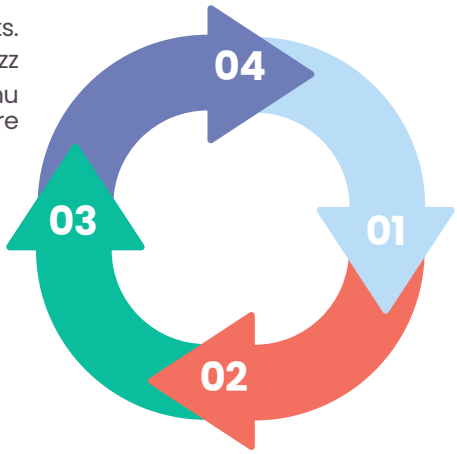
NOTRE DÉMARCHE DE CONCEPTION D'UNE FORMATION PERSONNALISÉE

ANALYSE

Analyse en besoin de montées en compétences

Définition des profils et matrices de compétences

Proposition d'accompagnement et de planning



CONSTRUCTION / ADAPTATION DU CONTENU

Atelier de travail

Construction des supports

Adaptation des messages

SESSIONS DE FORMATION

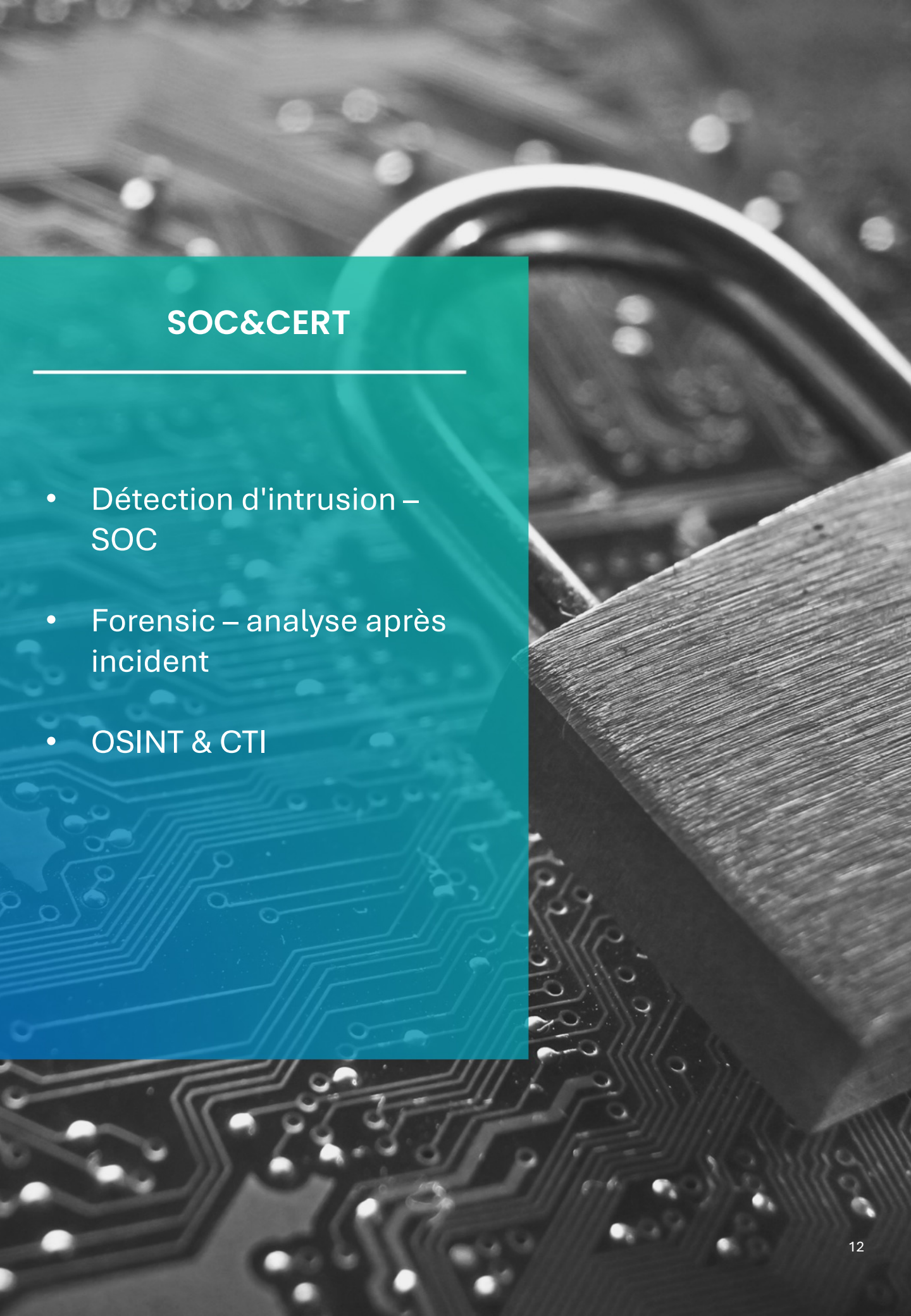
Animation des sessions de formation

CONTRÔLE

Suivi des retours des participants.

Suivi des résultats aux quizz

Nouvelles adaptations du contenu si nécessaire



SOC&CERT

- Détection d'intrusion – SOC
- Forensic – analyse après incident
- OSINT & CTI

Détection d'intrusion - SOC

Pourquoi choisir cette formation :

Elle offre une vision opérationnelle et concrète du fonctionnement d'un SOC, de la détection à la gestion des incidents, en s'appuyant sur les SIEM, la CTI et des cas d'usage réalistes. Grâce à des scénarios proches du réel (APT, ransomware), elle permet de développer des compétences directement exploitables par un analyste SOC.

Modalités

Durée	Langues	Niveau	
5 jours	Français Anglais	Expert	50% De pratique

Objectifs pédagogiques

- Appréhender les enjeux de la sécurité informatique
- Connaitre les différentes menaces cyber
- Comprendre les mécanismes de défense et de protection
- Détecter et qualifier les alertes de sécurité
- Analyser les incidents de sécurité
- Adopter une démarche proactive de la détection
- Évaluer la maturité de son service

Pour qui ?

- Analyste cybersécurité
- Analyste SOC N1 / N2 / N3
- Analyse Threat Detection / Threat Hunting
- Membre d'un CSIRT
- Administrateur & ingénieur techniques
- Analyste CTI
- RSSI
- Responsable SOC

Programme

J1	J2	J3	J4	J5
Introduction à la détection d'intrusion	Détection d'incident de sécurité avec un SIEM	Mise en œuvre de la stratégie de détection et traitement des alertes	Comprendre les menaces, les acteurs, les IOC, et les méthodologies	Etude de cas Scénario de compromission

Prérequis

- Connaissances de base en architecture réseau (protocoles, topologies)
- Familiarité avec les principes de sécurité des systèmes d'information

Forensic – Analyse après incident

Pourquoi choisir cette formation :

Elle apporte une approche méthodologique et opérationnelle de l'investigation numérique, de l'acquisition des preuves à leur analyse et leur restitution, dans le cadre de la réponse à incident.
Basée sur des standards reconnus et des scénarios réalistes, elle permet de développer des compétences forensic directement applicables sur le terrain.

Modalités

Durée	Langues	Niveau	
5 jours	Français Anglais	Expert	50% De pratique

Objectifs pédagogiques

- Comprendre les concepts essentiels de la réponse à incident et de l'investigation forensic.
- Acquérir les compétences nécessaires pour gérer et résoudre les incidents de sécurité.
- Apprendre les pratiques pour collecter, analyser et présenter des preuves numériques.
- Connaitre les phases clés de la réponse à incident.

Pour qui ?

- Analyste cybersécurité
- Analyste SOC N1 / N2 / N3
- Analyse Threat Detection / Threat Hunting
- Membre d'un CSIRT
- Administrateur & ingénieur techniques
- Analyste CTI
- RSSI
- Responsable SOC

Programme

J1	J2	J3	J4	J5
La réponse à incident et ses standards	L'acquisition de preuves et les techniques	Les artefacts et les techniques d'analyse	Analyse de fichiers malveillants	Formalisations des analyses

Prérequis

- Connaissances fondamentales en systèmes d'exploitation (Windows/Linux)
- Connaissances de base en architecture réseau (protocoles, topologies)
- Familiarité avec les principes de sécurité des systèmes d'information
- Être familiarisé avec les environnements de virtualisation (VMware, VirtualBox)

OSINT & CTI

Pourquoi choisir cette formation :

Elle propose une approche complète et opérationnelle du Cyber Threat Intelligence et de l'OSINT, des fondements du renseignement jusqu'à la production de livrables actionnables.
Les participants développent des compétences concrètes de collecte, d'analyse et d'enrichissement des données, en intégrant les enjeux d'OPSEC, de conformité et de gouvernance.

Modalités

Durée
5 jours

Langues
Français
Anglais

Niveau
Expert

50%
De pratique

Objectifs pédagogiques

- Comprendre les fondements du renseignement
- Appliquer des modèles d'analyse CTI
- Mener des opérations OSINT structurées et sécurisées
- Exploiter et enrichir des données techniques et contextuelles
- Produire un renseignement actionnable
- Intégrer les dimensions juridiques, de gouvernance et de veille

Pour qui ?

- Analyste cybersécurité
- Analyste SOC / CERT / CSIRT
- Analyste CTI / Threat Intelligence
- Responsables sécurité
- Analyste OSINT / investigation numérique
- Ingénieur sécurité, blue team, threat hunters
- Personnels impliqués dans la veille stratégique, gestion des risques, ou cybersécurité opérationnelle

Programme

J1 — Fondamentaux du renseignement et de la CTI

J2 — Collecte OSINT : sources, outils, pivoting et OPSEC

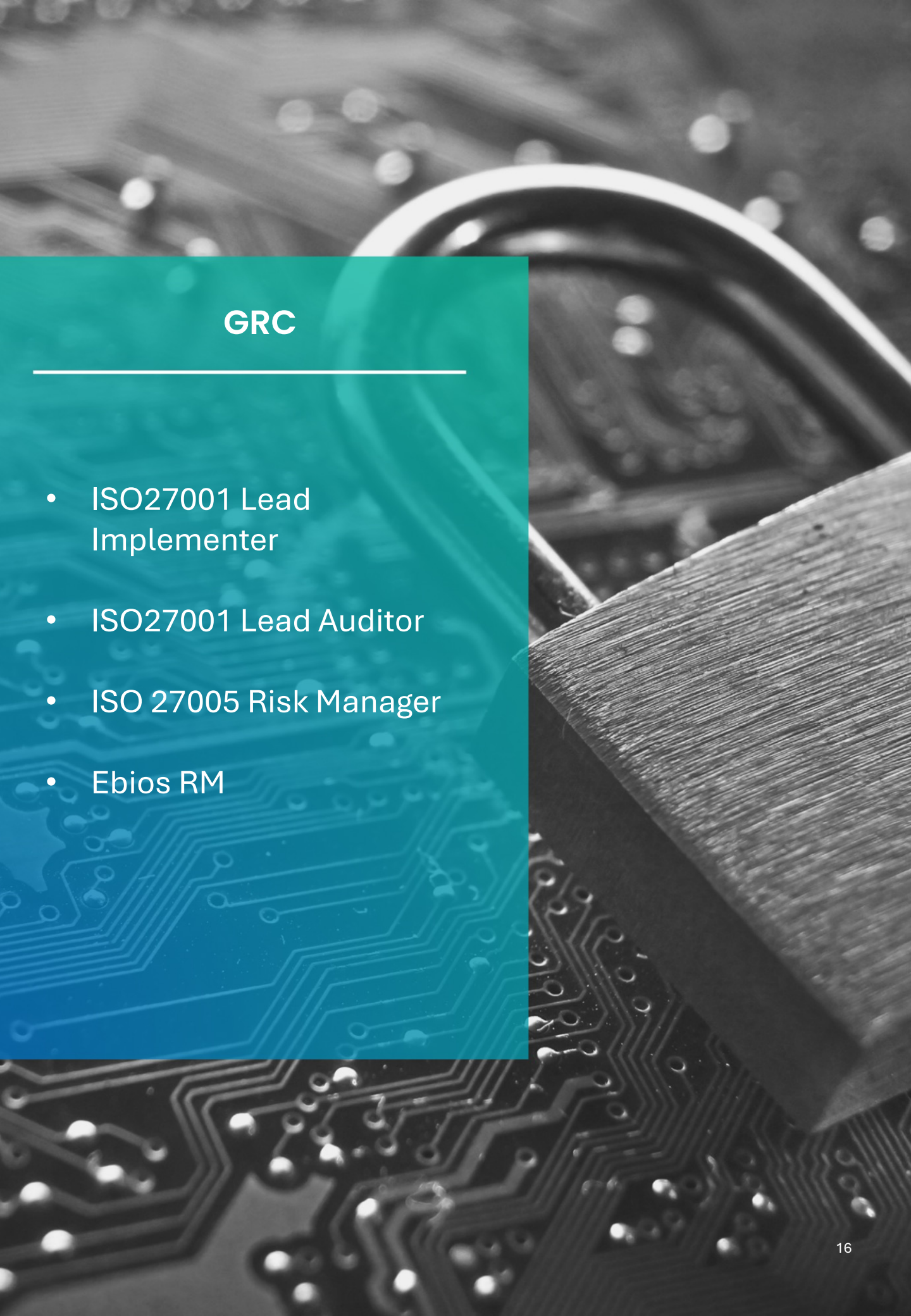
J3 — Données, logs, enrichissement massif et pivot vers l'attribution

J4 — Production CTI, outillage TIP, détection & automatisation

J5 — Cas pratique, droit, gouvernance et veille stratégique

Prérequis

- Connaissances de base en cybersécurité (réseaux, systèmes, menaces courantes).
- Compréhension générale des environnements IT / SOC.
- Notions préalables en analyse d'incidents, investigation numérique ou sécurité opérationnelle appréciées.
- Aisance avec les outils informatiques et les sources en ligne.



GRC

- ISO27001 Lead Implementer
- ISO27001 Lead Auditor
- ISO 27005 Risk Manager
- Ebios RM

ISO 27001 Lead Implementer

Certification

PECB AUTHORIZED GOLD PARTNER

Examen
3h
Format QCM

Obtention
70%

Modalités

Durée
5 jours

Langues
Français
Anglais

Niveau
Expert

Objectifs pédagogiques

- Comprendre les liens entre ISO 27001, ISO 27002 et autres cadres.
- Maîtriser les méthodes pour mettre en œuvre et gérer un SMSI.
- Interpréter les exigences ISO 27001 selon le contexte de l'organisation.
- Accompagner l'organisation dans tout le cycle de vie du SMSI.
- Conseiller sur les meilleures pratiques de sécurité de l'information.
- Préparer l'examen ISO 27001 LI.

Pour qui ?

- Experts de la sécurité de l'information et de l'audit
- Tous les professionnels qui évaluent, conçoivent, déploient, supervisent et optimisent la sécurité de l'information avec les mesures de sécurité associées
- DSI, RSI, RSSI, Chief Digital Officier
- Consultants Auditeurs IT / IS, tous professionnels du contrôle, de l'assurance, de la gestion des risques et de la sécurité de l'information

Programme

J1 — Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

J2 — Planification de la mise en œuvre d'un SMSI

J3 — Mise en œuvre d'un SMSI

J4 — Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

J5 — Examen de certification

Domaines adressés

- Principes et concepts fondamentaux du Système de management de la sécurité de l'information
- Système de management de la sécurité de l'information
- Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001
- Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001
- Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001
- Amélioration continue d'un SMSI selon la norme ISO/CEI 27001
- Préparation de l'audit de certification d'un SMSI

Prérequis

- Bonne compréhension des concepts de sécurité de l'information
- Connaissance ou expérience dans la gestion de processus ou de projets
- Connaissance ou expérience en projet sécurité, conformité ou qualité

ISO 27001 Lead Auditor

Certification

PECB AUTHORIZED GOLD PARTNER

Examen
3h
Format QCM

Obtention
70%

Modalités

Durée
5 jours

Langues
Français
Anglais

Niveau
Expert

Objectifs pédagogiques

- Comprendre le fonctionnement d'un SMSI conforme à la norme ISO 27001.
- Expliquer la corrélation entre la norme ISO 27001 et 27002.
- Comprendre le role d'un auditeur (planifier, diriger et assurer le suivi d'un audit).
- Savoir diriger un audit et une équipe d'audit ISO 27001.
- Acquérir les compétences d'un auditeur.
- Préparer l'examen ISO 27001 LA.

Pour qui ?

- Auditeurs souhaitant réaliser et diriger des audits de certification du SMSI
- Responsables ou consultants désirant maitriser le processus d'audit du SMSI
- Toute personne responsable du maintien de la conformité aux exigences du SMSI

Programme

J1 — Introduction au SMSI et à la norme ISO/CEI 27001

J2 — Principes, préparation et déclenchement de l'audit

J3 — Activités d'audit sur site

J4 — Clôture de l'audit

J5 — Examen de certification

Domaines adressés

- Principes et concepts fondamentaux du Système de management de la sécurité de l'information
- Système de management de la sécurité de l'information (SMSI)
- Principes et concepts fondamentaux de l'audit
- Préparation d'un audit ISO/CEI 27001
- Réalisation d'un audit ISO/CEI 27001
- Clôturer un audit ISO/CEI 27001
- Gérer un programme d'audit ISO/CEI 27001

Prérequis

- Principe de la sécurité de l'information
- Concepts de gestion de risques
- Fonctionnement général d'un SI
- Gouvernance et organisation
- Une connaissance préalable de la norme ISO 27001 est fortement recommandée

ISO 27005 Risk Manager

Certification

PECB AUTHORIZED GOLD PARTNER

Examen
1h
Format QCM

Obtention
70%

Modalités

Durée
3 jours

Langues
Français
Anglais

Niveau
Confirmé

Objectifs pédagogiques

- Comprendre le cadre normatif et méthodologiques
- Définir le contexte et le périmètre de gestion des risques
- Identifier et analyser les risques SSI
- Evaluer et prioriser les risques
- Définir et piloter le traitement des risques
- Acquérir les connaissances pour communiquer, documenter et décider
- Assurer la surveillance et l'amélioration continue

Pour qui ?

- Risk Manager SSI
- RSSI / RSSI adjoint
- Consultant GRC / cybersécurité
- Auditeur SSI / conformité
- Responsable gouvernance ou contrôle interne
- Chef de projet sécurité ou conformité
- Architecte sécurité impliqué dans l'analyse des risques

Programme

J1 — Fondamentaux et cadre de gestion des risques

J2 — Appréciation et traitement des risques

J3 — Examen de certification

Domaines adressés

- Principes et concepts fondamentaux
- Mise en œuvre d'un cadre de gestion des risques
- Appréciation des risques SSI
- Traitement et acceptation des risques
- Surveillance, revue et amélioration

Prérequis

- Connaissance de base en sécurité des SI
- Connaissances normatives recommandées (ISO 27001, 27005)
- Expérience professionnelle recommandée (gestion des risques, gouvernance, audit, analyse de risques)

EBIOS RM

Certification

PECB AUTHORIZED GOLD PARTNER

Examen
3h
Format QCM

Obtention
70%

Modalités

Durée
3 jours

Langues
Français
Anglais

Niveau
Confirmé

Objectifs pédagogiques

- Comprendre les concepts et principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Comprendre les étapes de la méthode EBIOS
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
- Acquérir les compétences nécessaires pour gérer les risques de sécurité
- Acquérir les compétences nécessaires afin de mener une étude EBIOS
- Savoir analyser et communiquer les résultats d'une étude EBIOS

Pour qui ?

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

Programme

J1
Introduction et mise en contexte de la méthode EBIOS

J2
Approfondissement des étapes d'analyse

J3
Examen de certification

Domaines adressés

- Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information selon la méthode EBIOS
- Programme de gestion des risques liés à la sécurité de l'information basé sur EBIOS
- Appréciation des risques liés à la sécurité de l'information basée sur la méthode EBIOS

Prérequis

- Bonnes compétences en sécurité des systèmes d'information
- Connaissances méthodologiques recommandées : ISO 27001, ISO 27005
- Expérience professionnelle recommandée : Gestion des risques, Gouvernance, audit, démarche ISO, NIS, RGPD

Sécurité opérationnelle

- Sécurité des réseaux

Sécurité des réseaux

Pourquoi choisir cette formation :

Elle offre une vision globale et structurée de la cybersécurité, des fondamentaux et des menaces actuelles jusqu'à l'identification des vulnérabilités et la réponse aux attaques. En combinant théorie, méthodologie de l'attaquant et ateliers pratiques, elle permet d'acquérir les bases essentielles pour prévenir, détecter, analyser et réagir efficacement aux incidents de sécurité.

Modalités

Durée	Langues	Niveau	30%
3 jours	Français Anglais	Débutant	De pratique

Objectifs pédagogiques

- Comprendre les fondamentaux de la cybersécurité
- Acquérir des bases en sécurité et en sécurité des réseaux
- Connaitre la méthodologie d'un attaquant
- Pouvoir identifier des vulnérabilités
- Connaitre les mesures à appliquer pour prévenir ces attaques
- Connaitre les bonnes pratiques d'administration
- Savoir détecter, analyser puis réagir à des incidents de sécurité courants

Pour qui ?

- Administrateurs systèmes et réseaux
- Techniciens et ingénieurs IT
- Analystes SOC débutants
- Responsable ou correspondants sécurité
- Chefs de projet techniques
- Toute personne souhaitant acquérir une vision structurée et opérationnelle de la sécurité des systèmes d'information

Programme

J1

Introduction à la sécurité : menaces, enjeux, risques, méthodologie

J2

Savoir identifier des vulnérabilités : pentest, audits, étape d'une attaque, techniques d'intrusion et d'exfiltration

J3

Administrer, détecter, analyser et réagir aux attaques

Prérequis

- Culture informatique générale (systèmes, réseaux, usage professionnel de l'IT).

MERCI

FORMIND

NOUS CONTACTER

formation@formind.fr

Possibilité d'inscription en ligne :

https://www.formind.fr/formation/

Formind

7 chemin de Bretagne
92130 Issy-les-Moulineaux

formind ACADEMY