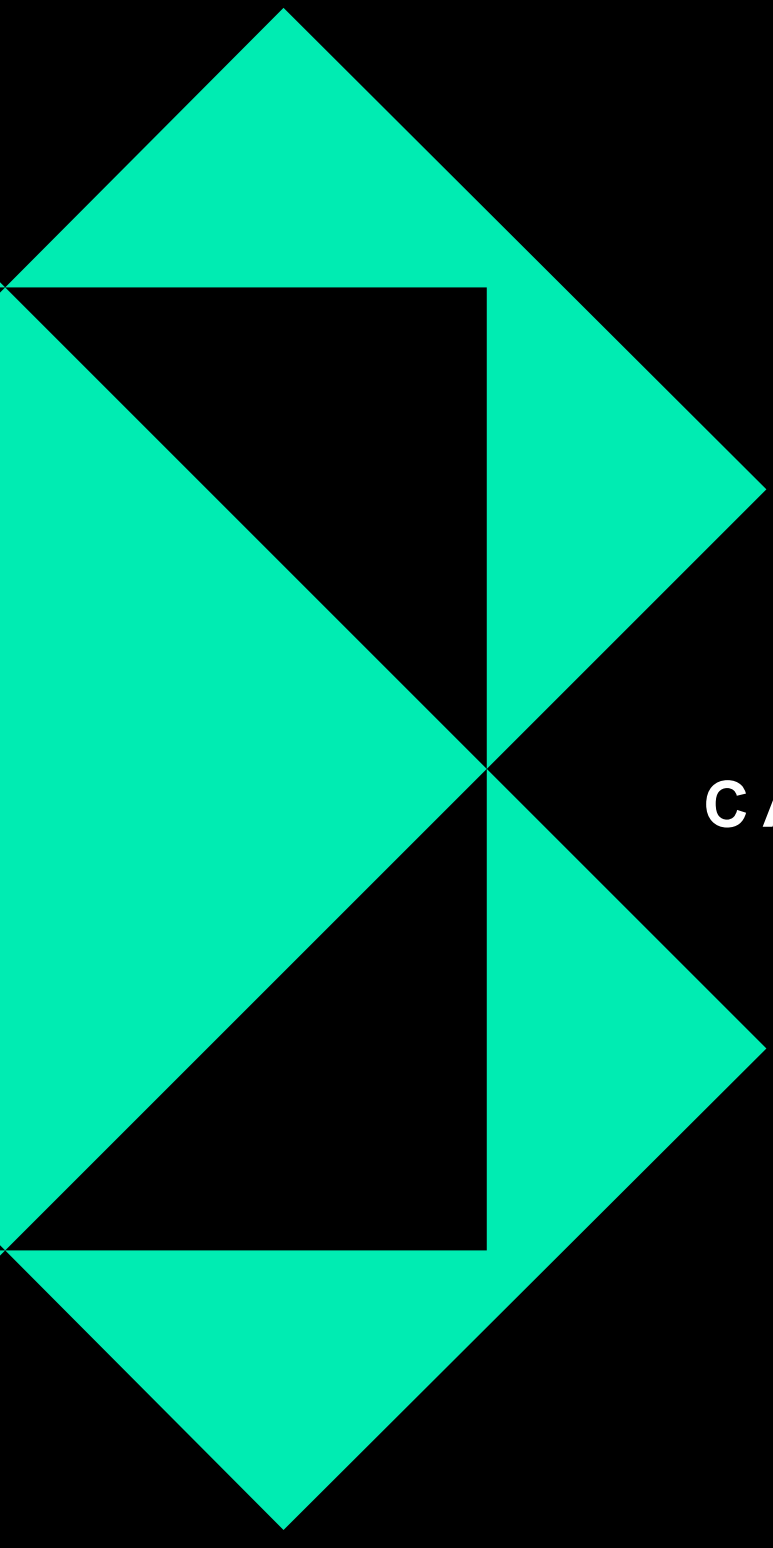
CHOISIR DE SE FORMER AUTREMENT



CATALOGUE DE FORMATION

almond
INSTITUTE

Almond
INSTITUTE

Organisme de formation agréé, Almond Institute fournit des actions pédagogiques conçues et dispensées par des experts dans les domaines de la Cybersécurité, du Cloud et des Infrastructures. Forts de leur expérience et des différentes situations auxquelles ils sont confrontés quotidiennement, les formateurs savent rendre parlant des sujets techniques à tout public tout en offrant à leur apprenant une vision 360° d'un sujet.

Alliant théorie, retours d'expérience, cas pratiques, mises en situation, pédagogie inversée, et échanges avec un expert, Almond Institute s'appuie sur des techniques pédagogiques diverses et variées pour construire ses actions pédagogiques et s'adapter aux besoins de ses apprenants.

Nos offres

01.
FORMATION
Développez les compétences et favorisez l'épanouissement professionnel de vos collaborateurs avec nos formations adaptées à leur profil.

02.
SENSIBILISATION
Protégez votre entreprise et sensibilisez efficacement vos équipes aux risques cyber en optant pour les moyens les plus adaptés à votre contexte et vos objectifs.

03.
E-LEARNING BYCE
Déployez votre campagne de sensibilisation en un temps record et faites de vos utilisateurs le maillon fort de votre sécurité avec notre plateforme.

04.
COACHING
Surmontez les défis et accompagnez vos collaborateurs dans l'atteinte de leurs objectifs professionnels grâce à un accompagnement personnalisé.

Notre démarche qualité

Nous sommes certifiés QUALIOPI depuis le 6 janvier 2022. Cette certification démontre notre engagement sur la qualité, la fiabilité et la pertinence des actions de formation délivrées à nos apprenants.

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

Almond INSTITUTE

Nos chiffres clés de 2023

381
Stagiaires formés

95%
Taux de réussite aux certifications

71%
Taux de session « sur-mesure »

29%
Taux de session « au catalogue »

86%
Taux de satisfaction des stagiaires

Miora RAHARINIRINA
Chargée de mission Formation

“

Chez Almond Institute, notre priorité est de fournir à nos clients des formations de qualité, conçues et animées par des experts passionnés dans les domaines de la cybersécurité, du cloud et des infrastructures. Axée sur la personnalisation et la progression, notre démarche pédagogique intègre sensibilisation, formation et coaching pour permettre à chaque utilisateur de votre système d'information de devenir un acteur conscient et compétent. Grâce à cette approche flexible et adaptée, nous garantissons des solutions sur mesure qui offrent des réponses concrètes aux défis rencontrés par nos clients.

”

almond
INSTITUTE

Vous souhaitez :

01. **Affronter les nouveaux enjeux stratégiques IT ?**

02. **Anticiper les cyber réalités à venir et avoir un temps d'avance ?**

03. **Dépasser vos acquis et envisager des projets jusqu'alors jamais appréhendés ?**

Nous avons la solution pédagogique adaptée à votre besoin !

Nos engagements

Sortir des sentiers battus avec des formats variés et une pédagogie innovante

Transmettre notre passion par nos experts sur nos expertises

Soigner l'expérience utilisateur en valorisant la convivialité et la qualité

SOMMAIRE

LES FORMATIONS EN SÉCURITÉ TECHNIQUE

Les techniques du développement informatique sécurisé

Les objectifs pédagogiques

01. Connaître **les principales failles** liées aux applications web (Top 10 OWASP).

02. Savoir détecter **la présence des failles présentées.**

03. Acquérir les **bonnes pratiques de développement.**

Programme

- Introduction (contexte, OWASP, Matrice MITRE ATT&CK)
- 1e phase de test (authentification, HTTP, RCE, XSS, etc.)
- 2e phase de test (Type Juggling PHP, Log froging, etc.)

Prérequis

Connaissance basique des environnements web :

- 1 langage web : PHP, JAVA, ASP .NET, Python, etc.
- 1 langage de base de données : SQL et/ou NoSQL
- 1 système d'exploitation : Linux et/ou Windows

Présentiel ou distanciel

Durée
2 jours
(14 heures)

Public

- Développeurs d'applications web, quelle que soit la technologie utilisée.

En savoir plus

“S’ENTRAÎNER AVEC LES OUTILS DES ATTAQUANTS POUR MIEUX DÉJOUER LEURS ATTAQUES

Jérôme SIMON
Ethical Hacker
Formateur en sécurité technique

Mon profil formateur

Sécurité d’un réseau interne basé sur Active Directory

Les objectifs pédagogiques

01. Connaître **les principales failles** liées aux réseaux internes basés sur Active Directory.

02. **Savoir détecter** la présence des failles présentées.

03. **Acquérir les bonnes pratiques** de sécurité d’administration.

Programme

- Introduction
- Protocoles d’authentification
- Obtenir un premier compte de domaine
- Obtenir les droits d’administrateur local sur des machines
- Élever ses privilèges sur le domaine
- Attaquer des relations d’approbation

Prérequis

- Notions de base en : réseau (protocoles, modèle OSI, etc.), environnement Active Directory, Système d’exploitation Windows

Présentiel ou distanciel

Durée
(3 jours)

Public

- Équipes d’administrateurs systèmes et réseaux
- Équipes de sécurité des systèmes d’information
- Équipes support utilisateurs

En savoir plus

Les techniques de réponse à incidents et d'analyse forensique dans le cadre du standard PCI-DSS

Les objectifs pédagogiques

01. **Sensibiliser les équipes IT** aux bonnes pratiques de réponse à incident.

02. **Présenter les techniques couramment utilisées** par les CERT pour délimiter le périmètre, identifier le mode opératoire et les TTP des attaquants.

03. **Détailler les bonnes pratiques à adopter** pour collecter, analyser les preuves techniques permettant de comprendre la séquence des évènements et la KillChain dans le respect du standard PCI-DSS.

Programme

- Introduction
- Cycle de vie d'un incident
- Rôle du CERT
- Collecte de preuves
- Analyse d'artefacts et timeline
- Travail collaboratif
- Synthèse des résultats

Prérequis

- Notions de base en informatique : réseau (protocoles, modèle OSI, etc.) et système (Linux ou Windows, gestion d'un serveur, etc.)

Présentiel ou distanciel

Durée
3 jours
(21 heures)

Public

- Équipes IT
- RSSI
- Équipes support
- Administrateurs système
- Administrateurs réseau

En savoir plus

LES FORMATIONS EN CONFORMITÉ

Certification ISO 27001 - Foundation

Les objectifs pédagogiques

01. Comprendre **la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI)** conforme à l'ISO 27001.

02. Connaître les **concepts, démarches, normes et méthodes** permettant de gérer efficacement un SMSI.

03. Comprendre **la relation entre un SMSI et la conformité aux exigences des différentes parties prenantes d'une organisation.**

04. Acquérir les connaissances nécessaires pour **contribuer à la mise en œuvre d'un SMSI** tel que spécifié dans l'ISO 27001.

Programme

- Introduction
- Mettre en œuvre des mesures de sécurité de l'information conformes
- Conduire un audit de certification ISO 27001

Prérequis

- Avoir des connaissances de base en sécurité de l'information.

Public

- Membres d'une équipe de sécurité de l'information
- Professionnels des SI souhaitant acquérir une compréhension globale des principaux processus d'un SMSI
- Personnel impliqué dans la mise en œuvre de la norme ISO 27001
- Techniciens impliqués dans les opérations liées à un SMSI
- Auditeurs
- Responsables et cadres supérieurs en charge de la gouvernance des TI d'une organisation et de la gestion de ses risques

Présentiel ou distanciel

Durée
2 jours
(14 heures)

En savoir plus

Certification ISO 27001 - Lead Implementer

Les objectifs pédagogiques

01. Comprendre les **concepts, approches, méthodes et techniques** utilisés pour la mise en œuvre et le management efficace d'un SMSI.

02. **Comprendre la corrélation entre les normes ISO/IEC 27001, ISO/IEC 27002** et d'autres normes et cadres réglementaires.

03. **Comprendre le fonctionnement d'un SMSI** et ses processus conformément à la norme ISO/IEC 27001.

04. Apprendre à interpréter et à **mettre en œuvre les exigences d'ISO/IEC 27001** dans le contexte spécifique d'un organisme.

Programme

- Introduction
- Planification est mise en place d'un SMSI basé sur l'ISO 27001
- Audit de certification d'un SMSI

Prérequis

- Avoir une connaissance de la norme ISO/CEI 27001 et avoir une bonne connaissance de la sécurité des systèmes d'information.

Public

- Chefs de projet ou consultants qui souhaitent préparer et assister une organisation dans la mise en œuvre de son SMSI
- Auditeurs ISO 27001 qui souhaitent comprendre le processus de mise en œuvre SMSI
- Les responsables et cadres supérieurs en charge de la gouvernance des TI d'une entreprise et de la gestion de ses risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologies de l'information
- Experts techniques souhaitant se préparer à occuper une fonction en sécurité de l'information ou en gestion de projet SMSI

Présentiel ou distanciel

Durée
5 jours
(35 heures)

En savoir plus

Certification ISO 27001 - Lead Auditor

Les objectifs pédagogiques

01. Acquérir l'expertise pour réaliser un **audit interne ISO 27001 suivant les lignes directrices ISO 19011.**

02. Acquérir l'expertise pour **gérer une équipe d'auditeurs de SMSI.**

03. **Comprendre le fonctionnement d'un SMSI** selon l'ISO 27001.

04. **Améliorer la capacité d'analyse** de l'environnement interne et externe d'une organisation, d'évaluation des risques d'audit et de prise de décision dans le contexte d'un audit SMSI.

Programme

- Modèle normatif ISO et système de management
- Planifier, initialiser et conduire l'audit de certification

Prérequis

- Avoir une connaissance de la norme ISO/CEI 27001 et avoir une bonne connaissance de la sécurité des systèmes d'information.

Public

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

Présentiel ou distanciel

Durée
5 jours
(35 heures)

En savoir plus

“LA FORMATION EST L’INTENTION DE COMPRENDRE POUR CHANGER LES CHOSES AVEC DU SENS !

Aurélien BARRAUD
Manager Governance, Risks & Compliance
Formateur en conformité

Mon profil formateur

Certification ISO HDS Foundation

Les objectifs pédagogiques

01. **Comprendre les enjeux d'un système de management HDS** pour protéger efficacement les données de santé.

02. **Acquérir la terminologie et les connaissances** de base nécessaires pour répondre aux exigences de l'ISO 27001 associées à l'ISO 20000.

03. **Découvrir les bonnes pratiques de management** de la sécurité de l'information et des données de santé et son articulation avec la gestion des risques.

Programme

- Hébergement de données de santé
- Démarche de certification
- HDS – exigences et preuves

Prérequis

- Avoir des connaissances de base en sécurité de l'information
- Avoir des connaissances sur la protection des données et des données de santé

Public

- 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 HDS
- Personnes souhaitant poursuivre une carrière dans le management HDS

En distanciel

Durée
2 jours
(14 heures)

En savoir plus

Maîtriser PCI DSS v4.0 et ses exigences

Les objectifs pédagogiques

01. Comprendre **les risques de vols de données CB.**

02. **Comprendre** les standards, les exigences et comment utiliser PCI DSS.

03. Comprendre **le périmètre à protéger.**

04. Éclairer les **équipes projets PCI DSS.**

Programme

- L'essentiel du standard PCI DSS
- Réussir son projet de mise en conformité
- Maîtriser les exigences

Prérequis

- Aucun prérequis

Présentiel ou distanciel

Public

- Directeurs, RSSI, DSI, Directeurs financiers, Acheteurs, Juristes, Direction des ressources humaines…
- Chefs de projets PCI DSS, Correspondants Sécurité, Auditeurs, Architectes techniques, Exploitants…

Durée
3 jours
(21 heures)

En savoir plus

LES FORMATIONS EN RISQUES

Les fondamentaux du risque

Les objectifs pédagogiques

01. **Comprendre ce qu'est un risque** et savoir l'évaluer.

02. **Différencier** le risque de sécurité de l'information du risque de sécurité des systèmes d'information.

03. **Appréhender les enjeux** de la gestion des risques.

04. **Se repérer dans la documentation** existante (normes et méthodologies).

Programme

- Panorama des principales menaces actuelles
- Comprendre les risques de sécurité de l'information et des systèmes d'information
- La gestion de risques

Prérequis

- Connaissances générales des systèmes d'information

Public

Toute personne souhaitant apprendre plus sur la gestion des risques en général et la gestion des risques de sécurité de l'information en particulier :

- Personnes responsables de la sécurité de l'information ou de la conformité au sein d'une organisation
- Gestionnaires des risques
- Chefs de projet
- Membres d'une équipe de sécurité de l'information
- Consultants en technologie de l'information

Présentiel ou distanciel

Durée
8 heures

En savoir plus

Coordination SSI - « Faire vivre la PSSI dans le cadre de la gestion des risques »

Les objectifs pédagogiques

01. **Déployer la PSSI** dans le cadre de la gestion globale des risques de l'entreprise.

02. **Mettre à jour la PSSI** pour prendre en compte des nouvelles menaces.

03. Mettre en place des moyens de mesure de **l'implémentation et du respect de la PSSI.**

Programme

- Le RSSI face aux risques
- Définir, déployer et mettre à jour la PSSI
- Mesurer et améliorer l'implémentation de la PSSI

Prérequis

- Connaissances générales des systèmes d'information
- Connaissances générales en gestion des risques
- Connaissances générales en sécurité des systèmes d'information

Public

- RSSI
- Risk Managers
- DSI
- Chefs de projet (techniques et/ou fonctionnels)
- Directeurs de programme

Présentiel ou distanciel

Durée
7 heures

En savoir plus

“LE PARTAGE EST L’UNE DES CLEFS DE L’APPRENTISSAGE

Albane GIROLLET
Consultante Governance, Risks & Compliance
Formatrice en risques

Mon profil formateur

Certification EBIOS Risk Manager

Les objectifs pédagogiques

01. **Comprendre les concepts, les enjeux et les principes de base** en gestion du risque liés à l'utilisation de la méthode EBIOS Risk Manager.

02. Comprendre les activités de la méthode EBIOS Risk Manager **de manière à suivre la réalisation d'analyse de risques en tant que maîtrise d'ouvrage.**

03. **Comprendre les conclusions** d'une étude EBIOS Risk Manager et ses principaux livrables.

04. Passer un examen de certification **pour valider les acquis** de la formation et être certifié « PECB EBIOS Risk Manager ».

Programme

- Introduction
- Cadrage et socle de sécurité
- Sources de risques
- Scénarios stratégiques et opérationnels
- Traitement des risques

Prérequis

- Connaissance de la gestion des risques et de ses fondamentaux
- Première connaissance de la méthodologie EBIOS 2010 ou EBIOS Risk Manager

Public

- Officiers de sécurité
- Gestionnaires de risques
- Responsables du traitement des données en entreprise
- Chefs de projets ou consultants
- CIO et managers responsables de la gestion IT d'une entreprise ainsi que la gestion des risques
- Membres d'une équipe de sécurité de l'information
- Conseillers experts en technologie de l'information
- Experts techniques voulant se préparer pour un poste en sécurité de l'information ou de RSSI

En présentiel

Durée
3 jours
(21 heures)

En savoir plus

Certification ISO 27005 - Risk Manager

Les objectifs pédagogiques

01. Comprendre les concepts, approches, méthodes et techniques permettant **une gestion efficace du risque selon l'ISO 27005.**

02. Interpréter les exigences d'ISO 27001 concernant la gestion du risque afin de **comprendre la relation entre un SMSI, des mesures de sécurité, et la conformité** aux exigences des différentes parties prenantes d'une organisation.

03. Acquérir les compétences pour **mettre en œuvre, maintenir et gérer un programme continu de gestion du risque** dans la sécurité de l´information.

04. Acquérir les compétences pour **conseiller efficacement une organisation** sur les meilleures pratiques en gestion du risque dans la sécurité de l'information.

Programme

- Introduction
- Evaluation du risque, traitement, acceptation selon ISO 27005
- Les fonctions transverses de la gestion des risques et autres méthodologies

Prérequis

- Connaissances générales des systèmes d'information
- Connaissances générales en sécurité des systèmes d'information
- Connaissances générales en gestion des risques

Public

- Gestionnaires de risques
- Personnes responsables de la sécurité de l'information ou de la conformité au sein d'une organisation
- Membres d'une équipe de sécurité de l'information
- Consultants en technologie de l'information
- Personnel de la mise en œuvre de la norme ISO 27001 ou cherchant à s'y conformer ou participant à un programme de gestion du risque

Présentiel ou distanciel

Durée
3 jours
(19 heures)

En savoir plus

LES FORMATIONS EN SENSIBILISATION

Sensibilisation à la Cybersécurité

Les objectifs pédagogiques

01. Comprendre **les risques cybersécurité les plus courants.**

02. Acquérir **les bonnes pratiques en termes de sécurité.**

03. **Repérer les signes** d'une attaque informatique et **réagir.**

Programme

- Introduction
- Faiblesses du matériel
- Sécurité des périphériques
- Mots de passe faibles
- Les logiciels malveillants
- L'ingénierie sociale

Prérequis

- Aucun prérequis

Présentiel ou distanciel

Public

- Toute personne au sein d'une organisation amené à utiliser le système d'information: Poste de travail, e-mail, smartphone. La formation est construite de manière à être accessible à tous, sans connaissances préalables dans le domaine informatique.

Durée
2 heures

En savoir plus

Sensibilisation à la protection du secret

Les objectifs pédagogiques

01. **Appréhender** et comprendre les enjeux de sécurité de l'information.

02. **Responsabiliser** face aux risques.

03. **Identifier** les menaces et les moyens de protection.

04. **Maîtriser** la gestion des communications, des documents et des réseaux en déplacement.

Programme

- Introduction
- Comprendre le secret et connaître son patrimoine informationnel
- Détecter les menaces
- Protéger et réagir

Prérequis

- Aucun prérequis

Présentiel ou distanciel

Public

- Le top management
- Toute personne au sein d'une organisation amenée à se déplacer avec de l'information
- Tout collaborateur

Durée
2 heures

En savoir plus

“APPRENDRE ENSEMBLE, C’EST RECEVOIR AUTANT QU’ON DONNE !

Alia SAADI
Consultante Governance, Risks & Compliance
Formatrice en sensibilisation

Mon profil formateur

Sensibilisation à l'éthique de l'IA

Les objectifs pédagogiques

01. **Sensibiliser** aux opportunités, aux risques et aux enjeux de l'IA.

02. **Responsabiliser** face aux risques.

03. **Identifier** les projets à risque.

04. Donner les clefs à l'initiation d'une **stratégie d'entreprise.**

Programme

- Introduction
- L'éthique de l'IA dans les projets
- Sensibilisation et bonnes pratiques
- Cas particuliers : l'IA dans un secteur particulier (sur demande)

Prérequis

- Aucun prérequis

Présentiel ou distanciel

Public

- Toute personne au sein d'une organisation amené à utiliser des outils d'IA : Outils internes, BOT, IA Génératives (Typer Chat GPT) etc. La formation est construite de manière à être accessible à tout le monde, sans connaissance préalable dans le domaine informatique.

Durée
8 heures

En savoir plus

Comprendre et mettre en œuvre le guide d'hygiène de l'ANSSI

Les objectifs pédagogiques

01. Comprendre les **42 règles du guide d'hygiène de l'ANSSI.**

02. **Réaliser un autodiagnostic** de son entreprise.

03. Établir un plan d'action **pour améliorer le niveau de sécurité de son organisme.**

Programme

- Sensibiliser et former
- Connaître le système d'information
- Authentifier et contrôler les accès
- Sécuriser les postes, le réseau et l'administration
- Gérer le nomadisme
- Maintenir le système d'information à jour
- Superviser, auditer et réagir

Prérequis

- Aucun prérequis

Présentiel ou distanciel

Durée
2 heures

Public

- L'ensemble des acteurs du système d'information

En savoir plus

Technique des pirates informatiques, comment s'en protéger ?

Les objectifs pédagogiques

01. Comprendre les **42 règles du guide d'hygiène de l'ANSSI.**

02. **Réaliser un autodiagnostic** de son entreprise.

03. Établir un plan d'action **pour améliorer le niveau de sécurité de son organisme.**

Programme

- Introduction
- Sécurité des applications web
- Faiblesses du matériel
- Sécurité des périphériques nomades
- Sécurité Active Directory
- L'ingénierie sociale
- Réseaux WIFI

Prérequis

- Notions de base en informatique : réseau (protocoles, modèle OSI, etc.) et système (Linux ou Windows, gestion d'un serveur, etc.)

Présentiel ou distanciel

Durée
7 heures

Public

- Équipe IT
- RSSI
- Équipe support
- Administrateur système
- Administrateur réseau

En savoir plus

“

L'IMPORTANT N'EST PAS DE CONNAÎTRE L'INFORMATION, MAIS DE SAVOIR OÙ LA TROUVER !

Steven GALLAIS
Consultant Governance, Risks & Compliance
Formateur en sensibilisation

Mon profil formateur

almond
INSTITUTE

Les modalités et délais d'accès

Le stagiaire est considéré inscrit lorsque :
→ Les prérequis et besoins sont identifiés et validés
→ La convention de formation est signée
Les demandes d'inscription peuvent être envoyées jusqu'à 10 jours ouvrés avant le début de la formation.

L'accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.
Si vous avez besoin d'une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Nos centres de formation

PARIS
Bâtiment Crisco Duo
7 avenue de la Cristallerie
92310 Sèvres

NANTES
Centre d'affaires Euptouyou
4 rue Edith Piaf Immeuble Asturia C
44800 Saint-Herblain

STRASBOURG
Centre d'affaires Regus les Halles
Tour Sébastopol, 3 quai Kléber
67000 Strasbourg

LYON
Wellio Part-Dieu
13-15 rue des Cuirassiers
69003 Lyon

GENÈVE
Route de la Galaise 11B
1228 Plan les Ouates
Suisse

CHEZ VOUS
Formations intra-entreprises
Contactez-nous pour concevoir votre projet.

Almond INSTITUTE

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

https://almond.eu/almond-institute/

Contact pour ce dossier

Miora RAHARINIRINA
Chargée de mission formation
almond.institute@almond.eu
07 64 42 71 56