

L'ALTERNANCE

2iTECH

Academy by M2i

**La voie d'Excellence pour
ton avenir professionnel**



2itechacademy.com

**INTELLI
GENCE**

INNOVATION

**TECHNO
LOGIES**

**NUMME
RIQUE**

INFORMATIQUE

“ L'école 2i Tech Academy a été construite sur des valeurs, le savoir-faire d'un groupe reconnu et des Hommes.

Au cœur de notre organisation, des hommes et des femmes philanthropes qui œuvrent pour un avenir brillant et honorable, un présent studieux et serein, et un passé sur lequel capitaliser en expérience.

Nous avons la chance de travailler dans des métiers de passion, une passion que nous aimons partager avec nos étudiants, notre équipe pédagogique et nos entreprises partenaires qui accueillent nos apprenants.

Peu importe le chemin parcouru pour arriver à ce que nous sommes tous aujourd'hui, l'important est de savoir où nous voulons aller et faire en sorte d'y arriver le mieux possible. Le sens de notre métier nous porte au quotidien.

Rejoindre 2i Tech Academy, c'est se donner la chance de s'accomplir. ”

Corinne Combes
Directrice 2i Tech Academy

SSO MM AA RE

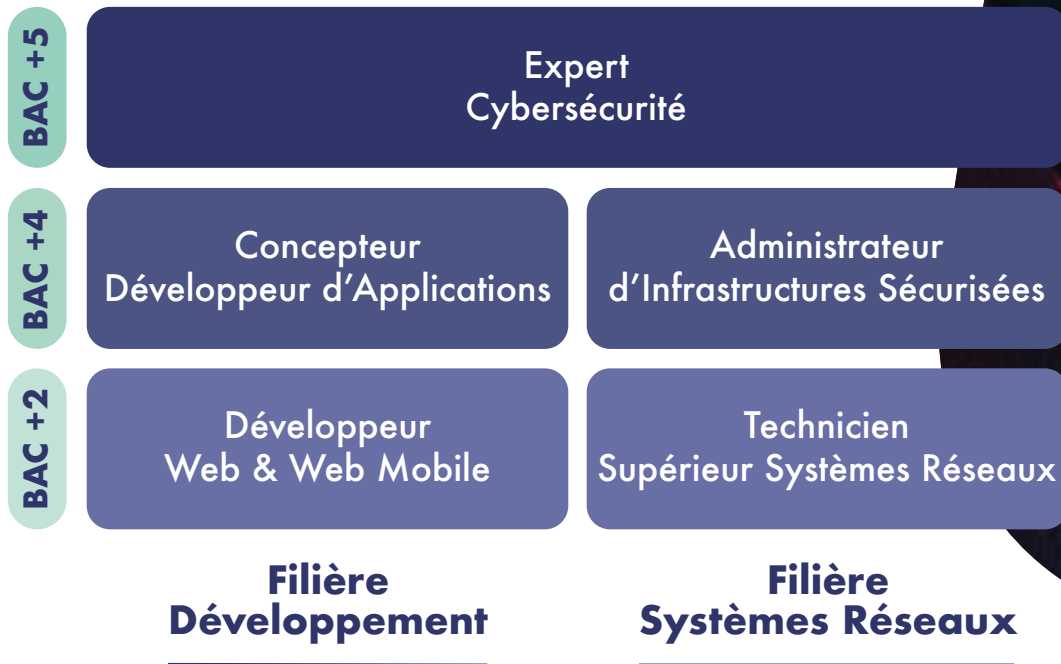
| | |
|---|----|
| Nos Parcours | 5 |
| Technicien Supérieur Sécurité Réseau <i>BAC +2 Niveau 5</i> | 8 |
| Développeur Web et Web Mobile <i>BAC +2 Niveau 5</i> | 10 |
| Administrateur d'Infrastructures Sécurisées <i>BAC +4 Niveau 6</i> | 12 |
| Concepteur Développeur d'Applications <i>BAC +4 Niveau 6</i> | 14 |
| Expert en Cybersécurité <i>BAC +5 Niveau 7</i> | 16 |
| Nos Campus | 19 |

NOS PARCOURS

A l'heure où le digital explose, les opportunités professionnelles sont nombreuses dans le monde IT.

Qu'il s'agisse de Cybersécurité, de réseaux ou de développement, notre objectif est de vous former sur des métiers à fort potentiel d'embauche et avec des conditions attractives dès le début de sa carrière.

Nos formations débouchent sur des diplômes reconnus par l'Etat de BAC +2 à BAC +5 et sur un métier.



Un groupe centré sur des valeurs



Bienveillance

Parce que nos apprenants sont nos meilleurs ambassadeurs, leur réussite est notre principal objectif.

Nous les accompagnons et les formons pour leur offrir la voie d'excellence vers leur avenir professionnel.



Excellence

Une pédagogie innovante et performante, couplée au plus grand réseau d'entreprises partenaires pour mettre en pratique ses acquis, est le facteur de succès de nos parcours.



Proximité

Un réseau de 35 agences handi-accueillantes en France et dans le monde pour répondre au plus près des attentes régionales tout en bénéficiant des avantages et partenariats d'un grand groupe.

POURQUOI CHOISIR 2i TECH ACADEMY ?



Un conseil individualisé

Parce que chaque projet est unique, nos recruteurs sont là pour vous accompagner et concrétiser votre parcours selon votre ambition.



Des formateurs experts

Nos formateurs ont été scrupuleusement sélectionnés pour vous donner la meilleure expérience pédagogique possible.



Le job de vos rêves !

Nos Chargés des relations entreprises œuvrent au quotidien pour bâtir des partenariats solides et vous ouvrir les portes du monde du travail.

COMMENT VOUS INSCRIRE ?

1.

Envoyez-nous votre candidature

En ligne, sur notre site internet 2itechacademy.com, ou en participant à l'une de nos sessions d'admission tous les Mercredis à 14h dans nos campus.

2.

Participez à nos sessions d'admission

Passage de tests de positionnement, logiques et techniques, et entretien individuel de motivation afin de s'assurer que la formation choisie est cohérente avec votre projet professionnel.

3.

Bienvenue chez 2i Tech Academy !

Une fois votre candidature validée, participez à notre journée d'intégration. Au programme : présentations avec les équipes qui vous accompagneront dans votre recherche d'entreprise, coaching, accompagnement et découverte de l'univers 2i Tech Academy.



NOS

FORMATIONS

TECHNICIEN SUPERIEUR SYSTEMES RESEAUX

BAC +2
Titre inscrit au RNCP de Niveau 5
24 mois

Titre Professionnel du Ministère de l'Emploi et de la Formation Professionnelle

Un poste au cœur des enjeux d'une DSI

Le Technicien Supérieur Systèmes et Réseaux participe à la mise en service et au maintien en condition opérationnelle de l'infrastructure informatique :

- Il intervient sur les systèmes et les réseaux, sur les éléments matériels et logiciels qui composent l'infrastructure, afin d'offrir aux utilisateurs et aux clients le niveau de service attendu par l'entreprise.
- Il assiste les utilisateurs dans l'utilisation de leur équipement numérique.
- Il contribue au développement des compétences des utilisateurs en expliquant les règles de sécurité et de bon usage des logiciels et des outils collaboratifs en ligne.
- Il vérifie que les sauvegardes de tous les éléments de l'infrastructure (serveurs et équipements actifs du réseau) ont été réalisées.
- Il surveille tous les équipements systèmes et réseaux et les journaux de sécurité et mènent les actions correctrices nécessaires.
- Il peut être sollicité par le centre de services pour diagnostiquer et résoudre les dysfonctionnements relevant du système, du réseau ou de la téléphonie sur IP.
- Il rétablit l'accès aux ressources partagées et aux applications.
- A la demande de son responsable, il crée, supprime ou modifie les moyens d'interconnexion des sites distants de l'entreprise.
- Il utilise les outils d'administration des différents environnements des services hébergés à l'externe et consulte les contrats pour rétablir ou améliorer le fonctionnement du service.
- Il automatise de nouvelles tâches et faire évoluer les scripts existants.
- Le technicien supérieur systèmes et réseaux assure une veille technologique et réglementaire afin de maintenir ses compétences à jour et de tester les nouvelles technologies.

Le technicien supérieur systèmes et réseaux travaille dans une entreprise de services du numérique (ESN) ou au sein de la Direction des Systèmes d'Information (DSI) d'une entreprise, d'une administration ou d'une collectivité territoriale.

Les pré-requis pour accéder à cette formation

- BAC Technologique (STIDD / SEN / STMG), Professionnel ou Scientifique ou niveau de connaissances équivalent
- 2 à 3 mois de stage comme technicien de maintenance / Helpdesk
- Goût pour la technique et adaptabilité permanente aux évolutions technologiques
- Pratique de l'anglais technique souhaitable
- Aptitudes relationnelles, rédactionnelles et techniques

Les intitulés de postes accessibles

- Technicien systèmes et réseaux
- Technicien support
- Technicien réseau
- Technicien informatique
- Technicien d'exploitation

Le parcours de formation

Cursus en alternance : 3 semaines en entreprise / 1 semaine en centre de formation

Certification éditeur Microsoft Windows Server OFFERTE

Ce parcours peut être suivi d'une formation **Administrateur d'Infrastructures Sécurisées, Niveau BAC +4**



PROGRAMME DE FORMATION

Compétences à acquérir

Assister les utilisateurs en centre de services :

- Mettre en service un équipement numérique
- Assister les utilisateurs sur leurs équipements numériques
- Gérer les incidents et les problèmes
- Assister à l'utilisation des ressources collaboratives

Maintenir, exploiter et sécuriser une infrastructure centralisée :

- Maintenir et exploiter le réseau local et la téléphonie
- Sécuriser les accès à internet
- Maintenir et exploiter un environnement virtualisé
- Maintenir et exploiter un domaine Active Directory et les serveurs Windows
- Maintenir et exploiter un serveur Linux

Maintenir et exploiter une infrastructure distribuée et contribuer à sa sécurisation :

- Configurer les services de déploiement et de terminaux clients légers
- Automatiser les tâches à l'aide de scripts
- Maintenir et sécuriser les accès réseaux distants
- Superviser l'infrastructure
- Intervenir dans un environnement de Cloud Computing
- Assurer sa veille technologique

Technologies, méthodes et outils abordés

- Comprendre le fonctionnement d'une infrastructure réseaux : TCP / IP, Switch, Routeurs...
- Acquérir une méthodologie de dépannage.
- Découvrir la gestion des processus de gestion des incidents avec ITIL
- Gérer un projet de mise en service d'équipements numériques à l'aide de SCRUM
- Paramétrer et maintenir une solution de téléphonie sur IP
- Configurer une plateforme collaborative Office 365 ou G Suite pour assister les utilisateurs

- Implémenter et administrer des serveurs Windows Server 2016 / 2019 et leurs services réseaux : DHCP, DNS...
- Mettre en place et gérer un Domaine Active Directory : comptes utilisateurs ou ressources partagées...
- Configurer et sécuriser les postes des utilisateurs à l'aide des GPO
- Administrer des serveurs Linux
- Virtualiser des serveurs avec HyperV
- Sécuriser les accès Internet avec un serveur Proxy / FireWall

- Mettre en place les services de déploiement WDS et MDT
- Comprendre les environnements Cloud : Amazon, Azure
- Gérer des services Windows Office 365
- Automatiser l'administration de serveurs Windows avec PowerShell
- Sécuriser les accès réseaux distants avec un service VPN
- Implémenter et paramétrer
- Mettre en place un environnement WIFI
- Comprendre les caractéristiques des Remote Desktop Services et déployer une infrastructure RDV et VDI
- Gérer un parc de machines et superviser avec GLPI et Nagios
- Mettre en place une veille technologique sur Internet et les réseaux sociaux
- Comprendre les aspects réglementaires de la sécurité et confidentialité : RGPD...

DEVELOPPEUR WEB ET WEB MOBILE

BAC +2

Titre inscrit au RNCP de Niveau 5
24 mois

Titre Professionnel du Ministère de l'Emploi et de la Formation Professionnelle

Un habile mélange entre technique et créativité

Le développeur Web et Web Mobile :

- Développe ou fait évoluer des applications orientées Web, ou Web mobile, en respectant les normes et standards reconnus par la profession.
- Conçoit la partie visuelle de l'application exécutée sur le navigateur côté ordinateur client.
- Ebauche la maquette des écrans de l'interface utilisateur et prévoit la navigation de l'application Web ou Web mobile.
- Code avec des langages de programmation web adaptés et une architecture applicative conforme aux bonnes pratiques du développement Web et Web mobile.
- Réalise la partie visuelle de l'application dans un premier temps de manière statique et en la rendant adaptable au contexte puis dans un deuxième temps capable d'interagir avec l'utilisateur de manière dynamique.
- En fonction des besoins de l'utilisateur, il peut installer et adapter une solution préétablie de gestion de contenu ou d'e-commerce.
- Respecte les principes de sécurisation des interfaces utilisateur et prend en compte la charte graphique, ou les interfaces utilisateur standardisées, ainsi que les règles d'accessibilité.
- Conçoit et code la partie back-end, c'est-à-dire exécutée côté serveur pour accéder aux données. Il crée la base de données et développe les composants d'accès aux données pour pouvoir les afficher et les mettre à jour dans l'application Web ou Web mobile.
- S'adapte en continu aux évolutions technologiques du secteur du développement Web et Web mobile.
- Selon le contexte, il collabore avec d'autres développeurs, un ergonomiste, un Web designer, un architecte logiciel, un testeur et avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) de son entreprise, de son client ou de son hébergeur.

Il peut travailler en tant que salarié ou en indépendant. Selon la taille du projet, il peut le mener en autonomie, de sa conception à son développement, ou au sein d'une équipe et sous la responsabilité d'un chef de projet.

Les pré-requis pour accéder à cette formation

- Bac Scientifique / Technologique (SEN / STIDD / STMG...) ou le niveau de connaissances équivalent
- Expérience en entreprise ou des connaissances autour des métiers du Web
- Pratique courante des smartphones, tablettes et outils bureautiques
- Goût pour la technique et adaptabilité permanente aux évolutions technologiques
- Pratique de l'anglais technique souhaitable

Les intitulés de postes accessibles

- Développeur web,
- Développeur web Front End
- Développeur Back End
- Développeur PHP
- Développeur web mobile
- Aptitudes relationnelles, rédactionnelles et techniques

Le parcours de formation

Cursus en alternance : 3 semaines en entreprise / 1 semaine en centre de formation

Certification M2i Développement PHP

Ce parcours peut être suivi d'une formation [Concepteur Développeur d'Applications, Niveau BAC +4](#)

PROGRAMME DE FORMATION

Compétences à acquérir

Développer la partie front-end d'une application Web ou Web mobile en intégrant les recommandations de sécurité :

- Maquetter une application
- Réaliser une interface utilisateur Web statique et adaptable
- Développer une interface utilisateur Web dynamique
- Réaliser une interface utilisateur avec une solution de gestion de contenu ou e-commerce

Développer la partie back-end d'une application Web ou Web mobile en intégrant les recommandations de sécurité :

- Créer une base de données
- Développer les composants d'accès aux données
- Développer la partie back-end d'une application Web ou Web mobile
- Elaborer et mettre en œuvre des composants dans une application de gestion de contenu ou e-commerce

Technologies, méthodes et outils abordés

- Maquetter une site Web ou une application mobile en respectant les standards de l'UX Design à l'aide de l'outil Adobe XD
- Gérer un projet Web à l'aide de méthodes agiles
- Concevoir des pages Web et une interface Responsive en HTML / CSS
- Interagir avec l'interface à l'aide du langage JavaScript
- Construire une interface utilisateur avec Vue.js
- Concevoir un site Web à l'aide du CMS WordPress
- Référencer un site Web

- Avoir une démarche DevOps
- Modéliser, à partir d'un cahier des charges, une application à l'aide d'UML
- Modéliser, exploiter et mettre en production une base de données MySQL en utilisant le langage SQL
- Développer un site Web dynamique à l'aide de PHP 7 et Symfony 4
- Développer des applications Web avec Angular 8
- Concevoir un site de e-commerce avec PrestaShop
- Développer une application Web multiplateforme avec IONIC 3



ADMINISTRATEUR D'INFRASTRUCTURES SECURISEES

BAC +4
Titre inscrit au RNCP Niveau 6
24 mois

Titre Professionnel du Ministère de l'Emploi et de la Formation Professionnelle

Un rôle stratégique au sein d'une DSI

L'Administrateur d'Infrastructures Sécurisées implémente, paramètre, sécurise et administre en condition opérationnelle, les infrastructures informatiques :

- Il propose et met en œuvre des solutions permettant de faire évoluer les infrastructures et contribue à la gestion des risques et à la politique de sécurité de l'entreprise.
- Il installe, sécurise et met en exploitation les composants de l'infrastructure (serveurs, matériels réseaux...). Il en supervise le fonctionnement et en assure le support, dans le respect des bonnes pratiques.
- Il met en place et administre l'infrastructure, centralisée ou distribuée, interne ou dans le cloud, permettant aux utilisateurs d'accéder aux données et aux applications, et assure la sécurité des accès et la protection des données.
- Il intègre les besoins liés à la mobilité dans l'environnement de travail des utilisateurs.
- Il applique la politique de sécurité de l'entreprise, en collaboration avec le responsable de la sécurité des systèmes d'information et contribue à son renforcement par l'étude et la mise en place de solutions techniques, d'actions de sensibilisation et de diffusion de bonnes pratiques, en français comme en anglais.
- Il est l'interlocuteur des clients (internes ou externes), des responsables métier et des décideurs ainsi que des partenaires externes.

Les pré-requis pour accéder à cette formation

- BAC + 2 en Informatique (BTS SIO option SISR, DUT, Titre Pro...)
- Expérience de 6 mois minimum en tant que technicien informatique / réseau
- Connaissances des fondamentaux de l'administration d'un serveur (Windows ou Linux)
- Pratique de l'anglais technique souhaitable
- Aptitudes relationnelles, rédactionnelles et techniques

Les intitulés de postes accessibles

- Administrateur systèmes et / ou réseaux
- Responsable infrastructure systèmes et réseaux.
- Administrateur sécurité
- Intégrateur d'exploitation



Le parcours de formation

Cursus en alternance : 3 semaines en entreprise / 1 semaine en centre de formation
Certification éditeur Microsoft Windows Server, Amazon Web Services OFFERTE
Ce parcours peut être suivi d'une formation **Expert en Cybersécurité, Niveau BAC +5**

PROGRAMME DE FORMATION

Compétences à acquérir

Administrer et sécuriser les composants constituant d'une infrastructure :

- Administrer et sécuriser un réseau d'entreprise, un environnement de systèmes hétérogènes et virtualisés
- Appliquer les bonnes pratiques et participer à la qualité de service

Intégrer, administrer et sécuriser une infrastructure sécurisée :

- Automatiser l'administration de différents systèmes à l'aide de scripts
- Administrer les services dans un environnement distribué
- Intégrer et gérer les environnements de travail des utilisateurs

Faire évoluer et optimiser une infrastructure et son niveau de sécurité :

- Superviser, mesurer et publier les performances et la disponibilité d'une infrastructure et de son niveau de sécurité
- Proposer une solution informatique répondant à de nouveaux besoins
- Participer à l'élaboration de la politique de sécurité en lien avec le RSSI

Technologies, méthodes et outils abordés

- Comprendre et mettre en œuvre les différents services réseaux et TCP / IP
- Implémenter et administrer des serveurs Windows Server 2016 / 2019 : AD FS, GPO, DFS...
- Implémenter et administrer des serveurs Linux dans un environnement Microsoft (Samba4)
- Sécuriser le réseau et les systèmes en implémentant la gestion des identités, une DMZ, des FireWall et un VPN
- Virtualiser et créer et gérer des conteneurs avec VMware vSphere, Hyper V, Docker et Kubernetes...
- Acquérir les concepts de base d'ITIL pour améliorer la qualité de services

- Automatiser avec PowerShell, Python et orchestrer l'administration de systèmes avec Ansible et Terraform
- Étendre et administrer le SI dans un environnement Cloud Azure et / ou Amazon
- Déployer (PXE, MDT, WIM...), administrer les environnements des utilisateurs, postes de travail ou device mobile dans un environnement multi-sites et virtualisé

- Utiliser les méthodes Agile pour faire évoluer l'infrastructure
- Mettre en œuvre une veille technologique pour augmenter le niveau de fiabilité et sécurité
- Superviser et gérer le suivi des incidents d'infrastructure : GLPI, SNMP et WMI
- Implémenter de la haute disponibilité des serveurs et matériels actifs et gérer un PCA / PRA
- Gérer un projet
- Faire une analyse des besoins et des contraintes
- Gérer un budget
- Analyser, synthétiser des documents en français et en anglais pour mieux communiquer à l'oral ou par écrit
- Mettre en place un POC



CONCEPTEUR DEVELOPPEUR D'APPLICATIONS

BAC +4
Titre inscrit au RNCP de Niveau 6
24 mois

Titre Professionnel du Ministère de l'Emploi et de la Formation Professionnelle

Un métier phare en plein BOOM du digital

Le Concepteur Développeur d'Applications :

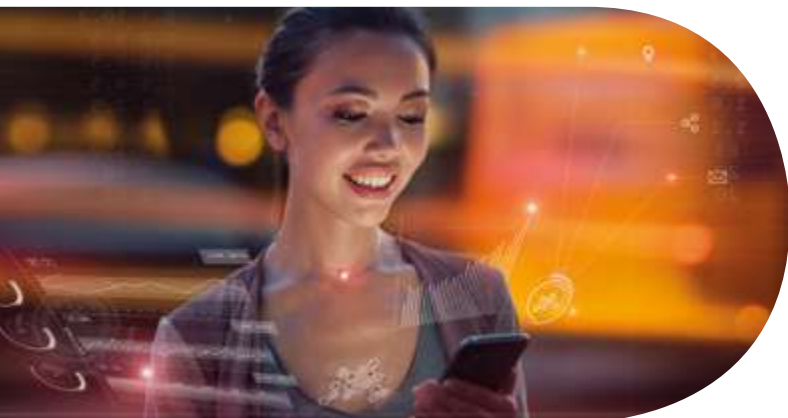
- Réalise de nouvelles applications Web et mobiles
- Travaille dans une startup ou une grande entreprise
- Analyse un cahier des charges fonctionnel afin de modéliser une base de données
- Intervient sur les différentes phases du processus de développement logiciel
- Elabore des maquettes et les fait valider
- Assure la maintenance corrective ou évolutive d'applications existantes
- Applique une démarche qualité
- Gère un projet ainsi qu'une équipe Web
- Assurer la maintenance corrective et évolutive des applications informatiques
- S'adapte en continu aux évolutions technologiques et réglementaires

Les pré-requis pour accéder à cette formation

- BAC + 2 en Informatique (BTS SIO option SLAM, DUT...) et avoir exercé des missions de développeur Web
- Maîtrise HTML, CSS et d'un langage de programmation
- Pratique de l'anglais technique souhaitable
- Aptitudes relationnelles, rédactionnelles et techniques

Les intitulés de postes accessibles

- Concepteur développeur, concepteur d'applications informatiques
- Développeur d'applications, développeur informatique
- Développeur Web, développeur Front End, développeur Back End
- Développeur d'applications mobiles, développeur Web mobile



Le parcours de formation

Cursus en alternance : 3 semaines en entreprise / 1 semaine en centre de formation

Certification M2i Développement Java OFFERTE

Ce parcours peut être suivi d'une formation **Expert en Cybersécurité, Niveau BAC +5**



PROGRAMME DE FORMATION

Compétences à acquérir

Concevoir et développer des composants d'interface utilisateur en intégrant les recommandations de sécurité :

- Maquetter une application
- Développer une interface utilisateur de type desktop
- Développer des composants d'accès aux données
- Développer la partie Front End d'une interface utilisateur Web
- Développer la partie Back End d'une interface utilisateur Web

Concevoir et développer la persistance des données en intégrant les recommandations de sécurité :

- Concevoir une base de données
- Mettre en place une base de données
- Développer des composants dans le langage d'une base de données

Concevoir et développer une application multicouche répartie en intégrant les recommandations de sécurité :

- Collaborer à la gestion d'un projet informatique et à l'organisation de l'environnement de développement
- Concevoir une application
- Développer des composants métier
- Construire une application organisée en couches
- Développer une application mobile
- Préparer et exécuter les plans de tests d'une application
- Préparer et exécuter le déploiement d'une application

Technologies, méthodes et outils abordés

- Concevoir des pages Web statiques et dynamiques avec HTML / CSS et JavaScript
- Modéliser avec UML
- Maitriser la programmation structurée et orientée objet à l'aide du langage Java et du langage PHP
- Créer une application Desktop
- Développer des applications Web côté serveur avec Java EE
- Maquetter une application Web en utilisant UX Design
- Développer une application simple avec Angular
- Gérer une base de données relationnelle (MySQL ou Oracle) en PHP-PDO et Java-JDBC
- Gérer une base de données noSQL (MongoDB) en Java

- Modéliser une base de données avec UML
- Utiliser des requêtes SQL pour interroger et modifier une base de données
- Créer des procédures stockées
- Concevoir une base de données noSQL (MongoDB)

- Gérer un projet avec Scrum et les méthodes Agiles
- Développer une application multicouche avec Symfony (Framework MVC PHP)
- Travailler avec le Framework Hibernate pour Java
- Développer une application multicouche avec Spring (Framework MVC Java EE)
- Concevoir et automatiser des tests unitaires avec JUnit et PHPUnit
- Gérer des versions différentes de code source avec Git ou Subversion
- Développer une application Android natif avec Java et Kotlin
- Développer une application mobile multiplateformes avec ionic
- Déployer une application

EXPERT EN CYBERSECURITE

BAC +5
Titre inscrit au RNCP de Niveau 7
16 mois

Une compétence rare et prisée dans tous les secteurs d'activité

L'Expert en Cybersécurité utilise ses compétences dans un contexte donné d'organisation afin de prévoir et concevoir et mesures de sécurité adaptées aux différents risques pesant sur celle-ci. Il a pour missions essentielles la compréhension des différentes cyberattaques et un rôle crucial de conseil auprès du comité de direction pour la mise en œuvre de plans associés. Son rôle à la fois technique et organisationnel lui permet d'avoir une vision complète au travers la rédaction de schémas directeur SSI.

L'expert en cybersécurité :

- Comprend les menaces pesant sur les systèmes d'information, identifie les points névralgiques et mets en œuvre les mesures de sécurité adaptées en s'alignement sur les différents besoins de l'organisation.
- Applique des méthodes d'investigations en cas de cyberattaques pour en remonter l'origine (détection, l'investigation et la réponse aux incidents de sécurité).
- Participe à la définition de la politique de sécurité du système d'information et veille à sa mise en application.
- Joue un rôle de conseil, d'assistance, d'information, de formation et d'alerte auprès de la direction.
- Joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité ou encadre une équipe composée d'experts techniques et de consultants.
- Analyse, conçoit, met en œuvre les techniques de sécurisation. Maitrisant les référentiels des domaines « métier », il est en mesure de faire converger les objectifs de sécurité et de sûreté de fonctionnement.
- Conduit des analyses de risques et propose des solutions résilientes afin de minimiser sans concession les impacts « métiers ».
- Élabore et met en œuvre dans son organisation un Plan de Continuité d'Activité (PCA).
- Assure le sous-ensemble des activités d'ingénierie nécessaire au développement de logiciels répondant à des exigences de sécurité.
- Valide la cartographie du système d'information et s'assure notamment que les hypothèses de sécurité relatives à l'environnement de son architecture sont clairement énoncées et prises en compte dans sa conception.

Les pré-requis pour accéder à cette formation

- BAC +3 ou BAC +4 Informatique minimum ou niveau de connaissances équivalent
- Expérience significative en entreprise en tant qu'administrateur
- Excellentes connaissances de conception d'infrastructure SI
- Niveau existant en matière de développement (exemple : Python, C, etc.)
- Intérêt natif à la Cybersécurité
- Pratique de l'anglais technique
- Aptitudes relationnelles, rédactionnelles et techniques

Les intitulés de postes accessibles

- Expert en Cybersécurité
- Responsable de la Sécurité des Systèmes d'Information (RSSI)
- Spécialiste en gestion de crise cyber
- Chef de projet sécurité
- Architecte sécurité
- Analyste SOC
- Expert réponse à incident
- Consultant sécurité « organisationnel » ou « technique »
- Analyste de la menace

Le parcours de formation

Cursus en alternance : 3 semaines en entreprise / 1 semaine en centre de formation
Certifications M2i Inforensic et M2i Pentesting OFFERTES

PROGRAMME DE FORMATION

Compétences à acquérir

Comprendre et maîtriser les différentes attaques pesant sur les systèmes d'information :

- Compréhension des différentes attaques cyber
- Maîtriser le développement d'outil pour effectuer des tests de sécurité
- Etude, intégration et sécurisation des notions d'intelligence artificielle au sein des systèmes d'informations

Concevoir, intégrer et ajuster les mécanismes de défense face aux cyberattaques :

- Etude approfondie des différents types de malwares pouvant impacter les systèmes d'information
- Investigation numérique à la suite d'une cyberattaque
- Concevoir et implémenter des mécanismes de cyberdéfense
- Renforcer la sécurité :
 - Des réseaux et systèmes industriels
 - Des applications Web
 - Des systèmes embarqués et objets connectés
- Intégration et optimisation de SIEM et SOC

Gouvernance et alignement de la cyberdéfense aux objectifs et obligations de l'organisation :

- Etude de gestion de crise SSI
- Identification des risques SSI relatifs au business de l'organisation
- Implémenter de la norme ISO 27001
- Comprendre les obligations SSI liées au règlement sur la protection des données (RGPD)
- Intégrer la notion Devops au sein des processus
- Ajuster les mécanismes et processus de continuité d'activité au sein d'une organisation

Technologies, méthodes et outils abordés

- Comprendre et savoir repérer les différentes cyberattaques pesant sur les systèmes d'information ainsi que les différents groupes d'attaquants et leurs différents process (APT, Redteam)
- Concevoir des outils permettant d'effectuer des tests et simulations d'attaques sur les systèmes d'une organisation (Python)
- Assimiler et mettre en pratique des détournements d'usage de l'intelligence artificielle dans le cas de cyberattaques

- Analyser le fonctionnement et la diffusion de différents types de malwares à travers les systèmes informatiques
- Mettre en œuvre l'ensemble des étapes permettant la compréhension d'une cyberattaque grâce à des méthodes et des éléments de preuves recueillis (Forensics)
- Concevoir, ajuster et renforcer la sécurité à l'aide de plans de défense adaptés aux différents risques encouru par l'organisation (Renforcement des infrastructures, revues de du développement des applications Web, durcissement des systèmes, etc.)
- Intégrer des solutions de type (SIEM) au sein des équipes de sécurité (SOC) afin d'identifier les différentes menaces et leurs proliférations dans un système d'information

- Savoir mettre en œuvre des processus, procédures et plans d'actions associés à une gestion de crise cyber
- Identifier les risques SI pesant sur une organisation à travers une analyse de risques (ISO 27005 & EBIOS) intégrant en outre les notions de réglementation RGDP
- Concevoir et implémenter un système de management de la sécurité de l'information aligné aux différents risques pesant sur l'organisation avec la norme ISO 27001 (SMSI)
- Mettre en œuvre la rationalisation entre les équipes de développement et les équipes opérationnelles au sein des processus d'une organisation (DevOps)
- Comprendre et ajuster les besoins en continuité d'activité d'une entreprise grâce à une étude des risques couplée à l'application de la norme ISO 22301 (PCA)



Suivez vos actus FORMATION

Offres de formation

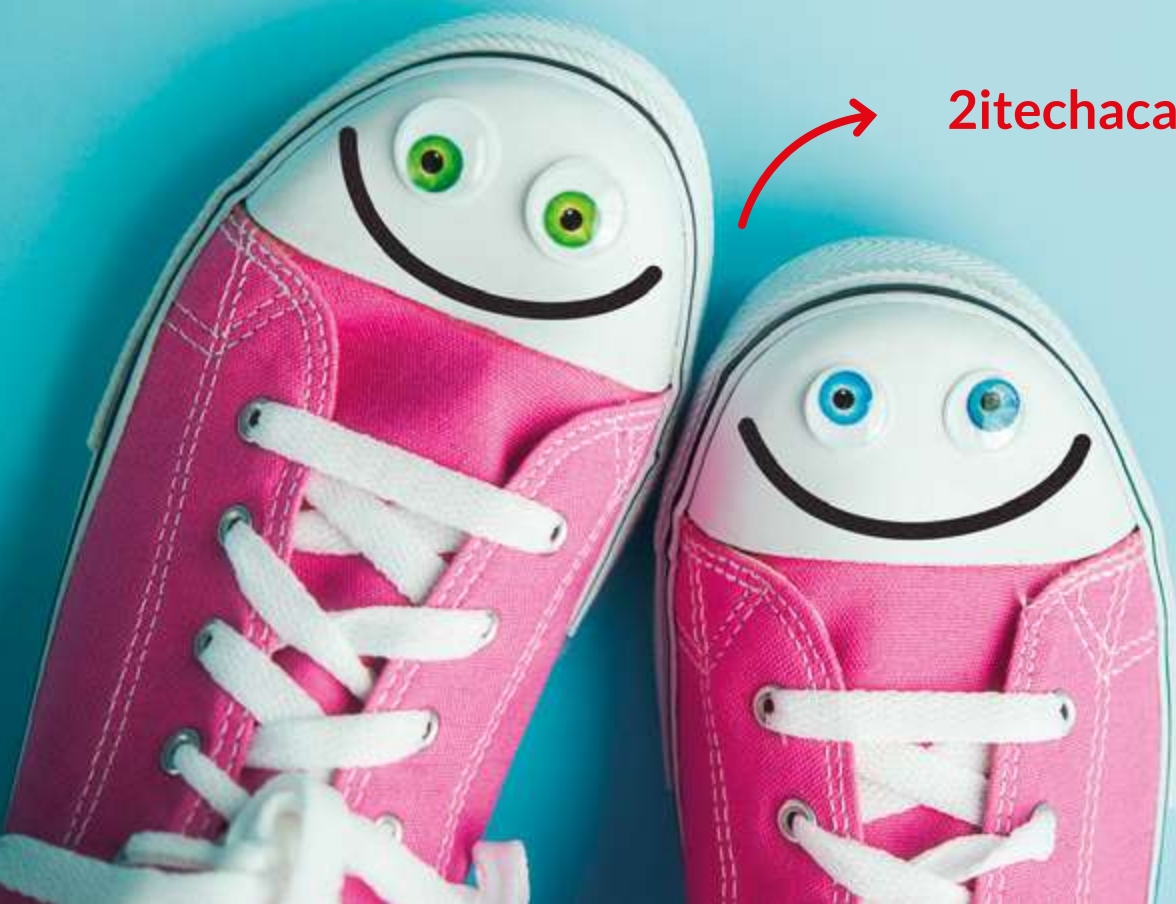


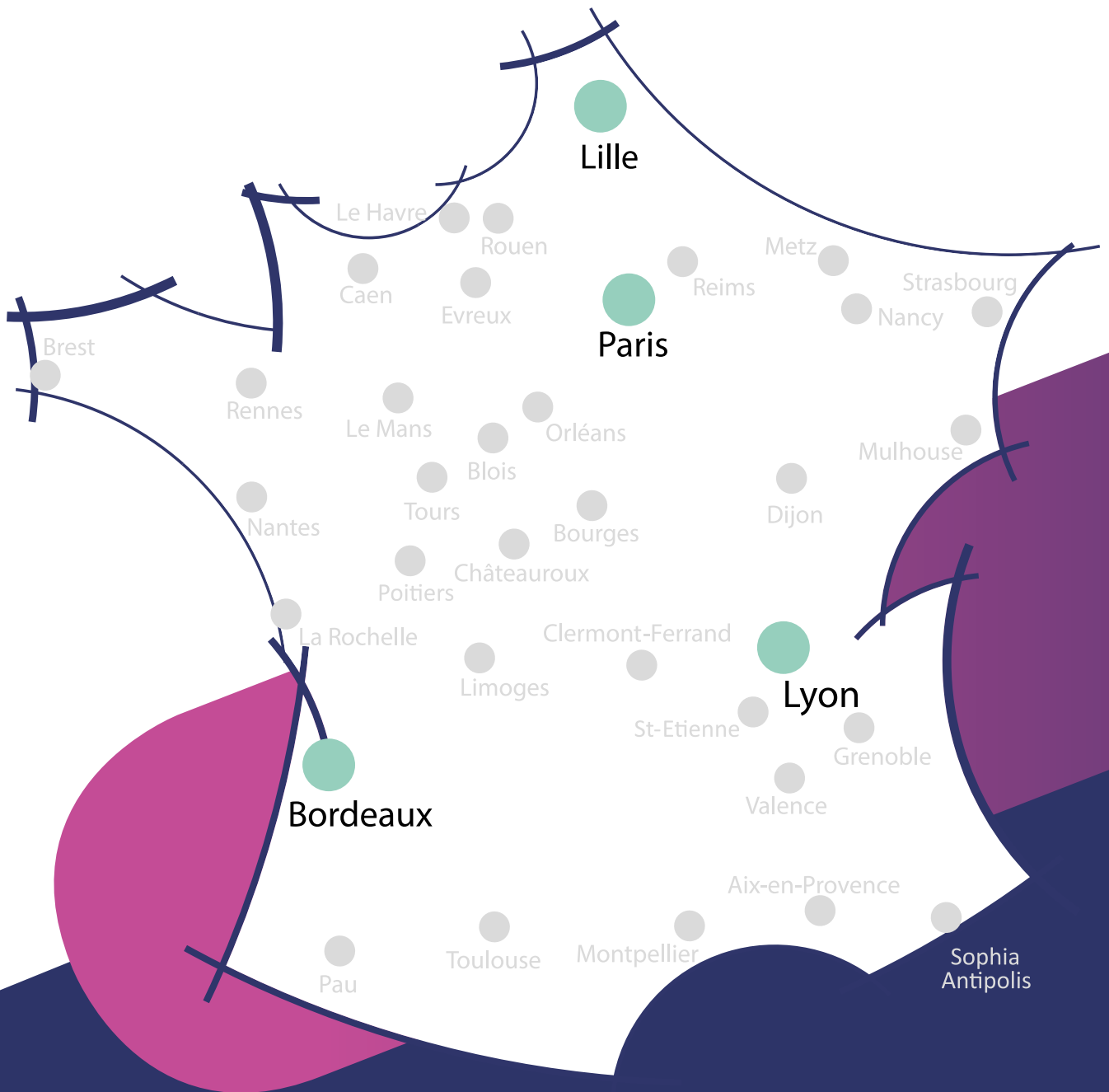
Conseils et astuces pour trouver
votre entreprise d'accueil



Détail de nos événements

2itechacademy.com





Paris

146-148 rue de Picpus
75012 Paris
01.44.53.36.30
admission-paris@2itechacademy.com
alternance-paris@2itechacademy.com

Lyon

Le Seven
69 avenue Tony Garnier
69007 Lyon
04.78.02.38.90
admission-lyon@2itechacademy.com
alternance-lyon@2itechacademy.com

Lille

4 avenue de l'Horizon
59650 Villeneuve-d'Ascq
03.20.98.17.62
admission-lille@2itechacademy.com
alternance-lille@2itechacademy.com

Bordeaux

15 bis allée James Watt
33700 Mérignac
05.57.19.07.60
admission-bordeaux@2itechacademy.com
alternance-bordeaux@2itechacademy.com

