IMIE PARIS
<L'école du numérique/>

ÉCOLE SUPÉRIEURE D'INFORMATIQUE

BACHELOR CYBERSÉCURITÉ

Titre reconnu par l'Etat

Inscrit au RNCP 39611 - Niveau 6 (Bac+3)

Administrateur Systèmes, Réseaux et Cybersécurité

3iL INGENIEURS

01 84 78 22 17

contact@imie-paris.fr

www.imie-paris.fr

BACHELOR CYBERSÉCURITÉ

</QUI SOMMES-NOUS ? >

IMIE Paris est une **école supérieure d'informatique** située à **Levallois-Perret** qui prépare depuis 2017 à la validation de 11 titres professionnels.
Notre **métier** est de **former** les futurs **talents** du **numérique** et d'**accompagner** les **révolutions technologiques**: web, applications mobiles, systèmes, réseaux, cloud, Big data, IA, Cybersécurité, architecture technique...

IMIE Paris dispense des **cursus qualifiants** en **formation continue** et **alternée** de niveau **Bac à Bac+5** aux métiers de l'**informatique**. En parallèle de l'alternance, IMIE Paris propose des parcours d'insertion ou de reconversion professionnelle en formation continue sur une période de 6 à 12 mois.
Nous formons aujourd'hui 250 à 300 stagiaires par an, ce qui représente plus de 1 000 carrières lancées depuis l'ouverture de l'école.
De plus, nous accompagnons **400 entreprises et institutions partenaires** dans leurs recrutements d'alternants.

</MOT DU DIRECTEUR ! >

Notre mission, former les futurs talents du numérique.

Le numérique, de quoi parle-t-on ?
Le numérique s'inscrit dans les sciences informatiques dédiées au développement d'applications mobiles ou fonctionnelles de sites web et des réseaux physiques ou virtuels. Il s'agit également des expertises émergentes liées à la gestion des données, à l'intelligence artificielle, aux objets connectés et à la cybersécurité...

Le numérique, une filière ouverte à toutes et tous ?
Absolument ! L'informatique se féminise car les prérequis pour se lancer dans cette filière reposent sur la motivation, la curiosité, l'ingéniosité et l'aptitude aux raisonnements logiques. Des qualités partagées par les femmes et les hommes.

Diversité des métiers, des secteurs ?
Le terrain de jeu est immense ! Nous vivons une révolution technologique qui nécessite de l'expertise à tous les niveaux et dans tous les secteurs d'activité. Il suffit d'observer notre environnement pour constater que le numérique est présent partout, qu'il s'agisse du secteur privé ou du secteur public.

La France accuse un retard dans le numérique ce qui amplifie encore les besoins de recrutement au point que les postes proposés ne sont pas tous pourvus.

Le secteur a besoin de compétences alors... lancez-vous !

</NOS ENGAGEMENTS >

- Former les futurs talents du numérique
- Déployer une pédagogie articulée autour d'apports théoriques et de mises en situation professionnelle
- Proposer un corps professoral exclusivement composé d'intervenants expérimentés
- Mettre à disposition les supports et outils pédagogiques
- Adapter annuellement les contenus des programmes en fonction des évolutions technologiques
- Accompagner nos stagiaires dans leurs recherches d'emploi

</LE BACHELOR CYBERSÉCURITÉ>
</BY IMIE PARIS >

Le **Bachelor Cybersécurité** vise à **former** des **professionnels** capables d'**assurer** le bon **fonctionnement**, la **sécurité** et l'**efficacité** des **infrastructures technologiques** des organisations. Dans un contexte où les **cybermenaces** sont de plus en plus **sophistiquées**, cette **formation** place la **cybersécurité** au **cœur** des **compétences développées**, garantissant aux apprenants une **expertise** indispensable pour **protéger** les **systèmes d'information** et les **données** des entreprises.

Ce **cursus** prépare à **relever** les **défis technologiques** actuels en **fournissant** les **compétences** nécessaires pour **administrer**, **sécuriser** et **surveiller les infrastructures** IT. Les **administrateurs systèmes**, **réseaux** et **cybersécurité** jouent un **rôle essentiel** dans la **gestion** et la **maintenance** des **systèmes d'exploitation**, en veillant à leur **mise à jour**, leur **sécurité** et leur **optimisation** pour garantir des **performances optimales**. Ils sont également **responsables** de la **configuration** et de l'**administration** des **infrastructures réseau**, ainsi que de la mise en œuvre de **stratégies** de **cybersécurité** visant à **anticiper** et **contrer** les **menaces informatiques**.

Le Bachelor Cybersécurité propose un **apprentissage progressif** et **professionnalisant**. Il met l'accent sur l'acquisition de **compétences techniques** solides et l'**adaptabilité** aux **environnements professionnels réels**. Ce cursus développe une **approche proactive** et **stratégique** de la **cybersécurité** en **intégrant** les **meilleures pratiques du secteur**.

Le Bachelor Cybersécurité est un **cursus** de formation **post bac** dispensé en **trois ans** qui prépare à la certification du **titre d'Administrateur Systèmes, Réseaux et Cybersécurité RNCP39611** de **niveau 6** (Bac+3) sous l'autorité du **certificateur 3iL ingénieurs**.

Les **deux premières années** de la formation se déroulent en **continu**. Un **stage** de deux à **trois mois** est prévu en **fin** de **deuxième année.** La **troisième année** du **Bachelor** peut être effectuée en **alternance ou en continu** (stage de deux à trois mois)**.**

La **première année** du cursus est un **tronc commun** visant à **acquérir** les **connaissances fondamentales** dans le domaine de l'**informatique.** La **suite du parcours** est dédié à la **spécialisation administration systèmes, réseaux et cybersécurité**. À l'issue de la première année, une **réorientation** est **possible** vers la seconde année du **Bachelor Full Stack**.

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr

</PROGRAMME DE LA FORMATION >

4J/ SEMAINE

ANNÉE 1 & 2 : CONTINU + STAGE 2 MOIS EN 2ÈME ANNÉE

ANNÉE 1 : TRONC COMMUN - 700 HEURES

Les fondations du numérique augmentées par l'Intelligence Artificielle

Cette première année intensive a pour objectif de transformer les apprenants en profils techniques polyvalents, capables de comprendre et de manipuler l'ensemble des couches de l'informatique moderne.
Ne vous contentez pas d'apprendre à coder : apprenez à développer plus vite, à concevoir mieux et à automatiser grâce à l'intégration de l'Intelligence Artificielle dès votre premier jour de cours.

Programmation & Conception logicielle

Maîtriser l'algorithmique, la programmation en Python et l'initiation à la conception orientée objet (POO) avec Java.
Apprendre également à concevoir des interfaces utilisateur professionnelles avec Figma et à modéliser vos architectures via UML.

Développement Web & Data

Construisez des applications web dynamiques (HTML5, CSS3, JavaScript) et connectez-les à des bases de données relationnelles (SQL).

Infrastructures, Systèmes & Réseaux

Plongez dans les bases de l'administration système sous Linux et Windows Server, configurez vos premiers équipements réseaux (Cisco, Routing/Switching basique) et découvrez la virtualisation (VMware/Hyper-V).

Culture Cybersécurité

Acquérez les premiers réflexes de protection des données (durcissement, OWASP) et acculturez-vous au cadre juridique du numérique (RGPD).

L'Avantage IA (Le Co-pilote)

Formez-vous au Prompt et au Context Engineering pour obtenir des résultats exploitables. Pratiquez le "Vibe Coding" (génération de code assistée par l'IA et pair-programming avec GitHub Copilot ou Claude) pour accélérer vos développements

Le Projet Fil Rouge (Chatbot Sécurisé)

Tout au long de l'année, vous concevrez, développerez et déploierez un Chatbot d'Entreprise Sécurisé de A à Z. De la maquette UI jusqu'à son hébergement sur des serveurs virtuels segmentés, en passant par sa connexion à une API d'IA générative.

ANNÉE 2 : SPÉCIALISATION CYBERSÉCURITÉ - 490 HEURES

Concevoir, développer et déployer des architectures de bout en bout

Systèmes et réseaux avancés

- Réseaux d'entreprise : VLAN, inter-VLAN routing, protocoles de redondance
- Configuration avancée Cisco : ACL, NAT/PAT, routage dynamique (OSPF, EIGRP)
- Conception et déploiement d'un réseau local complet
- Préparation aux certifications Cisco (CCNA – modules clés)

Administration des systèmes

- Administration Windows : Active Directory, GPO, gestion des utilisateurs
- Administration Linux : services, scripting Bash, automatisation
- Administration Windows Server : DNS, DHCP, services de fichiers
- Virtualisation avec VMware et Hyper-V : création et gestion de VM
- Déploiement et exploitation de serveurs virtuels en production
- Supervision et monitoring : mise en place d'une observabilité proactive

Sécurité des systèmes et réseaux

- Sécurité des réseaux : pare-feu (pfSense, iptables), VPN, segmentation
- Sécurité des systèmes : hardening Windows et Linux
- Surveillance, détection d'intrusion et gestion des incidents (SIEM)
- Mise en place de solutions de sécurité : antivirus, EDR, chiffrement
- Analyse des risques : méthodologie (EBIOS RM) et plans d'actions correctifs

Sécurité de l'IA

- Fonctionnement et architecture des modèles
- Référentiel des menaces spécifiques à l'IA : MITRE Atlas
- Vulnérabilités des API d'IA : sécuriser les points d'exposition des modèles
- Fondamentaux du Framework TRiSM (Trust, Risk and Security Management) de Gartner
- Intro aux risques "Shadow IA", "prompt injection", "empoisonnement des modèles"
- Audit de sécurité d'un déploiement IA et test de robustesse (avec Giskard.AI)
- Rédaction d'une politique de sécurité IA pour l'infrastructure déployée

Cloud et cybersécurité

- Introduction au cloud computing sécurisé et services managés
- xOps Engineering : Livrer vite (DevOps), exploiter fiable (SysOps), sécuriser by design (SecOps)
- Sécurité du cloud : IAM, chiffrement, conformité
- Introduction à l'AIOps : automatiser la détection d'anomalies avec l'IA

Compétences transversales & IA niveau 2

- Prompt Engineering avancé : requêtes spécialisées pour l'analyse de logs et la détection
- Context Engineering avancé : alimenter l'IA avec le bon contexte sécuritaire
- Veille sécurité : CVE, CERT-FR, threat intelligence
- Droit informatique avancé : RGPD, IA Act, NIS2 et obligations de sécurité
- Gestion de projet et gestion des opérations (ITIL)
- Communication professionnelle français / anglais technique
- Atelier de professionnalisation : CV, simulation d'entretiens techniques et soft skills

Projet fil rouge Cybersécurité – Défendre une infrastructure réelle

- Déployer, sécuriser et défendre une infrastructure complète face à des scénarios d'attaque réalistes. Un exercice grandeur nature pour prouver les compétences acquises.
- Déploiement d'une infrastructure réseau sécurisée de bout en bout
- Mise en œuvre de politiques de sécurité et de plans de réponse aux incidents
- Tests de performance et optimisation de l'infrastructure
- Utilisation de l'IA pour l'analyse de logs et la génération de rapports
- Soutenance devant un jury mixte (formateurs + professionnels de la cybersécurité)

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr

</PROGRAMME DE LA FORMATION >

1 SEMAINE / MOIS

ANNÉE 3 : ALTERNANCE OU CONTINU + STAGE 3 MOIS

ANNÉE 3 : CERTIFICATION CYBERSÉCURITÉ (ASRC) - 581 HEURES

Administration des Infrastructures sécurisées
- Administration et optimisation des systèmes d'exploitation : Windows Server, Linux avancé, Active Directory, annuaires
- Conception et déploiement d'environnements virtualisés : VMware, Hyper-V, clustering et haute disponibilité

Gestion de la Haute Disponibilité
- Solutions de redondance, réplication et clustering
- Plans de continuité et de reprise d'activité (PCA/PRA) : assurer la continuité de service

Supervision des infrastructures
- Surveillance et optimisation des performances : Zabbix, Centreon, Grafana
- Observabilité proactive : tableaux de bord, alertes, tendances

Gestion des incidents et système de ticketing
- Management du processus de gestion des incidents : procédures d'escalade, analyse post-mortem
- Systèmes de ticketing : GLPI, ServiceNow ou équivalent

Administration de Bases de Données
- Gestion et administration des SGBD relationnelles (SQL) et NoSQL
- Sauvegarde, récupération et optimisation des performances

Techniques de Scripting Système
- Automatisation des tâches d'administration : Bash, Python, PowerShell
- Développement de scripts de maintenance et de monitoring

Projet Infrastructures
- Déploiement complet d'une infrastructure système sécurisée, supervisée et automatisée

Infrastructures réseaux sécurisées
- Configuration de l'infrastructure réseau avancée : VLAN, VPN, routage dynamique, QoS, voix/data
- Déploiement des solutions de réseaux de données et télécommunications
- Supervision et maintenance du réseau

Architectures sécurisées – Cloud et hybrides
- Intégration et déploiement cloud : AWS, Azure, GCP en contexte infrastructure
- Intégration des pratiques de sécurité dans les processus de développement et d'opération

Infrastructure As Code
- Environnements virtualisés par conteneurisation : Docker, conteneurisation en production
- Orchestration de conteneurs avec Kubernetes
- Automatisation de l'infrastructure : Terraform, Ansible

Intégration et Déploiement Continus
- Pipelines CI/CD : Jenkins, GitHub Actions, GitLab CI
- Déploiement automatisé et monitoring
- Projet CI/CD + Infrastructure As Code (FM05)
- Mise en place complète d'un pipeline CI/CD couplé à une infrastructure automatisée

Cybermenaces et Risques
- Cartographie des menaces et analyse des vulnérabilités
- Analyse de risques : méthodologies EBIOS RM, ISO 27005

Politique de sécurité
- Développement, documentation et mise en œuvre de politiques de sécurité (PSSI)
- Conformité : ISO 27001, HDS, référentiels sectoriels

Audit de sécurité et amélioration continue
- Conduite d'audits de sécurité : tests d'intrusion, scan de vulnérabilités
- Élaboration d'actions correctives et plans de remédiation

Défenses Périmétriques
- Implémentation des outils de sécurité : pare-feu, IDS/IPS, WAF
- Architecture de défense en profondeur : segmentation, micro-segmentation

Techniques de Résilience
- Supervision des opérations de sauvegarde et de restauration
- Support et suivi des incidents IT

Gestion des identités et accès sécurisés
- Administration des systèmes d'identité : IAM, MFA, SSO, gestion des privilèges

Protection des données et conformité
- Conformité aux réglementations : RGPD, NIS2, IA Act
- Chiffrement et classification des données

Projet CyberSécurité
- Défendre une infrastructure complète face à des scénarios d'attaque réalistes et documenter votre stratégie de bout en bout.
- Mise en œuvre d'une politique de sécurité complète sur une infrastructure réelle
- Audit de sécurité et plan de remédiation
- Gestion d'un incident de sécurité simulé
- Soutenance devant un jury de certification

Étude d'avant-projet – MOA
- Analyse des besoins opérationnels et traduction en exigences techniques
- Rédaction de documents de spécification technique

Gestion de projet – MOE
- Planification et conduite du projet
- Coordination des équipes et communication

Gestion de projet architecture
- Orchestration et animation de projets informatiques en méthodes
- agiles
- Optimisation de la gestion des projets et suivi budgétaire

Gestion des coûts et du budget
- Gestion du budget de projet avec outils de gestion financière

Coordonner les équipes de projet – Communication
- Communication professionnelle et coordination d'équipe

Anglais professionnel et recherche documentaire
- Anglais technique et recherche documentaire multilingue

Veille technologique multilingue
- Veille technologique : analyse de sources d'informations spécialisées
- Analyse des données brutes et diffusion des scénarios à l'équipe IT

Projet Épreuves Certifiantes
- Le projet certifiant valide l'ensemble des compétences devant un jury de professionnels.
- Déploiement complet d'une infrastructure sécurisée certifiante
- Dossier technique professionnel : architecture, sécurité, documentation
- Soutenance orale devant un jury de certification

CERTIFICATION TITRE PROFESSIONNEL ADMINISTRATEUR SYSTÈMES, RÉSEAUX ET CYBERSÉCURITÉ CODE RNCP : 39611 - NIVEAU 6

3iLINGENIEURS

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr

</POURQUOI CHOISIR CETTE FORMATION ?>

8 raisons de nous rejoindre

L'IA au cœur de chaque module

Prompt Engineering, Context Engineering, agents IA, Vibe Coding... Vous ne subissez pas la révolution IA, vous en faites votre avantage compétitif. Dès le jour 1, vous apprenez à travailler avec l'IA, pas contre elle.

Une pédagogie par projets concrets

Chaque module débouche sur des livrables tangibles. Le projet fil rouge mobilise toutes vos compétences sur un défi réel, avec soutenance devant des professionnels du secteur.

Deux spécialisations à forte employabilité

Full Stack ou Cybersécurité : deux filières alignées sur les besoins les plus criants du marché. Les métiers du numérique affichent un taux d'emploi parmi les plus élevés tous secteurs confondus.

Des outils et technologies en phase avec le marché

Python, Java, React, Docker, Cisco, Git, Figma, AWS/Azure... Vous travaillez avec les mêmes technologies que les entreprises qui recrutent. Votre portfolio parle pour vous dès la sortie de formation.

Un titre RNCP Niveau 6 reconnu par l'État

En troisième année, vous préparez un titre certifié inscrit au RNCP (Niveau 6, équivalent Bac+3). Une reconnaissance officielle qui valorise votre parcours auprès de tous les employeurs et ouvre l'accès aux concours et formations de niveau supérieur.

Un accompagnement vers l'emploi

Ateliers de professionnalisation, rédaction de CV, simulations d'entretiens, personal branding et réseau professionnel. Vous n'êtes pas seul·e pour décrocher votre premier poste.

Un cadre légal et éthique intégré

RGPD, IA Act, NIS2 : vous comprenez les enjeux juridiques et éthiques du numérique. Un atout majeur pour les entreprises soumises à des obligations réglementaires croissantes.

3 ans pour passer de débutant à professionnel certifié

Un parcours progressif et cohérent : fondations solides en année 1, spécialisation en année 2, certification en année 3. Chaque année construit sur la précédente. À la sortie, vous êtes opérationnel, certifié, et prêt à relever les défis du numérique.

</PÉDAGOGIE ET MÉTHODES MOBILISÉES >

La **pédagogie** IMIE PARIS s'articule autour d'**apports théoriques** et de **mises en situation pratiques** dans les **laboratoires informatiques**. Nos **formateurs experts** encadrent les apprenants pour appliquer les **compétences acquises** en classe sur des **projets concrets**. Les **cours** sont dispensés en **présentiel** au sein du **campus**.

Tu pourras **élargir** tes **connaissances** lors de tes **participations** à différentes **conférences**, **salons** et **manifestations professionnelles** dans le domaine IT.

L'école offre également de nombreuses **opportunités professionnelles** à ses apprenants au sein de son réseau de partenaires. IMIE PARIS organise notamment des **Jobdatings** qui te permettront de **décrocher** ton **stage** ou ton **alternance**. Ces **immersions professionnelles développent** ton **expérience** et lancent ta **carrière** avec **succès** !

</OUTILS TECHNIQUES >

Linux · PowerShell · Windows Server · Microsoft Azure · Asterisk · vmware vSphere · pfsense

</NOS PARTENAIRES >

numeum · Planet Tech'Care · 3iL INGENIEURS — 6e au classement des écoles d'ingénieurs et écoles spécialisées en informatique et numérique · Talents du numérique

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr

</LES MÉTIERS ET LES DÉBOUCHÉS >

L'Administrateur Systèmes, Réseaux et Cybersécurité est le **gardien des clés numériques de l'entreprise**. Imaginez **Internet** comme un immense **royaume** rempli **d'informations et de données**. Le responsable cybersécurité **protège ces données** contre les attaques malveillantes. Il construit des **murs numériques**, appelés **pare-feux**, pour empêcher les intrus d'entrer. Il **traque** les signes de **comportement suspect** et met en place des **protocoles de sécurité** pour anticiper les attaques malveillantes.

L'Administrateur systèmes, réseaux et cybersécurité est un **profil recherché** par les entreprises de toutes tailles et tous secteurs d'activités. Le titre permet d'accéder à une **large gamme** de **métiers spécialisés** dans l'**administration des systèmes et réseaux**, ainsi que dans la **cybersécurité**, parmi lesquels :

- **Administrateur Systèmes et Réseaux** : Pilotage des infrastructures IT.
- **Ingénieur Réseaux et Sécurité** : Supervision et sécurisation des réseaux.
- **Consultant Cybersécurité** : Audit, conseil et déploiement de solutions de protection.
- **Responsable Infrastructure IT** : Gestion et optimisation des ressources IT.

35k €
Salaire moyen /an

</POUR QUI ? >

Les **formations** en **numérique** sont associées, à tort, aux sciences fondamentales. Le numérique est basé sur des **compétences variées**, c'est pourquoi **différents profils** peuvent trouver leur voie **au sein des métiers du numérique**.

Le **Bachelor Cybersécurité** est **ouvert à toutes et tous.** Une seule **condition**, être **titulaire** d'un titre de niveau 4 (**Bac**) pour une **entrée en 1ère année** ou de niveau 5 (**BAC+2**) pour une intégration en **3ème année**. Tu as un **fort intérêt** pour l'**informatique** et la **cybersécurité** ? Cette formation est faite pour toi !

</FINANCEMENT >

1ère, 2ème et 3ème année
en continu
7 000 € TTC par an

Inscription directe
en 3ème année en continu
8 500 € TTC

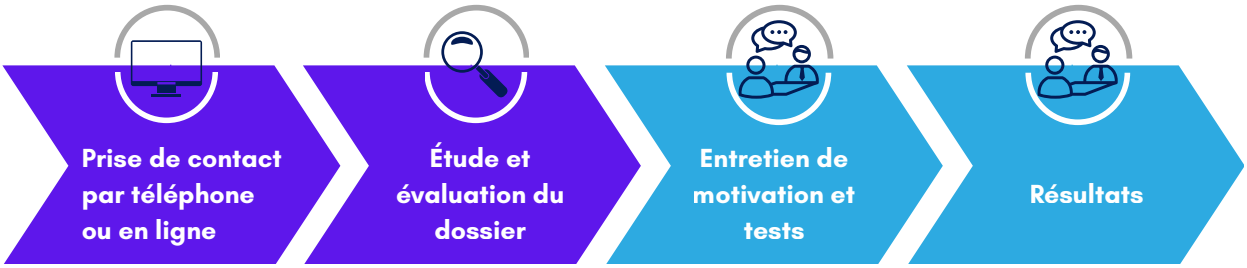
Si 3ème année effectuée
en alternance

Formation intégralement financée par l'entreprise

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr

</MODALITÉS D'ADMISSION>

L'admission se déroule en 4 temps :



Mise en relation sous 48 h

Réponse sous 48 h

</POURQUOI CHOISIR IMIE PARIS ?>

8 ans
D'expérience

11
Titres RNCP

1 000
Carrières lancées

80 %
Taux de réussite

4
Laboratoires
IA & IoT & Cybersécurité

École
à taille humaine

Au cœur de
l'écosystème francilien

Accompagnement
personnalisé

</INFOS PRATIQUES>

NOUS CONTACTER :

Par téléphone : **01 84 78 22 17**
Par e-mail : **contact@imie-paris.fr**
IMIE PARIS

NOUS RENCONTRER :

Lors de nos JPO et de nos événements entreprises.
Vérifiez notre agenda sur **www.imie-paris.fr**

NOS RENDEZ-VOUS DE L'ORIENTATION :

Pour parler de vos aspirations, de votre projet d'étude ou professionnel, de votre dossier scolaire, n'hésitez pas à prendre rendez-vous à **contact@imie-paris.fr**.

ACCESSIBILITÉ

Formation ouverte aux personnes en situation de handicap.
Pour plus d'informations, contactez notre référent(e) handicap :
service.pedagogique@imie-paris.fr

LOCALISATION

70, rue Anatole France
92300 Levallois-Perret

M3 Anatole France
L Clichy Levallois

</BOOTCAMP >

Le **boot camp,** c'est un **stage de perfectionnement** en mode **intensif** de 2 à 4 semaines.

Le **summer camp,** c'est une **immersion anglophone** au soleil.

Le **winter camp,** c'est une pause hivernale pour **glisser** sur les **pistes** et **vivre** une **aventure** avec sa **promotion**.

</PAROLES D'ÉTUDIANTS>

SCAN ME

MAX

Ce que **j'aime le plus** à propos de l'IMIE Paris, c'est que c'est une **école à taille humaine,** où on nous écoute !

MAX

C'est une **école** avec une **très bonne structure d'encadrement,** des **profs de qualité** et qui nous offre une **formation reconnue et qualifiée**

ABDESLAM

Les **cours** sont vraiment **axés sur la pratique**

ANAB

Les **formations** à l'IMIE Paris ne sont **pas uniquement réservées à la gent masculine**

UNE QUESTION ? 01 84 78 22 17 contact@imie-paris.fr