

**2026**

# Formations Numérique pour l'industrie

AUTOMATISATION / ROBOTISATION - CYBERSÉCURITÉ IT / OT - IA / DATA - IIOT



# ÉDITO

## Le Groupe Aforp vous accompagne vers le numérique

**Bienvenue à l'Aforp, Pôle formation UIMM Île-de-France.**

Le numérique n'est plus une option : il est devenu un levier stratégique majeur de compétitivité pour l'industrie. **Cybersécurité, data, automatisation, intelligence artificielle...** ces transformations redéfinissent les métiers, les compétences et les organisations.

Présent au plus près des entreprises, **agile, innovant et connecté aux enjeux technologiques et sociétaux**, le Groupe AFORP accompagne cette mutation depuis plus de 60 ans.

Pour répondre à l'accélération des besoins en compétences numériques industrielles, nous avons ouvert en septembre 2024 un **nouveau campus à Cachan**, entièrement dédié aux technologies d'avenir.

Nous proposons des parcours en alternance du **Bac au Master**, ainsi qu'une offre complète de **formation continue pour les salariés**, structurée autour de quatre domaines clés du numérique industriel : **Cybersécurité OT/IT, IIoT, IA & Data, Automatisation & Robotisation.**

Leader de l'apprentissage industriel en Île-de-France, **le Groupe AFORP accompagne chaque année près de 1 750 apprentis**, avec un taux d'insertion professionnelle de plus de 90 % dans les six mois suivant la formation. Intégrer l'AFORP, c'est choisir un métier d'avenir, des compétences durables et des formations diplômantes et certifiantes reconnues.

**Nous accompagnons également près de 3 900 salariés par an** dans le développement de leurs compétences et l'obtention de certifications professionnelles, avec une ambition forte : sécuriser l'employabilité tout au long de la vie professionnelle.

Partenaire de confiance des entreprises et des individus, l'AFORP permet à chacun de concrétiser son projet, notamment via le Compte Personnel de Formation (CPF).

**Ce guide illustre notre engagement** : former aujourd'hui les compétences numériques qui feront l'industrie de demain.



# SOMMAIRE<sup>2</sup>

		BASES DE L'IA ET DU MACHINE LEARNING	20	
		COLLECTE, TRAITEMENT ET QUALITÉ DES DONNÉES INDUSTRIELLES	21	
		ANALYSE PRÉDICTIVE APPLIQUÉE À L'INDUSTRIE	22	
		IA EMBARQUÉE ET TEMPS RÉEL (EDGE AI)	23	
		INTRODUCTION ET ENJEUX DE L'IIOT	24	
		TECHNOLOGIES ET PROTOCOLES IIOT	25	
		DÉPLOIEMENT ET PILOTAGE D'UN PROJET IIOT	26	
		MAINTENANCE PRÉDICTIVE ET OPTIMISATION	27	
		FORMATIONS EN ALTERNANCE	28	
	02	LE GROUPE AFORP		
	12	INTRODUCTION À L'AUTOMATISATION INDUSTRIELLE		
	13	ROBOTS ET COBOTS EN PRODUCTION		
	14	PROGRAMMATION DES AUTOMATES ET INTÉGRATION SYSTÈME		
	15	SUPERVISION ET OPTIMISATION CONTINUE		
	16	FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE		
	17	GOUVERNANCE ET NORMES (ISO 27002, IEC 62443)		
	18	SÉCURISATION DES SYSTÈMES OT / SCADA		
	19	RÉPONSE AUX INCIDENTS ET REPRISE D'ACTIVITÉ		



AUTOMATISATION / ROBOTISATION



IA / DATA



IIOT



CYBERSÉCURITÉ IT / OT

## FORMATIONS EN ALTERNANCE

30 BAC PRO CIEL - Cybersécurité, Informatique et réseaux, Electronique

31 BTS SIO -  
Option: SISR  
Option: SLAM

33 BTS CIEL -  
Option A : Informatique et réseaux  
Option B : Électronique et réseaux

35 ADMINISTRATEUR  
SYSTÈMES, RÉSEAUX ET  
CYBERSÉCURITÉ

36 CONCEPTEUR DE SYSTÈMES  
AUTOMATISÉS ET INTERFACES  
ASSOCIÉES

37 FORMATION « CARE » CYBER  
ADMINISTRATEUR DES RÉSEAUX  
D'ENTREPRISES

38 MASTER SÉCURITÉ  
INFORMATIQUE (MSI)



39 MASTER PROFESSIONNEL  
INGÉNIERIE DES RÉSEAUX  
ET SYSTÈMES - IRS



40 INGÉNIEUR SYSTÈMES, RÉSEAUX  
ET SÉCURITÉ - ISRS

41 EXPERT EN INGÉNIERIE ET  
DÉVELOPPEMENT DE LOGICIELS  
POUR L'INDUSTRIE

42 EXPERT EN NUMÉRISATION  
INDUSTRIELLE

43 TITRE TSSR - TECHNICIEN SUPÉRIEUR  
SYSTÈMES ET RÉSEAUX

44 TITRE TIP - TECHNICIEN  
INFORMATIQUE DE PROXIMITÉ

# UNE PÉDAGOGIE 4.0 AU SERVICE DES COMPÉTENCES INDUSTRIELLES

Le Groupe AFORP s'inscrit pleinement dans une démarche de **pédagogie 4.0**, en intégrant des méthodes d'apprentissage innovantes, immersives et adaptées aux profils des apprenants.

Depuis plusieurs années, l'AFORP déploie des parcours hybrides combinant présentiel, distanciel et contenus numériques, grâce à sa plateforme LMS EASI. Cette approche permet de proposer des **formations souples, modulaires et accessibles**, en phase avec les usages actuels.

## Des parcours personnalisés et évolutifs

Chaque formation est ajustée en fonction du profil d'apprentissage, des compétences initiales et des Objectifs professionnels.

**L'approche globale place** l'apprenant au cœur du dispositif, favorisant ainsi l'apprentissage par l'action et préparant efficacement aux enjeux concrets de l'industrie 4.0.

## Pour chaque formation, l'AFORP mobilise :

- Des solutions intégrant l'intelligence artificielle,
- Des outils collaboratifs (cloud, chat, forums), facilitant l'échange et le travail en équipe.

- Des environnements immersifs en présentiel conçus pour se rapprocher des situations industrielles.

## Des outils numériques innovants intégrés au cœur des apprentissages.

- **Réalité virtuelle (VR)** : habilitations électriques, manipulation de fluides, pilotage et maintenance de lignes robotisées ;
- **Réalité augmentée (AR)** : opérations de maintenance, changement de références, brasure à l'étain, assistance pas à pas ;
- **Lignes automatisées, robots et cobots**, pour évoluer dans des conditions proches de l'industrie du futur, en toute sécurité.



# PARTENAIRES & Certifications DE L'AFORP DANS LE NUMÉRIQUE

Le groupe AFORP est partenaire du CNAM, de Sorbonne Université et de Université Paris-Saclay.

L'AFORP est certifiée Microsoft, agréée Académie Cisco et centre de formation de formateurs Cisco.



Elle prépare aux certifications numériques suivantes :

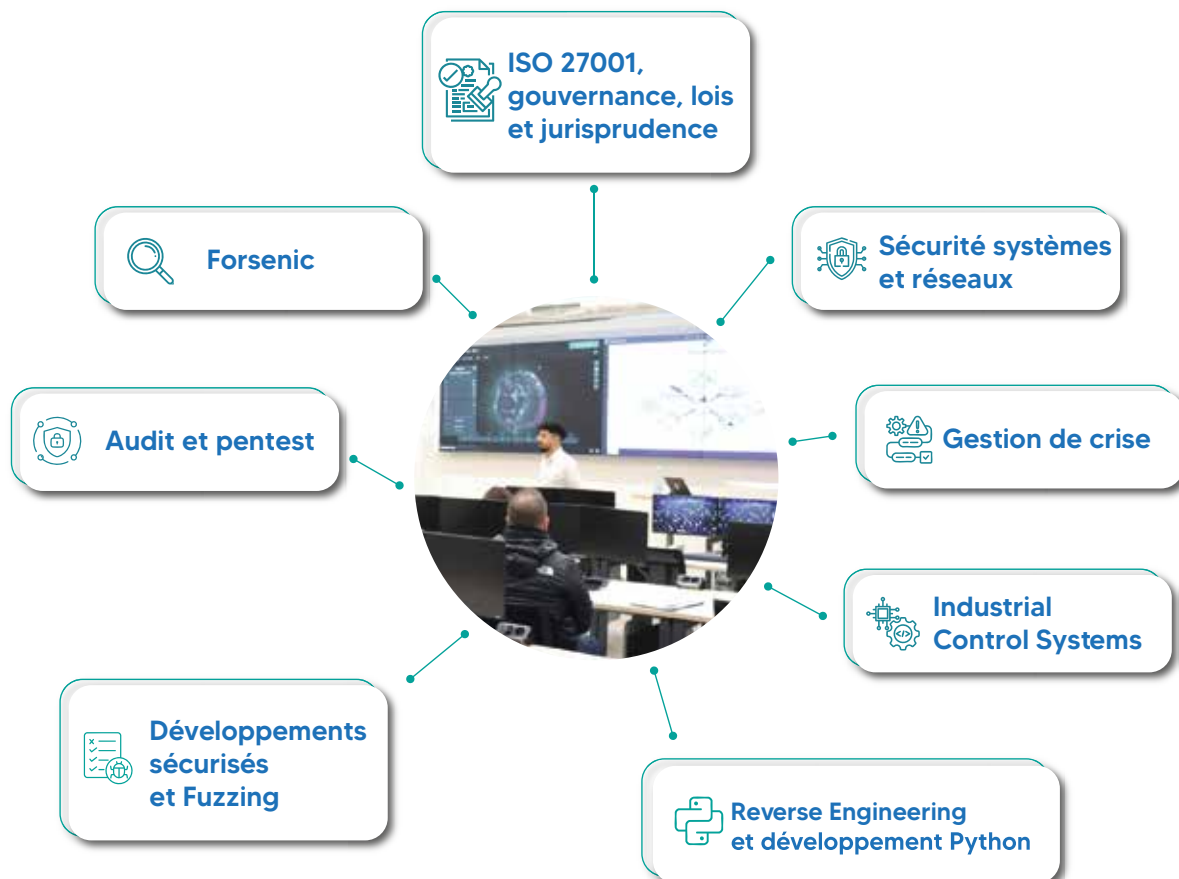
OSCP, CCNA, CyberOps, DevNet, PCAP

Le groupe Aforp est membre titulaire de l'association Talents du Numérique



Pour renforcer notre pédagogie le groupe Aforp dispose d'un SOC (Security Operations Center) : centre de surveillance de cybersécurité. Grâce à notre approche pédagogique, il permet aux entreprises de simuler des attaques pour former leurs équipes et renforcer leur capacité de réaction.

## Une pédagogie autour d'un soc



# CONSTRUISEZ VOTRE RÉUSSITE

Créé par et pour les entreprises industrielles et numériques, le Groupe Aforp - Pôle formation UIMM Île-de-France accompagne le développement des compétences des jeunes, salariés, demandeurs d'emploi.



## DÉFINIR VOTRE PROJET EN ENTREPRISE

- Orientation
- Accompagnement individualisé



## DÉVELOPPER VOS COMPÉTENCES

- Accompagnement par un tuteur en entreprise pour acquérir une expérience professionnelle
- Formateurs bénéficiant d'une expérience professionnelle en entreprise et reconnus comme spécialistes de leur domaine
- Pédagogie par projet et accompagnement personnalisé avec accès à une plateforme d'e-learning



## CERTIFIER VOS COMPÉTENCES

**Diplômes** et titres RNCP  
**Certifications** (CQPM, TOEIC, Voltaire...) et habilitations



## TROUVER UN CONTRAT EN ALTERNANCE OU UN STAGE

**Aide à la rédaction** de CV, lettre de motivation

**Ateliers techniques** pour démarcher et relancer les entreprises

**Préparation** à l'entretien de recrutement

**Job board** pour avoir accès à plus de 700 offres de contrat en alternance et rencontrer des entreprises

**Job dating** pour rencontrer des entreprises



# CONTRATS & FINANCEMENTS

## Contrat d'apprentissage

Pour former des jeunes de 16 à 29 ans, le contrat d'apprentissage permet de préparer des diplômes et titres reconnus, du niveau 3 - CAP au niveau 7 - master.

## Contrat de professionnalisation

Adapté aux besoins de recrutement rapide ou de reconversion, il concerne les jeunes de moins de 26 ans ou des demandeurs d'emploi. Il permet de développer des compétences ciblées sur un métier industriel précis.

Les + de l'alternance



## Contrat de transition professionnelle

Outil de reconversion sécurisée, il permet à un salarié d'évoluer vers un métier industriel porteur tout en conservant une rémunération. Ce dispositif est soumis à éligibilité et validation du projet.

## CPF - Compte Personnel de Formation

Le CPF permet aux salariés de financer des formations certifiantes, notamment sur les compétences industrielles et numériques. Il peut être mobilisé seul ou complété par des abondements entreprise, dans une logique de co-investissement compétences.

## POEI / POEC

Ces dispositifs répondent aux besoins immédiats des entreprises industrielles. La POEI est directement liée à un recrutement identifié, tandis que la POEC permet de former plusieurs candidats sur des compétences en tension. Financées via France Travail et les OPCO.

# OFFRE FORMATION CONTINUE

## AUTOMATISATION / ROBOTISATION

L'automatisation consiste à concevoir des systèmes capables d'exécuter des tâches de manière autonome grâce à des algorithmes et des logiciels industriels.

La robotisation complète cette approche en déployant des robots ou cobots pour réaliser des tâches répétitives sur des lignes de production.



## CYBERSÉCURITÉ IT / OT

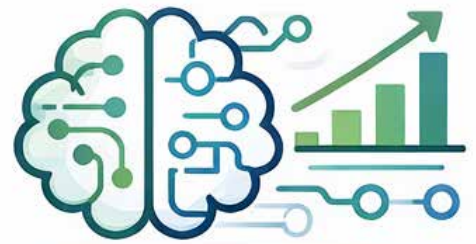
La cybersécurité regroupe l'ensemble des moyens permettant de protéger les systèmes d'information et les systèmes industriels (IT & OT) contre les menaces, en sécurisant les réseaux, les communications, les protocoles, les systèmes et les équipements.

Elle vise une sécurité globale à 360° garantissant la continuité, la sûreté et la fiabilité des environnements numériques et industriels.



## IA / DATA

L'IA et la Data couvrent l'ensemble du cycle de vie des données : collecte, stockage, traitement, analyse et restitution, afin d'optimiser les informations pour la prise de décision. Elles mettent en avant les données provenant de systèmes différents (IT et OT) grâce à des algorithmes, des bases de données adaptées et des outils de visualisation.



## IIOT (INDUSTRIAL INTERNET OF THINGS)

L'IloT : l'interconnexion des équipements industriels se fait grâce à des réseaux et des protocoles de communication dans l'objectif de collecter, exploiter et sécuriser les données issues des systèmes de production. L'IloT permet de superviser, optimiser et piloter des projets industriels connectés de bout en bout.



# INTRODUCTION À L'AUTOMATISATION INDUSTRIELLE



Automatisation / Robotisation

Ce module introduit les fondamentaux de l'automatisation industrielle, ses composants (capteurs, actionneurs, automates) et ses applications. Les participants découvriront comment identifier les opportunités d'automatisation et améliorer la productivité et la sécurité des processus.

## Objectifs

- Comprendre les composants d'un système automatisé (capteurs, actionneurs, automates).
- Identifier les opportunités d'automatisation.
- Analyser l'impact sur la productivité et la sécurité.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 380 € HT/ jour  
ou Intra : 1500 € HT / jour pour un groupe

## Moyens Pédagogiques

- Apports théoriques et démonstrations
- Études de cas pratiques
- Supports numériques et e-learning

## Évaluation & suivi

- Exercices de cas pratiques
- Études de cas en groupe
- QCM de validation des acquis

## La FORMATION

- Introduction aux systèmes automatisés
- Capteurs, actionneurs et automates programmables (PLC)
- Applications industrielles de l'automatisation
- Supervision et contrôle des processus automatisés
- Cas d'usage : automatisation du tri de colis dans la logistique ; pilotage automatique de température dans l'agroalimentaire
- Introduction aux enjeux de l'automatisation
- Impacts organisationnels et humains
- Bonnes pratiques de sécurité dans l'automatisation

## Prérequis

Culture générale en systèmes industriels  
Notions en électronique/électrotechnique appréciées

## Pour qui

Techniciens, ingénieurs, responsables de production et maintenance

# ROBOTS & COBOTS EN PRODUCTION



Automatisation /  
Robotisation

Ce module explore l'intégration des robots et cobots dans les environnements industriels. Les participants apprendront à distinguer les différents types de robots, cobots et AGV, à analyser l'ergonomie des cellules robotisées et à identifier les bénéfices en santé au travail et en productivité.

## Objectifs

- Distinguer robot, cobot et AGV.
- Analyser l'ergonomie et la sécurité des cellules robotisées.
- Identifier les bénéfices en productivité et santé au travail.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 380 € HT/ jour  
ou Intra : 1500 € HT / jour pour un groupe

## Moyens Pédagogiques

- Démonstrations et études de cas pratiques
- Ateliers collaboratifs autour de robots et cobots
- Supports numériques et e-learning

## Évaluation & suivi

- Exercices pratiques et ateliers de déploiement
- Études de cas et restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Panorama des robots et cobots en production
- Robots, cobots, AGV : définitions et différences
- Ergonomie et sécurité dans l'intégration robotisée
- Études de cas d'applications en production
- Cas d'usage : intégration d'un cobot pour vissage répétitif en électronique ; robot de peinture autonome dans l'industrie automobile
- Compréhension des enjeux humains et organisationnels
- Ergonomie et santé au travail
- Introduction aux perspectives de la robotisation

### Prérequis

Connaissances générales en automatisation  
Notions de sécurité industrielle appréciées

### Pour qui ?

Techniciens, ingénieurs, responsables de production et maintenance

# PROGRAMMATION DES AUTOMATES & INTÉGRATION SYSTÈME



Automatisation / Robotisation

Ce module forme les participants à la programmation des automates industriels et à l'intégration des systèmes dans les environnements de production. Ils apprendront à utiliser les langages d'automatisme (Ladder, Grafcet) et à intégrer les échanges avec SCADA, IHM ou bus industriels.

## Objectifs

- Maîtriser les langages d'automatisme (Ladder, Grafcet).
- Intégrer les échanges avec SCADA, IHM ou bus industriels.
- Développer des applications automatisées adaptées à la production.

## Infos

### DURÉE

3 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 380 € HT/ jour  
ou Intra : 1500 € HT / jour pour un groupe

## Moyens Pédagogiques

- Exercices pratiques de programmation
- Simulations sur automates et systèmes industriels
- Supports numériques et e-learning

## Évaluation & suivi

- Exercices pratiques sur automates
- Études de cas et analyses collectives
- QCM de validation des acquis

## La FORMATION

- Introduction aux automates programmables (PLC)
- Langages de programmation Ladder et Grafcet
- Intégration avec systèmes SCADA, IHM et bus industriels
- Mise en œuvre pratique sur lignes simulées
- Cas d'usage : programmation d'un automate pour ligne d'embouteillage ; gestion synchrone de convoyeurs via Grafcet
- Introduction aux architectures d'automatisation
- Gestion de projet d'intégration industrielle
- Bonnes pratiques de sécurité et fiabilité

## Prérequis

Connaissances de base en automatisation  
Notions d'électrotechnique et d'informatique industrielle

## Pour qui ?

Techniciens et ingénieurs en automatisation, responsables maintenance et production

# SUPERVISION & OPTIMISATION CONTINUE



Automatisation /  
Robotisation

Ce module permet aux participants de mettre en place des outils de supervision industrielle (SCADA, MES) et de suivre en temps réel les indicateurs de performance. Ils apprendront à détecter rapidement les dérives et à améliorer en continu la production.

## Objectifs

- Mettre en place des outils de supervision (SCADA, MES).
- Suivre les indicateurs de performance en temps réel (OEE, TRS).
- Détecter les dérives et proposer des actions correctives.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 420 € HT / jour  
ou Intra : 1650 € HT / jour pour un groupe

## Moyens Pédagogiques

- Exercices pratiques sur outils SCADA/MES
- Études de cas industriels
- Supports numériques et e-learning

## Évaluation & suivi

- Études de cas et restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction à la supervision et ses enjeux
- Présentation des outils SCADA et MES
- Suivi en temps réel des indicateurs OEE, TRS
- Détection des dérives et optimisation continue
- Cas d'usage : suivi en temps réel de l'énergie consommée par ligne ; alerte automatique sur dérive de cadence
- Introduction aux démarches d'amélioration continue
- Gestion de la performance et pilotage industriel
- Communication et collaboration autour des indicateurs

## Prérequis

Connaissances de base en automatisation et supervision  
Notions en gestion de production industrielle

## Pour qui ?

Techniciens, ingénieurs, responsables production et qualité

# FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE



Cybersécurité  
IT / OT

Ce module apporte les bases indispensables pour comprendre et sécuriser les environnements industriels (OT) interconnectés aux systèmes d'information (IT). Il permet d'identifier les cybermenaces propres aux systèmes industriels, de maîtriser les principes de gestion des risques et d'appréhender les bonnes pratiques de sécurisation dans un contexte de continuité de production.

## Objectifs

- Comprendre les risques, menaces et typologie des attaques cyber-industrielles.
- Assimiler les principes d'analyse de risques, politiques et gestion d'incidents.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT / jour ou

Intra : 2000 € HT / jour pour un groupe (12 pers max)

## Moyens Pédagogiques

- Apports théoriques illustrés d'exemples concrets
- Études de cas et simulations industrielles (SOC pédagogique, usine 4.0 virtuelle)
- Supports numériques et e-learning complémentaires

## Évaluation & suivi

- Études de cas évaluées en groupe
- QCM de validation des acquis

## La FORMATION

- Panorama des cybermenaces dans l'industrie (malwares, ransomware, sabotage, espionnage)
- Principes de cybersécurité appliqués aux environnements OT/IT
- Introduction aux normes et référentiels (ANSSI, ISO/IEC, IEC 62443)
- Méthodologie d'analyse des risques et gestion d'incidents
- Études de cas et mise en situation (attaque simulée, confinement post-incident)
- Gouvernance SSI et conformité (ANSSI, ISO 27001, IEC 62443)
- Culture du risque et communication en situation d'incident
- Bonnes pratiques utilisateurs et sensibilisation

## Prérequis

Connaissances de base en réseaux et systèmes informatiques

Familiarité avec l'environnement industriel souhaitée

## Pour qui ?

Professionnels en poste dans l'IT/OT ou ingénieurs industriels

# GOVERNANCE & NORMES (ISO 27002, IEC 62443)



Ce module présente les référentiels incontournables de cybersécurité (ISO 27002, IEC 62443) et apporte une méthodologie pour structurer la gouvernance des systèmes d'information et industriels. Il permet aux participants de comprendre le rôle des parties prenantes et d'intégrer la cybersécurité dans une démarche globale de conformité et d'amélioration continue.



Cybersécurité  
IT / OT

## Objectifs

- Maîtriser les principaux référentiels (ISO, IEC) et savoir les appliquer au contexte industriel.
- Structurer une gouvernance cyber adaptée.
- Intégrer les rôles et responsabilités (CISO, opérationnels).

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise



### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe

## Moyens Pédagogiques

- Études de cas pratiques (audit fictif, revue documentaire)
- Supports normatifs et grilles d'audit
- Apports théoriques et échanges collectifs

## Évaluation & suivi

- Études de cas pratiques
- Restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction aux enjeux de la gouvernance en cybersécurité
- Présentation des normes et référentiels (ISO 27001/27002, IEC 62443)
- Mise en place d'une PSSI et alignement avec la stratégie d'entreprise
- Définition des rôles et responsabilités des acteurs (RSSI, direction, opérationnels)
- Étude de cas : revue de conformité dans une usine sous directive NIS2
- Gouvernance d'entreprise appliquée à la cybersécurité
- Rôles et responsabilités des parties prenantes (RSSI, opérationnels)
- Gestion des risques et alignement avec NIS2

## Prérequis

Connaissances de base en cybersécurité  
Compréhension des environnements industriels

## Pour qui ?

Responsables cybersécurité, RSSI, responsables qualité, vs de projets industriels

# SÉCURISATION DES SYSTÈMES OT/SCADA



Cybersécurité  
IT / OT

Ce module permet d'identifier les menaces spécifiques aux environnements OT/SCADA et de mettre en œuvre des mesures concrètes de protection. Les participants apprendront à appliquer segmentation, patching et défense périmétrique afin de réduire l'exposition des systèmes industriels aux cyberattaques.

## Objectifs

- Identifier les menaces spécifiques aux environnements OT (SCADA, brute force, ransomware).
- Appliquer segmentation, patching et défense périmétrique.
- Mettre en œuvre des mesures de sécurité adaptées aux contraintes de production.

## Infos

### DURÉE

3 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe

## Moyens Pédagogiques

- Apports théoriques et démonstrations techniques
- Simulations pratiques sur environnements virtualisés OT/SCADA
- Études de cas (centrale énergétique, usine connectée)

## Évaluation & suivi

- Exercices pratiques en environnement simulé
- Études de cas et analyses collectives
- QCM de validation des acquis

## La FORMATION

- Panorama des menaces sur les systèmes OT/SCADA
- Bonnes pratiques de sécurisation des infrastructures industrielles
- Techniques de segmentation réseau et défense périmétrique
- Gestion des mises à jour et patching en milieux critique
- Étude de cas : isolation d'un réseau SCADA après intrusion
- Sensibilisation aux risques OT/SCADA
- Méthodologies de sécurité industrielle
- Retours d'expérience (ransomware, sabotage industriel)

### Prérequis

Connaissances de base en réseaux industriels

Familiarité avec les architectures SCADA/ PLC souhaitée

### Pour qui ?

Responsables OT, ingénieurs systèmes industriels, équipes SSI/DSI

# RÉPONSE AUX INCIDENTS & REPRISE D'ACTIVITÉ

Ce module fournit les méthodes et outils nécessaires pour préparer et gérer efficacement une réponse aux incidents cyber affectant un environnement industriel. Les participants apprendront à élaborer un plan de gestion de crise, définir un protocole de communication, et mettre en place des procédures de reprise d'activité (PRA/PCA) adaptées aux contraintes de production.



Cybersécurité  
IT / OT

## Objectifs

- Élaborer un plan de crise et protocole de communication.
- Simuler et améliorer les procédures de reprise d'activité.
- Préparer une organisation résiliente face aux cyber-attaques.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe

## Moyens Pédagogiques

- Études de cas pratiques et mises en situation
- Ateliers collaboratifs pour la construction de plans PRA/PCA
- Simulations de gestion de crise en environnement industriel

## Évaluation & suivi

- Exercices pratiques et simulations
- Restitutions collectives des plans de crise
- QCM de validation des acquis

## La FORMATION

- Introduction à la gestion de crise en cybersécurité
- Élaboration d'un plan PRA/PCA adapté aux environnements OT/IT
- Mise en place d'un protocole de communication en situation de crise
- Simulations d'incidents et retours d'expérience
- Étude de cas : mise en place d'un PRA après attaque ransomware
- Communication de crise et gestion des parties prenantes
- Culture de la résilience et amélioration continue
- Sensibilisation à l'importance du retour d'expérience (REX)

### Prérequis

Connaissances de base en cybersécurité  
Familiarité avec l'organisation industrielle et les contraintes de production

### Pour qui ?

Managers industriels, ingénieurs de production, responsables digitalisation et innovation



IA / Data

Ce module introduit les concepts fondamentaux de l'intelligence artificielle et du machine learning. Les participants apprendront à distinguer les différents types d'apprentissage (supervisé, non supervisé, réseaux de neurones) et à comprendre leurs applications concrètes dans l'industrie.

## Objectifs

- Comprendre les principes fondamentaux de l'IA, du machine learning et des cas d'usage industriels.
- Distinguer apprentissage supervisé, non-supervisé, et réseaux de neurones.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe



## Moyens Pédagogiques

- Apports théoriques et démonstrations pratiques
- Études de cas appliqués à l'industrie
- Supports numériques et e-learning

## Évaluation & suivi

- Études de cas pratiques
- Exercices appliqués en groupe
- QCM de validation des acquis

## La FORMATION

- Introduction à l'IA et au machine learning
- Présentation des principaux algorithmes et modèles
- Apprentissage supervisé vs non supervisé
- Introduction aux réseaux de neurones
- Cas d'usage : tri automatisé de produits défectueux par reconnaissance d'image ; recommandation de maintenance en IA faible
- Introduction aux concepts fondamentaux de l'IA
- Enjeux stratégiques de l'IA pour l'industrie
- Cas d'usage industriels illustratifs

### Prérequis

Culture numérique générale  
Notions en mathématiques/statistiques appréciées

### Pour qui ?

Managers, ingénieurs, techniciens souhaitant acquérir les bases de l'IA appliquée à l'industrie

# COLLECTE, TRAITEMENT & QUALITÉ DES DONNÉES INDUSTRIELLES



IA / Data



Ce module initie les participants aux techniques de collecte, de nettoyage et de structuration des données industrielles. Il aborde les enjeux de qualité, de gouvernance et de cycle de vie des données pour les rendre exploitables par des outils d'analyse et d'IA.

## Objectifs

- Apprendre à collecter, nettoyer et structurer les données issues des capteurs ou systèmes existants.
- Comprendre les enjeux de qualité, gouvernance et cycle de vie des données.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe (12 pers max)

## Moyens Pédagogiques

- Ateliers pratiques de traitement de données
- Études de cas appliqués aux environnements industriels
- Supports numériques et e-learning

## Évaluation & suivi

- Travaux pratiques sur données réelles ou simulées
- Restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction aux données industrielles et leurs sources
- Collecte des données issues des capteurs et systèmes OT/IT
- Nettoyage, normalisation et structuration des données
- Qualité et gouvernance des données (pipeline, anonymisation, GDPR)
- Cas d'usage : mise en place d'un pipeline de données pour un atelier connecté ; échantillonnage automatique des données de production
- Gouvernance et qualité des données
- Cycle de vie des données industrielles
- Aspects réglementaires et conformité (GDPR)

## Prérequis

Connaissances de base en traitement de données

Notions en informatique industrielle ou systèmes OT/IT appréciées

## Pour qui ?

Ingénieurs, techniciens, responsables qualité et data managers

# ANALYSE PRÉDICTIVE APPLIQUÉE À L'INDUSTRIE



IA / Data

Ce module permet aux participants d'exploiter les données industrielles pour anticiper les pannes, optimiser la qualité et améliorer la performance des processus. Il s'appuie sur des méthodes de modélisation prédictive et des outils analytiques adaptés au contexte industriel.

## Objectifs

- Construire des modèles prédictifs sur données historiques.
- Appliquer l'IA à la maintenance, la qualité et la chaîne logistique.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 420 € HT/ jour  
ou Intra : 1650 € HT / jour pour un groupe (12 pers max)

## Moyens Pédagogiques

- Apports théoriques et démonstrations pratiques
- Études de cas appliqués à l'industrie
- Supports numériques et e-learning

## Évaluation & suivi

- Études de cas pratiques
- Exercices appliqués en groupe
- QCM de validation des acquis

## La FORMATION

- Introduction à l'analyse prédictive et ses enjeux
- Méthodes de régression et détection d'anomalies
- Construction de modèles prédictifs à partir de données historiques
- Tableaux de bord et indicateurs de performance (dashboard)
- Cas d'usage : prédiction des incidents sur moteurs industriels ; ajustement automatique des cadences en fonction de la qualité
- Introduction aux concepts de modélisation prédictive
- Compréhension des bénéfices pour l'industrie
- Gestion et valorisation des données industrielles

### Prérequis

Connaissances de base en analyse de données  
Notions en statistiques ou machine learning appréciées

### Pour qui ?

Ingénieurs, techniciens, responsables production, data analysts industriels

# IA EMBARQUÉE & TEMPS RÉEL (EDGE AI)



IA / Data

Ce module forme les participants au déploiement de modèles d'intelligence artificielle directement sur site (capteurs, passerelles, microcontrôleurs), sans dépendre du cloud. Ils apprendront à gérer les contraintes de calcul, consommation et latence propres à l'Edge Computing.

## Objectifs

- Déployer des modèles IA sur capteurs ou passerelles (Edge computing).
- Maîtriser les contraintes de calcul, consommation et latence.
- Comprendre les architectures d'IA embarquée adaptées aux environnements industriels.

## Infos

### DURÉE

3 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe (12 pers max)

## Moyens Pédagogiques

- Ateliers pratiques sur plateformes Edge AI
- Simulations et cas d'usage industriels
- Supports numériques et e-learning

## Évaluation & suivi

- Exercices pratiques et ateliers de déploiement
- Études de cas et restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction à l'IA embarquée et à l'Edge computing
- Contraintes techniques : consommation, latence, puissance de calcul
- Déploiement de modèles IA sur capteurs et passerelles
- Optimisation et gestion des ressources locales
- Cas d'usage : caméra de détection de défauts sur ligne de production ; tri optique en temps réel sans cloud
- Compréhension des enjeux stratégiques de l'IA embarquée
- Cas d'usage industriels (qualité, maintenance, production)
- Gouvernance et intégration de l'Edge AI dans l'organisation

## Prérequis

Connaissances de base en IA et analyse de données  
Notions en systèmes embarqués ou IoT appréciées

## Pour qui ?

Ingénieurs, techniciens, responsables OT/IT et data engineers



Ce module propose une première approche de l'Internet Industriel des Objets (IIoT), ses différences avec l'IoT grand public, ainsi que ses impacts stratégiques pour l'industrie 4.0. Les participants découvriront les bénéfices de l'IIoT en termes de performance, réactivité et compétitivité.

## Objectifs

- Différencier IIoT/IoT grand public et identifier les bénéfices industriels.
- Comprendre les enjeux stratégiques de l'IIoT pour l'industrie 4.0.

## Infos

### DURÉE

1 jour

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe (12 pers max)

## Moyens Pédagogiques

- Apports théoriques avec exemples concrets
- Illustrations de cas réels d'industries connectées
- Supports numériques et e-learning complémentaires

## Évaluation & suivi

- Études de cas pratiques
- Restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Panorama de l'IoT et de l'IIoT : définitions et enjeux
- Applications clés de l'IIoT dans les industries (production, énergie, logistique)
- Les bénéfices en termes de performance, traçabilité, qualité et maintenance
- Facteurs de réussite et freins à l'adoption
- Cas d'usage : surveillance continue température/pression en agroalimentaire ; alertes en temps réel sur lignes sensibles
- Enjeux stratégiques pour l'industrie 4.0
- Facteurs humains et organisationnels liés à l'adoption de l'IIoT
- Perspectives et tendances futures

### Prérequis

Culture générale en industrie et technologies numériques

### Pour qui ?

Managers industriels, ingénieurs de production, responsables digitalisation et innovation

# TECHNOLOGIES & PROTOCOLES IIOT



IIOT (Industrial Internet of Things)

Ce module permet de comprendre les technologies, protocoles et architectures de communication propres à l'Internet Industriel des Objets (IIoT). Les participants apprendront à connecter des équipements hétérogènes en sécurisant les flux et en fiabilisant les échanges de données.

## Objectifs

- Comprendre MQTT, OPC-UA, Edge, protocoles industriels.
- Identifier les enjeux de connectivité et d'intégration dans un environnement industriel.
- Appliquer les bonnes pratiques de sécurisation des communications IIoT.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 460 € HT/ jour  
ou Intra : 1800 € HT / jour pour un groupe

## Moyens Pédagogiques

- Ateliers pratiques sur protocoles IIoT (MQTT, OPC-UA)
- Simulations d'architectures Edge et Cloud
- Études de cas et démonstrations industrielles

## Évaluation & suivi

- Travaux pratiques sur protocoles IIoT
- Restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction aux technologies et protocoles IIoT
- Présentation de MQTT, OPC-UA et protocoles industriels
- Architectures Edge et Cloud appliquées à l'IIoT
- Sécurisation des flux de données et contraintes spécifiques
- Cas d'usage : choix d'un protocole pour remonter des données machines ; architecture Edge pour usine isolée
- Concepts de connectivité et d'interopérabilité
- Gouvernance et standards de communication IIoT
- Facteurs humains et organisationnels liés à l'intégration

## Prérequis

Connaissances de base en réseaux et systèmes industriels  
Notions sur l'IoT et la digitalisation industrielle

## Pour qui ?

Ingénieurs, techniciens OT/IT, responsables digitalisation et innovation

# DÉPLOIEMENT & PILOTAGE D'UN PROJET IIOT



IIOT (Industrial Internet of Things)

Ce module fournit les méthodes et outils nécessaires pour structurer et piloter un projet IIoT. Les participants apprendront à concevoir un POC, à mesurer le ROI, à gérer les risques et à conduire un déploiement à l'échelle industrielle.

## Objectifs

- Structurer un projet IIoT (POC, budget, pilote).
- Évaluer le ROI et anticiper les risques.
- Mener un déploiement à l'échelle en assurant la gouvernance du projet.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 420 € HT/ jour  
ou Intra : 1650 € HT / jour pour un groupe (12 pers max)



## Moyens Pédagogiques

- Études de cas pratiques
- Ateliers collaboratifs de gestion de projet IIoT
- Simulations de déploiement industriel

## Évaluation & suivi

- Études de cas pratiques
- Restitutions collectives
- QCM de validation des acquis

## La FORMATION

- Introduction au cycle de vie d'un projet IIoT
- Méthodologie de conception d'un POC
- Budget, ROI et gestion des risques
- Gouvernance et pilotage de projets IIoT
- Cas d'usage : pilotage d'une usine smart city ; projet IIoT pour contrôle énergétique municipal
- Gouvernance et organisation projet
- Méthodologies de gestion des risques
- Communication et gestion des parties prenantes

### Prérequis

Connaissances générales en gestion de projet  
Notions de base sur l'IIoT et ses applications industrielles

### Pour qui ?

Chefs de projets, ingénieurs OT/IT,  
responsables innovation et digitalisation

# MAINTENANCE PRÉDICTIVE & OPTIMISATION



IIOT (Industrial Internet of Things)

Ce module forme les participants à l'utilisation de l'IloT et des données industrielles pour anticiper les pannes et optimiser la **Durée** de vie des équipements. Il permet de concevoir des modèles prédictifs, d'analyser les données capteurs et de mettre en œuvre une stratégie de maintenance proactive.

## Objectifs

- Créer des modèles prédictifs sur données capteurs.
- Réduire les temps d'arrêt non planifiés.
- Améliorer l'efficacité et prolonger la Durée de vie des équipements.

## Infos

### DURÉE

2 jours

### LIEUX

Campus AFORP (Cachan, Tremblay) ou intra-entreprise

### COÛT

Inter : 520 € HT/ jour  
ou Intra : 2000 € HT / jour pour un groupe

## Moyens Pédagogiques

- Études de cas industriels (automobile, agroalimentaire)
- Simulations et mise en œuvre de modèles prédictifs
- Supports numériques et e-learning complémentaires

## Évaluation & suivi

- Exercices pratiques de modélisation
- Études de cas et analyses collectives
- QCM de validation des acquis

## La FORMATION

- Introduction à la maintenance prédictive et ses enjeux
- Collecte et analyse des données capteurs (température, vibration, pression)
- Construction de modèles prédictifs et jumeaux numériques
- Mise en œuvre d'alertes et indicateurs de performance
- Cas d'usage : maintenance prédictive sur ligne automobile ; réduction des coûts via capteurs vibration
- Culture de la maintenance proactive
- Organisation et pilotage de la maintenance prédictive
- Communication et gestion du changement

## Prérequis

Connaissances de base en systèmes industriels et données capteurs

Notions en statistiques ou data science appréciées

## Pour qui ?

Ingénieurs et techniciens de maintenance, responsables OT/IT, responsables production



# **FORMATIONS**

# **EN ALTERNANCE**

# FORMATIONS EN ALTERNANCE

## INFORMATIQUE DÉVELOPPEMENT INDUSTRIEL (DEV, IOT, DATA)

### BAC +5

Cycle Master / Mastère

EXPERT EN INGÉNIERIE ET DÉVELOPPEMENT DE LOGICIELS POUR L'INDUSTRIE

EXPERT EN NUMÉRISATION INDUSTRIELLE

### BAC +3

Titre niveau 6

CONCEPTEUR DE SYSTÈMES AUTOMATISÉS ET INTERFACES ASSOCIÉES

### BAC +2

Titre niveau 5

BTS SIO - Option SLAM  
BTS CIEL - Option ER

### BAC

Titre niveau 4

TITRE TIP - TECHNICIEN INFORMATIQUE DE PROXIMITÉ

BAC PRO CIEL

## CYBERSECURITÉ

MASTER MSI



MASTER IRS  
Option Cybersécurité



CYBER ADMINISTRATEUR DES RÉSEAUX D'ENTREPRISES (CARE) M1

ADMINISTRATEUR SYSTÈMES, RÉSEAUX ET SÉCURITÉ

TSSR - TECHNICIEN SUPÉRIEUR SYSTÈMES ET RÉSEAUX

BTS SIO - Option SISR  
BTS CIEL - Option IR

## SYSTÈMES ET RÉSEAUX

INGÉNIER SYSTÈME RÉSEAUX ET CYBERSÉCURITÉ

MASTER IRS  
Option Réseaux et Systèmes



# BAC PRO CIEL - CYBERSÉCURITÉ, INFORMATIQUE & RÉSEAUX, ELECTRONIQUE

Option Solutions d'Infrastructure, Systèmes et Réseaux

Titre niveau 4 RNCP : 37489

Le baccalauréat professionnel « Cybersécurité, Informatique et réseaux, Électronique » (CIEL) est un diplôme de niveau 4 qui a pour objet de former des techniciennes ou techniciens capables d'intervenir dans les processus de réalisation et de maintenance de produits électroniques, dans la mise en œuvre de réseaux informatiques, et dans la valorisation de la donnée en intégrant les enjeux de cybersécurité.

## Objectifs

Analyser des besoins, rechercher et choisir une solution adaptée

Gérer et administrer un parc (matériels et logiciels) informatique

Produire des livrables en réponse à un cahier des charges intégrant les dimensions économique, juridique et managériale

Concevoir, produire et maintenir des solutions d'infrastructures réseau ou des solutions applicatives

Assurer et maintenir la sécurité des systèmes d'information

Fournir des services informatiques aux utilisateurs (installation, formation...)

Présenter un rapport d'activité

## Infos

### DURÉE

3 ans

### LIEUX

Cachan, Mantes-la-Ville, Tremblay-en-France

### RYTHME

2 semaines en CFA /

2 semaines en entreprise

## Prérequis

Avoir plus de 16 ans

Bac en 1 an - bac ou sortie terminale

Bac en 2 ans - 1ère STI 2D

Bac en 3 ans - 3ème des collèges

## La FORMATION

### FORMATION TECHNIQUE - 1350 h

- Gestion de projet et communication
- Réalisation et maintenance des produits électroniques
- Mise en œuvre de réseaux informatiques
- Valorisation de la donnée et cybersécurité
- Anglais technique
- Eco-gestion
- Préparation et certification habilitation électrique
- Prévention Santé Environnement

### CONDUITE DE PROJET

- Réalisation de maquettes et prototypes sur différents systèmes
- Participation à des actions humanitaires

### FORMATION GÉNÉRALE - 675 h

- Français, Histoire/ géographie et enseignement moral et civique
- Co-intervention français atelier
- Mathématiques
- Co-intervention mathématiques-atelier
- TP de sciences physiques
- Arts appliqués et cultures artistiques
- Anglais
- Éducation physique et sportive

# BTS SIO - SISR : SERVICES INFORMATIQUES AUX ORGANISATIONS

Option Solutions d'Infrastructure, Systèmes et Réseaux

Titre niveau 5 RNCP : 40792

Le technicien est formé à la cybersécurisation d'une infrastructure réseau, d'un système ou d'un service. Il administre, modifie et adapte les solutions d'infrastructure ainsi que la qualité de service des équipements du réseau informatique.

## Objectifs

Analyser des besoins, rechercher et choisir une solution adaptée

Gérer et administrer un parc (matériels et logiciels) informatique

Produire des livrables en réponse à un cahier des charges intégrant les dimensions économique, juridique et managériale

Concevoir, produire et maintenir des solutions d'infrastructures réseau ou des solutions applicatives

Assurer et maintenir la sécurité des systèmes d'information

Fournir des services informatiques aux utilisateurs (installation, formation...)

Présenter un rapport d'activité

## Infos

### DURÉE

2 ans

### LIEUX

Cachan, Tremblay-En-France

### RYTHME

2 semaines en CFA /

2 semaines en entreprise

## Prérequis

Bac général, Bac STI 2D, voir autres profils  
Bac Pro CIEL

## La FORMATION

- Culture économique, juridique et managériale pour l'informatique
- Algorithmie appliquée
- Administration des systèmes et des réseaux
- Cybersécurité des services informatiques
- Supports et mise à disposition des services informatiques
- Projets personnalisés encadrés
- Préparation et certification habilitation électrique
- Culture générale et expression
- Mathématiques
- Langue vivante-anglais
- Formation spécifique
- Préparation et certification Voltaire
- Parcours d'intégration : RNG
- Proactivité
- Positionnement / Remédiation



# BTS SIO - SLAM : SERVICES INFORMATIQUES AUX ORGANISATIONS

Option Solutions Logicielles et Applications Métiers

Titre niveau 5 RNCP : 35340

Le technicien est formé à la cybersécurisation d'une solution applicative et de son développement. Il participe à la conception, au développement, ainsi qu'au déploiement et à la maintenance des composants logiciels d'une solution applicative.

## Objectifs

Analyser des besoins, rechercher et choisir une solution adaptée

Gérer et administrer un parc (matériels et logiciels) informatique

Produire des livrables en réponse à un cahier des charges intégrant les dimensions économique, juridique et managériale

Concevoir, produire et maintenir des solutions d'infrastructures réseau ou des solutions applicatives

Assurer et maintenir la sécurité des systèmes d'information

Fournir des services informatiques aux utilisateurs (installation, formation...)

Présenter un rapport d'activité

## Infos

### DURÉE

1 an

### LIEU

Cachan

### RYTHME

2 semaines en CFA /

2 semaines en entreprise

## Prérequis

BAC professionnel industriel, Bac STI2D, Bac général

## La FORMATION

- Architecture matérielle et logicielle (PC, Windows, Serveur, client serveur)
- Gestion de projet (Merise, UML)
- Paramétrage routeurs Cisco (Modules 1 & 2 CCNA)
- Sécurité des réseaux
- Algorithmes et programmation
- Conception de solutions informatiques en réponse à une problématique
- Mathématiques et algorithmes appliqués
- Économie, droit et gestion
- Expression, communication professionnelle
- Anglais

# BTS CIEL - IR : CYBERSÉCURITÉ, INFORMATIQUE & RÉSEAUX, ÉLECTRONIQUE

Option A : Informatique et réseaux

Titre niveau 5 RNCP : 37391

Selon l'emploi occupé, le technicien supérieur pourra être en charge de l'étude, de la conception de solutions techniques en informatique et réseaux, de l'exploitation et de la maintenance de réseaux informatiques, ainsi que la valorisation de la donnée et la cybersécurité

## Objectifs

Étudier et concevoir des réseaux informatiques

Exploiter et maintenir en état de fonctionnement des réseaux informatiques

Valoriser la donnée et exercer la cybersécurité

## Infos

### DURÉE

2 ans

### LIEUX

Cachan, Mantes-la-Ville,  
Tremblay-En-France

### RYTHME

2 semaines en CFA /  
2 semaines en entreprise

## Prérequis

Bac S - Bac STI 2D  
Bac Pro SN / CIEL

## La FORMATION

### FORMATION TECHNIQUE - 900 h

#### PRATIQUE PROFESSIONNELLE

- Étude et conception de réseaux informatiques
- Exploitation et maintenance de réseaux informatiques
- Valorisation de la donnée et cybersécurité
- Projet E62 (en entreprise)
- Préparation et certification habilitation électrique
- Gestion de projets
- Construction de maquettes
- Fabrication

### FORMATION GÉNÉRALE - 450 h

#### EXPÉRIMENTATION

- Mathématiques
- Sciences physiques et chimiques appliquées
- Gestion

#### COMMUNICATION ET CULTURE

- Expression, communication professionnelle
- Anglais

# BTS CIEL - ER CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

Option B : Électronique et réseaux

Titre niveau 5 RNCP : 37391

Selon l'emploi occupé le technicien supérieur pourra être en charge de l'étude, de la conception de solutions techniques électroniques, de la production, de l'intégration et la maintenance de produits, ainsi que la mise en œuvre de réseaux informatiques

## Objectifs

Étudier et concevoir des produits électroniques

Mettre en œuvre des réseaux informatiques

Réaliser et assurer la maintenance de produits électroniques

## Infos

### DURÉE

2 ans

### LIEUX

Cachan, Mantes-la-Ville,  
Tremblay-En-France

### RYTHME

2 semaines en CFA /  
2 semaines en entreprise

## Prérequis

Bac S - Bac STI 2D  
Bac Pro SN / CIEL

## La FORMATION

### FORMATION TECHNIQUE - 900 h

#### PRATIQUE PROFESSIONNELLE

- Étude et conception de produits électroniques
- Mise en œuvre de réseaux informatiques
- Réalisation et maintenance de produits électroniques
- Projet E 62 (en entreprise)
- Préparation et certification habilitation électrique

#### CONDUITE DE PROJET

- Gestion de projets
- Construction de maquettes
- Fabrication

### FORMATION GÉNÉRALE - 450 h

#### EXPÉRIMENTATION

- Mathématiques
- Sciences physiques et chimiques appliquées
- Gestion

#### COMMUNICATION ET CULTURE

- Expression, communication professionnelle
- Anglais

# ADMINISTRATEUR SYSTÈMES, RÉSEAUX ET CYBERSÉCURITÉ

Titre niveau 6 RNCP : 39851

L'administrateur systèmes et réseaux est indispensable dans toute entreprise équipée d'appareils informatiques connectés entre eux et/ou à un réseau externe. Il a pour responsabilité de gérer les infrastructures informatiques d'une société, permettant l'accès et le partage de données, ainsi que la communication numérique. Il maîtrise les techniques de configuration de poste, câblage, routage (LAN, WAN) et de sécurité.

## Objectifs

Concevoir et implémenter une infrastructure réseau

Installer et configurer les systèmes et les différents services associés

Concevoir et implémenter la sécurité sur une infrastructure réseau

Concevoir et mettre en œuvre une infrastructure informatique résiliente

Concevoir, implémenter et gérer un système d'information

Concevoir et implémenter une infrastructure de téléphonie (VoIP)

## Infos

### DURÉE

2 ans

### LIEU

Cachan

### RYTHME

2 semaines en CFA /  
2 semaines en entreprise

## Certifications

- CCNA3
- TOIEC À 550

## Prérequis

Bac +2 validé (BTS SN, SIO, DUT)  
en réseaux et systèmes

## La FORMATION

### MODULE RÉSEAUX

- Architecture Protocolaires
- Supervision des réseaux
- Réseaux WIFI, opérateurs WIFI
- CCNA 3
- VoIP et QoS
- Interconnexion des réseaux
- Gestion des terminaux mobiles
- Routage avancé
- VoIP et QoS
- Automatisation des configurations (PUPPET, CHEF, ANSIBLE)

### MODULE SYSTÈME

- Windows Server les fondamentaux
- Support et Ingénierie Windows
- Fondamentaux Linux
- Support et Ingénierie Linux
- Powershell AD
- Docker
- Sauvegardes et politiques de sauvegarde
- Virtualisation (VMWare, HyperV, XenSource, VirtualBox, KVM) PKI / IAM
- Cloud

### PROJET

- Mise en place d'une infrastructure résiliente incluant les différentes technologies étudiées dans le cursus.
- Droit informatique
- Anglais - passage du TOIEC à 550

# CONCEPTEUR DE SYSTÈMES AUTOMATISÉS ET INTERFACES ASSOCIÉES

Titre niveau 6 RNCP : 39349

Le concepteur de systèmes automatisés et interfaces associées conçoit et développe les systèmes automatisés & interfaces qui intègre les technologies clés de l'industrie 4.0 : Intelligence artificielle, IoT, cybersécurité, réalité virtuelle ou encore jumeaux numériques.

## Objectifs

Analyser un besoin d'automatisation industrielle à partir d'un cahier des charges

Proposer une solution technique et matérielle relative au système numérique d'une installation automatisée

Développer l'application informatique de l'installation automatisée

Concevoir et intégrer une interface homme-machine (IHM)

Réaliser les tests, la mise au point et la mise en service d'une installation automatisée

Assurer un appui technique à l'utilisateur final

## La FORMATION

### FORMATION TECHNIQUE - 500 h

- Analyse du besoin d'automatisation, cahier des charges
- Architectures de systèmes automatisés et réseaux industriels
- Développement logiciel industriel Automatismes
- Développement applicatif industriel d'interfaces homme-machine et supervision
- Exploitation des données issues des systèmes automatisés
- Tests, mise en service et validation



## Infos

### DURÉE

1 an

### LIEU

Cachan

### RYTHME

1 semaine en CFA

3 semaines en entreprise



## Prérequis

- Bases solides en informatique : algorithmique, programmation (au moins un langage), logique et compréhension des environnements numériques.

# FORMATION « CARE » CYBER ADMINISTRATEUR DES RÉSEAUX D'ENTREPRISES

Titre niveau 6 RNCP: 34474

Cette formation intensive spécialisée en réseau et cybersécurité permettra d'acquérir les Compétences nécessaires à la poursuite d'études en master 2 IRS (ingénierie des réseaux et des systèmes). En fin de cursus, l'apprenant est autonome pour intégrer une équipe réseau/cybersécurité et participer à la conception, au déploiement et à la sécurisation d'un système d'information moderne.

## Objectifs

Concevoir un système d'information

Déployer le système d'information

Administrer et exploiter un système d'information

Manager un projet

## Infos

### DURÉE

2 ans

### LIEU

Cachan

### RYTHME

1 semaine en CFA /

3 semaines en entreprise

## Certifications

- Cyberops Associate
- TOEIC à 785

## La FORMATION

- Module Réseau - 70 h
- Module Système Windows Server - 35 h
- Module Système Linux - 35 h
- Module Gestion de l'identité et des certificats - 35 h
- Module Cloud - 35 h
- Module Base de données - 35 h
- Module Sécurité - 35 h
- Module Qualité de Service (QoS) - 35 h
- Introduction à l'Internet des Objets (IoT) - 14 h
- Module Projet - 105 h
- Module Droit - 21 h
- Module Anglais (préparation TOEIC) : 35 h

+

## Prérequis

Bac +3 validé (Licence) en réseaux et systèmes  
Titre RNCP niveau 6 en réseaux et systèmes

# MASTER SÉCURITÉ INFORMATIQUE (MSI)

AVEC SORBONNE UNIVERSITÉ

Titre niveau 7 RNCP : 39278



L'ingénieur DevOps gère des infrastructures réseaux de grandes tailles et automatise les déploiements des configurations des systèmes et réseaux. Il virtualise les différents services mis en place dans l'Entreprise et facilite le déploiement de nouvelles machines en automatisant la création de la machine et sa mise à disposition.

## Objectifs

Sécuriser des SI et des ICS

Réaliser des pentests (tests de pénétration)

Faire de l'analyse médico-légale (Forensic)

Être capable de faire de la cryptologie et de la cryptologie post quantique

Maîtriser les techniques de gouvernances SSI (RGPD, SMSI, Gestion des risques)

Maîtriser la sécurité prédictive et adaptative  
Savoir sécuriser un code (Reverse, Fuzzing, analyse de code)

Être apte à la gestion de crise (PRA, PCA)

## Infos

### DURÉE

2 ans

### LIEU

Cachan

### RYTHME

1 semaine en CFA /

3 semaines en entreprise

## La FORMATION

### Année 1

- Architecture des réseaux
- Secure coding
- Sécurité des bases de données
- Ethical Hacking & Pentests
- Audit de la sécurité des SI
- Sécurité des communications
- Primitives Cryptographie et fonctions de Sécurité
- Reverse Engineering
- Projet Sécurité M1

### Année 2

- Cryptologie moderne
- Attaque par des canaux auxiliaires
- Supervision et réponse incident
- Forensic
- Sécurité des plateformes mobiles
- Management des systèmes d'information
- Anglais
- Projet Sécurité M2

+

## Prérequis

Licence ou licence professionnelle informatique

Titre RNCP niveau 6 en réseaux et systèmes

# MASTER INGÉNIERIE DES RÉSEAUX ET SYSTÈMES - IRS

AVEC PARIS SACLAY

Titre niveau 7 RNCP : 39278

université  
PARIS-SACLAY

L'ingénieur réseaux et systèmes conçoit, planifie et développe des architectures de systèmes en réseau en intégrant les besoins présents et futurs des utilisateurs, tout en anticipant les évolutions générées par les nouvelles technologies.

En M2, il est possible de se spécialiser en systèmes et réseaux ou en cybersécurité.

## Objectifs

Concevoir, modéliser et implémenter une infrastructure réseau

Installer et configurer les systèmes et les différents services associés

Concevoir et implémenter la sécurité sur une infrastructure réseau

Concevoir et implémenter une architecture de système d'information

Assurer la sécurité du système d'information

Assurer le bon fonctionnement du système d'information

## Infos

### DURÉE

2 ans

### LIEUX

Cachan, St Quentin-en-Yvelines (ISTY),  
Versailles (UVSQ)

### RYTHME

1 semaine en CFA /  
3 semaines en entreprise

## Certifications

- CCNA
- TOEIC à 785

## Prérequis

Licence ou licence professionnelle  
informatique  
Titre RNCP niveau 6 en réseaux et systèmes

## La FORMATION

### Année 1

- Mise à niveau maths et langages
- Savoir-être et méthodologie (ITIL, gestion de projet)
- Fondamentaux des réseaux
- Architecture des réseaux
- Modélisation des réseaux
- Anglais et communication
- Systèmes et bases de données
- Droit informatique et certifications
- Virtualisation et supervision
- Introduction à la sécurité
- Projet École

### Année 2

- Sécurité avancée des réseaux
- Convergence réseaux fixes et mobiles
- Infrastructure des réseaux
- Savoir-être et gestion des risques
- Sécurité des bases de données
- QoS et performance des réseaux
- Recherche et Innovation
- Virtualisation et Sécurité
- Certification et Cybercriminalité
- Anglais et Communication
- Projet École

+



# INGÉNIEUR SYSTÈMES, RÉSEAUX & SÉCURITÉ - ISRS

Titre niveau 7 RNCP : 38105

L'ingénieur DevOps gère des infrastructures réseaux de grandes tailles et automatise les déploiements des configurations des systèmes et réseaux. Il virtualise les différents services mis en place dans l'Entreprise et facilite le déploiement de nouvelles machines en automatisant la création de la machine et sa mise à disposition.

## Objectifs

Sécuriser des SI et des ICS

Réaliser des pentests (tests de pénétration)

Faire de l'analyse médico-légale (Forensic)

Être capable de faire de la cryptologie et de la cryptologie post quantique

Maîtriser les techniques de gouvernances SSI (RGPD, SMSI, Gestion des risques)

Maîtriser la sécurité prédictive et adaptative  
Savoir sécuriser un code (Reverse, Fuzzing, analyse de code)

Être apte à la gestion de crise (PRA, PCA)

## Infos

### DURÉE

2 ans

### LIEU

Cachan

### RYTHME

1 semaine en CFA /  
3 semaines en entreprise

## VS

- CCNA
- TOEIC à 785

## Prérequis

Licence ou licence professionnelle informatique  
Titre RNCP niveau 6 en réseaux et systèmes

## La FORMATION

### Année 1

- Anglais
- Sécurité des bases de données
- Cyberops Associate
- Pentest
- PRA/PCA ISO 22301
- Développement personnel
- Projet
- Conception et sécurisation des Réseaux ICS
- Audit des SI
- Projet IaaS, SaaS
- Mobile Device Management
- Droit informatique
- Scripting Python
- Supervision
- Virtualisation d'infrastructure (SDN, SDS, Cluster, HA)
- Wireshark
- Ethical hacking

### Année 2

- Anglais/Toeic
- Blockchain
- FORENSIC
- Architecture Datacenter
- IAM
- IoT
- DEVNET
- Développement personnel
- IaaS Virtualisation des Services
- Projet IA Infrastructure adaptative
- Sécurité des plateformes mobiles (IOS, Android)
- SDN, IBN, SDWAN
- Machine Learning, Deep Learning
- Droit cyber
- Soutenance
- Virtualisation NSX - Proxmox

# EXPERT EN INGÉNIERIE & DÉVELOPPEMENT DE LOGICIELS POUR L'INDUSTRIE

Titre niveau 7 RNCP : 40350

L'industrie 4.0 et la transformation numérique des systèmes industriels requièrent des experts capables de concevoir, développer et sécuriser des solutions logicielles innovantes. Face aux enjeux d'interopérabilité des systèmes, de cybersécurité, d'intelligence artificielle et de durabilité numérique, il est essentiel de former des professionnels qualifiés, en adéquation avec les exigences actuelles et futures du secteur industriel.

## Objectifs

Piloter un projet de développement de logiciel industriel

Analyser et formaliser les besoins clients

Concevoir l'architecture, développer et industrialiser une solution logicielle

Maintenir, faire évoluer et sécuriser les logiciels industriels

## Infos

### DURÉE

2 ans

### LIEU

Cachan

### RYTHME

3 semaines en entreprise

1 semaine au CFA

## Certifications

- DEVNET
- TOEIC à 785

## Prérequis

Licence ou licence professionnelle informatique Titre niveau 6 - Bachelor développement  
Diplôme Bac +4 ou Bac +5 scientifique

## La FORMATION

### COMPÉTENCES TECHNIQUES

- Programmation avancée : C / C++, Java, Python, Rust
- Conception et modélisation logicielle : UML, SysML
- Systèmes embarqués et temps réel : RTOS, Linux Yocto
- Sécurité des logiciels industriels : OWASP, chiffrement AES / TLS
- Protocoles de communication industrielle : Modbus, CAN, OPC UA, MQTT
- DevOps, intégration et déploiement continu : Docker, Kubernetes

### COMPÉTENCES MANAGÉRIALES ET TRANSVERSES

- Gestion de projet en mode Agile / Scrum
- Communication avec des équipes pluridisciplinaires
- Veille technologique et capacité d'innovation
- Analyse critique et résolution de problèmes complexes

# EXPERT EN NUMÉRISATION INDUSTRIELLE

Titre Niv 7 RNCP : 38477

L'expert en numérisation industrielle transforme les systèmes de production pour améliorer performance, qualité et compétitivité. Il déploie des technologies innovantes (IA, IoT, robotique...) et accompagne les équipes dans le changement.

## Objectifs

**Analyser** un besoin industriel et comprendre les enjeux techniques

**Concevoir** des solutions innovantes adaptées à la production

**Développer** et intégrer des systèmes (automatisme, robotique, IA...)

**Tester**, sécuriser et fiabiliser les installations

**Piloter** des projets et accompagner le changement

**Optimiser** la performance industrielle en continu

## Infos

### DURÉE

2 ans

### LIEU

Tremblay-en-France

### RYTHME

1 semaine en CFA /  
3 semaines en entreprise

## Prérequis

Accessible après une licence, un BUT ou un titre niveau 6 (informatique, maintenance, automatisme, robotique) ou équivalent.

Ou avec au moins 5 ans d'expérience professionnelle en tant que technicien supérieur ou équivalent.

## La FORMATION

### BLOC 1

- Concevoir l'architecture d'un système de production complexe à partir de l'analyse d'un système de production existant
- Analyse du besoin de la transformation numérique des systèmes de productions industrielles
- Étude de faisabilité de la transformation numérique des systèmes de productions industrielles
- Conception de l'architecture système d'un système de production complexe en incluant des briques technologiques

### BLOC 2

- Réaliser et intégrer un système de production complexe
- Réalisation d'un système de production complexe en incluant des briques technologiques
- Intégration et validation du système de production complexe incorporant des briques technologiques

### BLOC 3

- Gérer et manager un projet de transformation numérique industrielle
- Pilotage des projets de transformation numérique industrielle
- Accompagnement des parties prenantes vers la transformation numérique industrielle

# TITRE TSSR - TECHNICIEN SUPÉRIEUR SYSTÈMES ET RÉSEAUX

Titre niveau 5 RNCP : 37682

Le Technicien Supérieur Systèmes et Réseaux administre, maintient et sécurise les infrastructures informatiques (serveurs, réseaux, cloud). Il gère les incidents, accompagne les utilisateurs et contribue à la cybersécurité des systèmes d'information.

## Objectifs

Support utilisateurs N1/N2 (ITIL), ticketing, supervision

Administration systèmes Windows & Linux, Active Directory

Réseaux IP : configuration, maintenance, diagnostic (OSI, DHCP, DNS, VLAN)

Virtualisation & cloud : VMware, Proxmox, Hyper-V, IaaS / SaaS

Sécurité & continuité : PRA/PCA, sauvegardes, VPN, pare-feu, ANSSI

Déploiement postes Windows, images, VDI

Automatisation par scripts PowerShell / Bash

## Infos

### DURÉE

1 an

### LIEU

Cachan

### RYTHME

1 semaine en CFA /

3 semaines en entreprise

## Prérequis

Titre professionnel de niveau 4 (ou équivalent Bac).

Possibilité d'accès dès un niveau 3 avec forte motivation et projet professionnel cohérent.

## La FORMATION

### FORMATION TECHNIQUE - 400h

- Support utilisateur & exploitation (ITIL / Outils / Supervision)
- Systèmes Windows & Active Directory
- Systèmes Linux & services open source
- Réseaux IP & interconnexions
- Virtualisation & infrastructures hybrides (Cloud)
- Cybersécurité, accès distants & sauvegardes
- Déploiement & automatisation (Scripts / VDI / Masterisation)
- Projet fil rouge

### FORMATION GÉNÉRALE - 100h

- Communication professionnelle (écrite / orale)
- Résolution de problèmes (méthodologie TSSR)
- Anglais technique (niveau B1 écrit, A2 oral - référentiel officiel)
- Veille technologique & documentation technique
- RGPD & bonnes pratiques ANSSI
- Préparation au titre (mise en situation pro, entretien technique, dossier professionnel)
- Aide à l'insertion professionnelle (CV, entretien, posture)

+



Le Technicien informatique de proximité assure l'installation, la maintenance et le support des équipements numériques, intervient sur les réseaux (Wi-Fi, VPN, Active Directory) et veille à la disponibilité et à la sécurité des systèmes en appliquant les bonnes pratiques de cybersécurité et en sensibilisant les utilisateurs.

## Objectifs

Accompagner les utilisateurs dans l'usage quotidien de leurs équipements numériques et assurer un support technique adapté.

Installer, configurer, maintenir et sécuriser les postes de travail, périphériques et solutions logicielles.

Déployer et sécuriser les équipements réseaux (Wi-Fi, VPN) et gérer les comptes utilisateurs dans l'annuaire Active Directory.

Appliquer les protocoles de cybersécurité et contribuer à la protection des données.

Développer des compétences relationnelles et organisationnelles pour communiquer efficacement et travailler en équipe.

## Infos

### DURÉE

1 an

### LIEU

Cachan

### RYTHME

1 semaine en CFA /

3 semaines en entreprise

## Prérequis

Accessible à tout public.

Titre professionnel de niveau 4

Accès possible dès un niveau 3

## La FORMATION

### CCP 1 - ASSURER LE SUPPORT UTILISATEUR (150 H)

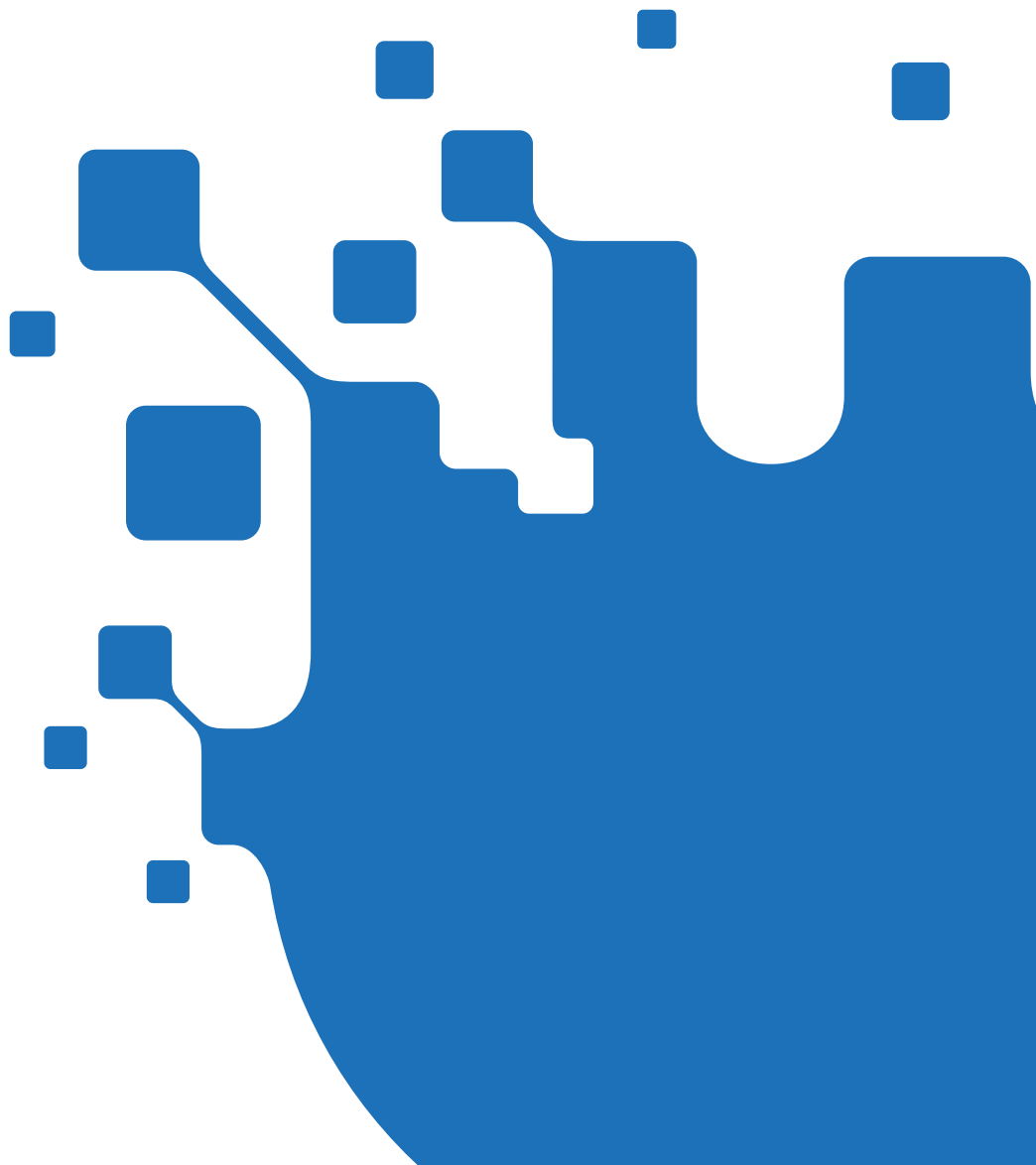
- Gestion des demandes et incidents, suivi du parc
- Assistance et formation des utilisateurs
- Diagnostic et résolution d'incidents techniques ou applicatifs
- Préparation Cisco IT Essentials - bases hardware, OS et dépannage

### CCP 2 - METTRE EN SERVICE DES ÉQUIPEMENTS NUMÉRIQUES (170 H)

- Préparation et déploiement de postes et logiciels
- Maintenance et optimisation des équipements numériques
- Sécurisation des postes et protection des données
- Préparation Cisco Cybersecurity Essentials - hygiène informatique, protection des données

### CCP 3 - INTERVENIR SUR LES ÉLÉMENTS DE L'INFRASTRUCTURE (120 H)

- Déploiement et sécurisation des réseaux (Wi-Fi, VPN, routeurs, switches)
- Gestion des comptes et ressources dans Active Directory
- Préparation Cisco CCST Networking - fondamentaux des réseaux
- Communication professionnelle et relation client
- Cybersécurité & RGPD (bonnes pratiques ANSSI)
- Méthodologie de résolution de problèmes et veille technologique
- Anglais technique appliqué (10 h) : lecture et compréhension de documentations, notices et ressources professionnelles
- Préparation aux épreuves de certification TIP et accompagnement à l'insertion professionnelle







Inscrivez-vous en ligne  
[www. \*\*Aforp\*\*.fr](http://www.Aforp.fr)

**RETROUVEZ-NOUS**

**PARIS NORD 2  
TREMBLAY-EN-FRANCE**

64 avenue de la Plaine de France  
93290 Tremblay-en-France

**CACHAN**

8 Av. de l'Europe  
94230 Cachan

**MELUN  
VAUX LE PENIL**

238 Rue de la Justice  
77000 Melun

**EMERAINVILLE**

Rue Willy Brandt  
77184 Émerainville

**GENNEVILLIERS**

40 Av. Marcel Paul  
92230 Gennevilliers

**MANTES-LA-VILLE**

6, rue Camélinat  
78711 Mantes-la-Ville