

# Cybersécurité

*Une palette de métiers et de formations*

*Catalogue des formations certifiantes et  
diplômantes en cybersécurité proposées sur le  
Territoire de Rennes Métropole*



# SOMMAIRE

Édito - page 4

C'est quoi la cybersécurité ? - page 5

5 bonnes raisons de travailler dans la cybersécurité - page 6

Les métiers de la cybersécurité : des métiers variés pour des femmes et des hommes ! - page 10

Quelques liens pour en savoir plus sur les métiers, formations et commencer à se former - page 23

Se former en cybersécurité : une diversité de formation et de parcours possibles - page 24

Liste des établissements de formations - page 28

Formation niveau 4 / Bac - page 29

Formation niveau 5 / Bac + 2 - page 32

Formation niveau 6 / Bac + 3 - page 39

Formation niveau 7 / Bac + 5 - page 49

Remerciements - page 73

« La cybersécurité est un enjeu sociétal dont on prend, jour après jour de plus en plus conscience.

Il concerne les acteurs socioéconomiques, la nation ou encore chacun d'entre nous dans notre vie quotidienne. Elle est une brique constitutive de la confiance numérique.

Aussi Rennes Ville et Métropole prend toute sa part pour accompagner son développement en particulier pour que la disponibilité de personnels qualifiés ne soit pas un facteur limitatif à son développement.

Pour ce faire, en partenariat avec la Région, les services de l'Etat (Ministère des Armées et ANSSI), les entreprises, les académiques mais aussi tous les acteurs qui accompagnent l'emploi, Rennes Ville et Métropole a mis en place une Gestion Prévisionnelle des Emplois et Compétences territoriale cyber avec l'appui de We Ker.

[association présente sur le Bassin d'emploi de Rennes qui porte notamment des actions GPEC-T]. Cette dernière doit permettre de voir durablement converger l'offre et la demande, avec une attention toute particulière pour faire profiter de ces opportunités une diversité de publics.

Afin de porter à connaissance du plus grand nombre les différents métiers de cette filière, qui ne sont pas tous techniques et encore moins réservés aux seuls ingénieurs, il a été décidé d'élaborer ce document présentant la cybersécurité et ses métiers ainsi que les formations et cursus permettant de les rejoindre.

Les métiers de la cybersécurité sont accessibles à tous, comme l'attestent les témoignages présents dans ce document. »

### **Sébastien SEMERIL**

Vice-président en charge de l'Economie et de l'Emploi chez Rennes Ville et Métropole

## C'EST QUOI LA CYBERSECURITE ?

On appelle cybersécurité la sécurité contre les menaces des systèmes d'information, c'est-à-dire à peu près tous les dispositifs qui nous entourent et qui sont pourvus d'une capacité minimale de calcul :

ordinateurs, smartphones ou tablettes numériques, mais aussi clés de voiture, cartes à puce, objets connectés ou installations domotiques...

La cybersécurité va donc bien au-delà d'Internet, elle concerne aussi la vie de tous les jours. Alors que la numérisation gagne en importance, toutes les sphères de la société, des individus aux gouvernements en passant par les entreprises, les organisations à but non lucratif et les établissements d'enseignement, sont de plus en plus exposées aux risques croissants de cyberattaques.

En effet, chaque année, on assiste à l'émergence d'attaques virulentes et très développées comme les Ransomware, le Phishing, The Denial Of Services...

Pour faire face à ces dangers, il est devenu indispensable de recruter de nouveaux talents, spécialisés dans la cybersécurité.

# 5

## BONNES RAISONS DE TRAVAILLER DANS LA CYBERSÉCURITÉ

### 1 Un secteur en plein boom

Dans son plan d'investissement « France 2030 », et plus particulièrement dans le volet sur la stratégie nationale de cybersécurité, [la stratégie nationale cyber s'inscrit dans le plan d'investissement pour l'avenir](#), le gouvernement s'est donné comme objectif de faire émerger les futurs champions technologiques de demain et accompagner les transitions de nos secteurs d'excellence.

Les enjeux autour de la **cybersécurité** sont ambitieux : un financement à hauteur de 1,039 milliards d'euros et la création de 37 000 emplois. « Environ 9 250 personnes seront formées afin de devenir des spécialistes du domaine à tous les niveaux de bac, bac +2 à bac +8, avec notamment un nouveau bac professionnel CIEL (Cybersécurité Informatique Electronique). La recherche doit également être soutenue via le financement d'une centaine de thèses », a annoncé le gouvernement.

**Représente de belles opportunités en perspective** pour les nouveaux arrivants sur ce marché du travail en pleine évolution et en recherche constante de profils qualifiés.

La Région Bretagne et le territoire de Rennes Métropole en particulier, font partie des territoires qui recrutent avec de véritables opportunités d'emplois et la possibilité d'y faire carrières, tant dans le secteur public que privé.

Cela se traduit par une diversité d'employeurs du secteur privée : start'up, PME, Grands Groupes mais aussi étatique avec la présence sur Rennes Métropole de la Direction Générale de l'Armement (DGA) à Bruz, du COMCYBER, de l'ANSSI.

### 2 Une diversité de métiers pour une diversité de profils

Les entreprises, les associations et les structures publiques ont besoin de talents pour identifier les vulnérabilités dans leurs systèmes d'information, mettre en place une politique et des outils de cybersécurité efficaces pour contrer les cyberattaques et évangéliser les bonnes pratiques auprès de leurs collaborateurs.

La cybersécurité s'affirme aujourd'hui comme un secteur non seulement en plein essor, mais également critique pour la protection de notre société numérique. Que l'on vienne d'une formation spécialisée ou même en reconversion professionnelle, le marché du travail en cybersécurité se présente comme un champ d'action vaste et diversifié. Il nécessite une gamme étendue de compétences, permettant ainsi à chacun, selon ses intérêts et aptitudes, de trouver sa voie et de contribuer à un enjeu majeur de notre époque.

En entreprise ou au sein d'organismes publics, vous pouvez ainsi travailler du côté de la conception des Systèmes d'Information (SI) en tant qu'Architecte sécurité ou cryptologue, en prévention et gestion des risques cyber au poste d'analyste SOC ou de Pentesteur ou encore choisir des métiers plus transverses comme celui de consultant en cybersécurité.

Les besoins en talents sont permanents. Quelque soit votre profil ou votre niveau, il est possible de s'orienter, de se reconvertir ou d'ajouter une brique technique à votre parcours professionnel si vous désirez vous spécialiser dans la cybersécurité.

Vous avez **toutes les chances** de trouver un emploi stable. En vous formant ou en suivant un projet de reconversion, vous pourrez intégrer une filière en pleine croissance.

En 2021, l'**ANSSI** (l'Agence Nationale de la Sécurité des Systèmes d'Information) a lancé son **Observatoire des métiers de la cybersécurité** et a mené des travaux [Profils cybersécurité](#) à partir d'une enquête interrogeant 2 381 professionnels.

### 3 Des emplois porteurs de sens qui répondent à des enjeux sociétaux

Travailler dans la sécurité informatique, c'est aussi s'engager pour défendre les intérêts de tous face aux menaces des pirates informatiques : les menaces sont diverses, allant des ransomwares aux logiciels malveillants sur ordinateurs et téléphones mobiles, en passant par les failles de sécurité détectées dans différents systèmes (Apple, Windows, WordPress, etc.), les sabotages et espionnages informatiques par des organisations malveillantes, ou encore les attaques ciblant des infrastructures critiques.

Que vous choisissiez de travailler pour des entreprises publiques ou privées, tous les métiers de la cybersécurité participent à défendre des valeurs essentielles de respect et de protection des données.

*En choisissant de vous spécialiser dans la cybersécurité, vous ne vous lancez pas seulement dans un parcours professionnel prometteur, vous prenez part à une mission essentielle pour la sécurité et le bien-être numérique global.*

### 4 Un domaine passionnant en évolution constante

Ce domaine, à l'intersection de la technologie, de la protection des données et de la défense contre les cybermenaces, offre une multitude d'opportunités de carrières passionnantes et enrichissantes, où l'innovation et la vigilance sont au cœur de chaque action.

En constante évolution le domaine de la cybersécurité exige une adaptation et un apprentissage continu, ce qui peut satisfaire la soif de connaissances et de défis intellectuels des passionnés de technologie.

En tant que professionnels vous devez rester au fait des dernières technologies, des tendances des cyberattaques et des pratiques de défense, ce qui favorise un environnement de travail dynamique et stimulant. Cette exigence d'apprentissage perpétuel participe à vous enrichir personnellement, en vous offrant, une croissance professionnelle continue.

Dans le même temps, les missions confiées aux personnes expérimentées par les entreprises ou les collectivités évoluent vite et amènent en général plus de responsabilités. Elles peuvent par exemple vous amener à intégrer des fonctions tournées vers le management, la gestion de projet.

### 5 Des opportunités de carrière en France et à l'international

La diversité des rôles et des défis à relever dans le secteur offrent des carrières dynamiques et challengeantes et cela que ce soit dans le secteur public ou privé. Les passerelles entre les deux secteurs sont aussi fréquentes.

Parmi les avantages qu'offrent les métiers de la cybersécurité, vous avez la possibilité d'exercer votre profession selon le statut de votre choix :

- en tant que salarié.e dans une structure publique ou privée, pour assurer la sécurité informatique de ses infrastructures,
- comme consultant.e dans une agence ou une ESN, où vous réaliserez des missions pour un ou plusieurs clients,
- ou bien en étant à votre propre compte, en freelance

Si différents pôles cyber se développent en France, notamment en Bretagne, les entreprises du secteur sont aussi implantées à l'international et permettent à leurs collaborateurs, l'opportunité de vivre une expérience à l'étranger et d'en tirer de nombreux bénéfices. Travailler à l'international permet d'acquérir une expérience multiculturelle, de développer sa pratique des langues étrangères, d'apprendre à s'adapter aux autres cultures et d'augmenter son employabilité et être source de motivation.

# LES METIERS DE LA CYBERSECURITE :

des métiers variés pour des FEMMES et des HOMMES !

Vous êtes curieux, vous aimez apprendre par vous-même, vous aimez les défis, vous vous adaptez facilement, vous appréciez travailler en équipe, vous êtes à l'aise dans la rédaction d'écrits. Les profils sont valorisables, alors quel que soit votre profil, votre parcours, vous pouvez trouver un poste adapté à vos envies, votre caractère.

**Osez donner un sens à vos compétences, le domaine de la cybersécurité est fait pour Vous !!**

## Les domaines de la Cyber sécurité

### Cybersécurité & Business

Prestations de services cyber  
(Entreprise Service du Numérique)  
Ventes / Développement de produit de sécurité  
(Logiciel / Matériel / Réseau / Cloud...)  
Surveillance / Défense interne de l'entreprise

### Cybersécurité étatique

Ministériel (ANSSI) - DGA  
Armée / Police / Gendarmerie / Douane (COMCYBER)  
Service de renseignement (DGSE, DGSI...)

### Cybersécurité & Recherche

Labos de recherche (Public ou Privé)  
Centre de surveillance / réaction (SOC, CERT)

# LES MÉTIERS DE LA SÉCURITÉ OFFENSIVE

Les objectifs de la sécurité offensive sont d'évaluer la robustesse des systèmes de sécurité pour en déceler les faiblesses, d'améliorer ces systèmes pour les rendre plus résistants aux attaques informatiques et d'aider les organisations à mieux se protéger contre les cyberattaques.

La sécurité offensive peut également être utilisée pour collecter des informations sur les menaces potentielles et les méthodes utilisées par les attaquants afin de garder une longueur d'avance et limiter les angles morts.

## Exemples de métiers de la sécurité offensive :

**L'auditeur** est responsable de l'évaluation de la sécurité des systèmes d'information d'une entreprise, afin d'en garantir le niveau de sécurité attendu. Son but est de les protéger contre les différentes techniques et méthodes des cyberattaquants. L'auditeur en sécurité travaille en étroite collaboration avec les équipes de sécurité pour identifier les vulnérabilités des systèmes et suggérer des solutions pour les corriger.

**Le pentester** teste la sécurité des systèmes d'information en réalisant des scénarios d'attaques techniques et organisationnels (par exemple en utilisant le phishing). Son rôle est de proposer des plans d'action concrets pour corriger les vulnérabilités mises en lumière par ses tests et les scénarios utilisés au cas par cas.

# LES MÉTIERS DE LA CYBERDÉFENSE

Les métiers de la cyberdéfense s'articulent souvent autour du service SOC (le Security Operations Center) sur des sujets allant de la détection à la remédiation d'incidents de sécurité. Un SOC, c'est une équipe et un ensemble de processus qui a pour but de protéger un système d'information en continu. Cela passe par la surveillance du réseau, la détection, l'analyse et la remédiation des incidents de sécurité. Le SOC veille donc en permanence sur les éléments stratégiques d'une entreprise : ses données, ses actifs (PC, serveurs, cloud...), ses utilisateurs...

Les professionnels de la cyberdéfense sont chargés de détecter les attaques informatiques le plus tôt possible pour renforcer la sécurité opérationnelle d'une organisation. Cette surveillance constante permet de lutter plus efficacement contre les nouveaux modes opératoires cybercriminels.

Parmi les métiers de la cyberdéfense on trouve :

## **Le Sécurité Operator :**

Ce professionnel surveille 24h/24h et 7J/7 les alertes qui remontent dans le SOC. Il doit suivre des procédures bien précises pour transmettre les incidents à l'Analyste SOC qui se chargera ensuite de corréler toutes les informations pour proposer une médiation

## **L'Analyste SOC :**

Il priorise, trie et corréle les alertes qui pourraient nuire à un système d'information selon leur degré de criticité. Il œuvre au quotidien avec des outils et des systèmes d'intelligence artificielle du SOC qui pré-mâchent le travail de tri, ce qui lui permet de se concentrer sur les vraies problématiques et d'être réactif en cas d'incident majeur.

## **Le manager SOC :**

Il agit de l'alter ego du RSSI (le Responsable de la Sécurité des Systèmes d'Information) sur la partie opérationnelle. Il contrôle si les alertes remontent correctement et peut faire évoluer les plans de surveillance, de communication des clients en fonction des failles et vulnérabilités qui lui parviennent. Il travaille en étroite collaboration avec les Analystes sécu pour limiter au maximum les risques de crise. Il a un rôle de conseiller et oriente les clients sur la meilleure stratégie de sécurité à adopter.

## LES MÉTIERS DE LA GOUVERNANCE CYBER

Dans le secteur de la cybersécurité, **la gouvernance** regroupe les protocoles, outils, méthodologies et procédures à suivre en cas de crise dans l'objectif d'assurer la continuité de la stratégie de cybersécurité d'une entreprise. Les métiers de la cybersécurité et plus particulièrement de la gouvernance cyber peuvent inclure plusieurs expertises.

Le **consultant cybersécurité** a pour mission d'exécuter la politique de cybersécurité d'une organisation en respectant une méthodologie et un cahier des charges bien précis. Son objectif est d'assurer la protection des données des systèmes d'information, et de veiller à la bonne « hygiène cyber » au sein d'une entreprise (systèmes de sauvegardes, détection du phishing et des logiciels malveillants, l'ingénierie sociale...).

Le **consultant conformité** spécialisé en cybersécurité est quant à lui chargé d'analyser le niveau de conformité d'une organisation, ou d'un système d'information en fonction des réglementations en vigueur. Il s'assure que la sécurisation des informations sensibles respecte le RGPD et les préconisations de la CNIL. Il définit et lance des plans d'action correctifs pour faire évoluer les politiques de sécurité au besoin. Il réalise également une veille juridique et technologique constante sur ses domaines d'intervention, pour rester à l'affût des évolutions réglementaires et des préconisations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

## LES MÉTIERS DE GESTION DE PROJETS CYBER

**Travailler dans la cybersécurité** englobe aussi les métiers de la **gestion de projets**. Discipline accessible pour les non-spécialistes, elle peut se composer de plusieurs corps de métiers.

Le **chef de projet cyber** est chargé de coordonner toutes les parties prenantes des projets de sécurité informatique. À l'instar d'un chef d'orchestre, il doit identifier les chantiers prioritaires, les ressources humaines et les coûts nécessaires à mobiliser pour cadencer l'avancement des livrables. Il a également pour mission de faire remonter les progrès et les difficultés rencontrées auprès des clients et s'assurer que tous les objectifs sont atteints.

Le **PMO (ou Project Management Officer)** réalise principalement des tâches administratives. Il est par exemple en relation avec les sous-traitants, ou encore les prestataires, et doit vérifier les clauses dans les contrats. Il veille à la bonne organisation des projets et s'assure que tout est en ordre d'un point de vue bureaucratique.

Le **responsable de la communication cyber** sensibilise les équipes. Il peut par exemple créer des supports sous des formats originaux pour rappeler les bonnes pratiques cyber aux salariés.



# LES DEV OPS

Les techniques DevOps ont une approche de **gestion de projet de développement** qui vise à optimiser la coopération et la communication entre les équipes de développement et d'exploitation d'un système informatique.

Le but de ces techniques est d'accélérer les processus de développement et de mise en production des logiciels, tout en assurant un haut niveau de qualité et de fiabilité

Les métiers DevOps combinent des compétences en développement de logiciels et en administration de systèmes.

On peut retrouver :

**L'administrateur systèmes et réseaux** : sa mission est d'analyser, fiabiliser et optimiser la plateforme du SOC une fois mise en production.

**Le software developer** : son rôle est de coder la totalité des composants logiciels et de les mettre à jour régulièrement. Il garantit également des logiciels secured-by-design (conçus dans le but d'être conformes d'un point de vue sécurité et de risques cyber). Le product owner (PO) Ce métier nécessite de coordonner toutes les parties prenantes pour développer les composants du SOC selon la méthodologie agile. Son objectif est de veiller à ce que le produit soit le plus en phase avec les attentes des clients. Il doit répondre aux besoins des équipes en interne et des utilisateurs finaux en effectuant des tests et en livrant le produit sur des itérations courtes.

[Une partie des éléments cités ci dessus provienne de la source: site](#)

[Source : site : travailler dans la cyber](#)

# CARTOGRAPHIE DES MÉTIERS DE LA CYBERSÉCURITÉ – RÉFÉRENCE ANSSI

[Panorama des métiers de la cybersécurité](#)

[Cartographie des métiers de la Cybersécurité - référence ANSSI](#)

## Gestion de la sécurité et pilotage des projets de sécurité

Cette famille regroupe les métiers contribuant au pilotage de la démarche de sécurité, ainsi que les métiers visant à mettre en oeuvre les projets de sécurités des SI.

## Conception et maintien d'un SI sécurisé

Cette famille regroupe les métiers qui assurent la prise en compte de la sécurité dans la conception des SI, l'expertise sur la sécurité d'un domaine particulier, l'administration des solutions de sécurité, ainsi que l'audit de la sécurité des SI.

## Gestion des incident et des crises de sécurité

Cette famille regroupe les métiers qui assurent la détection et le traitement des incidents de sécurité, ainsi que les métiers qui gèrent les crises de sécurité.

## Conseils, services et recherche

Cette famille regroupe les métiers que l'on peut rencontrer au sein des entreprises spécialisées en cybersécurité : entreprises de conseil, entreprises de formation, laboratoire d'évaluation, éditeur de produits de sécurités, intégrateurs de produits de sécurité, laboratoires et instituts de recherche.

PILOTAGE, MISE EN OEUVRE,  
MANAGEMENT, GOUVERNANCE

Directeur cybersécurité DSSI (FR), CSO (EN)  
Responsable de la Sécurité des SI : RSSI (FR), CISO (EN)  
Coordinateur sécurité  
Responsable de programme de sécurité  
Responsable de projet de sécurité  
Responsable R&D en sécurité

Gestion Sécurité et Pilotage Projets

EXPERTISE, ARCHITECTURE,  
R&D, AUDIT

Architecte Sécurité  
Expert sécurité  
Développeur en sécurité  
Auditeur Technique  
Cryptologue

Conception et maintien d'un SI sécurisé

## Les métiers DE LA CYBER

Conseil, Services, Recherche

Consultant cyber  
Formateur cyber  
Développeur de solutions de sécurité  
Intégrateur de solutions de sécurité  
Auditeur Organisationnel  
Chercheur cyber

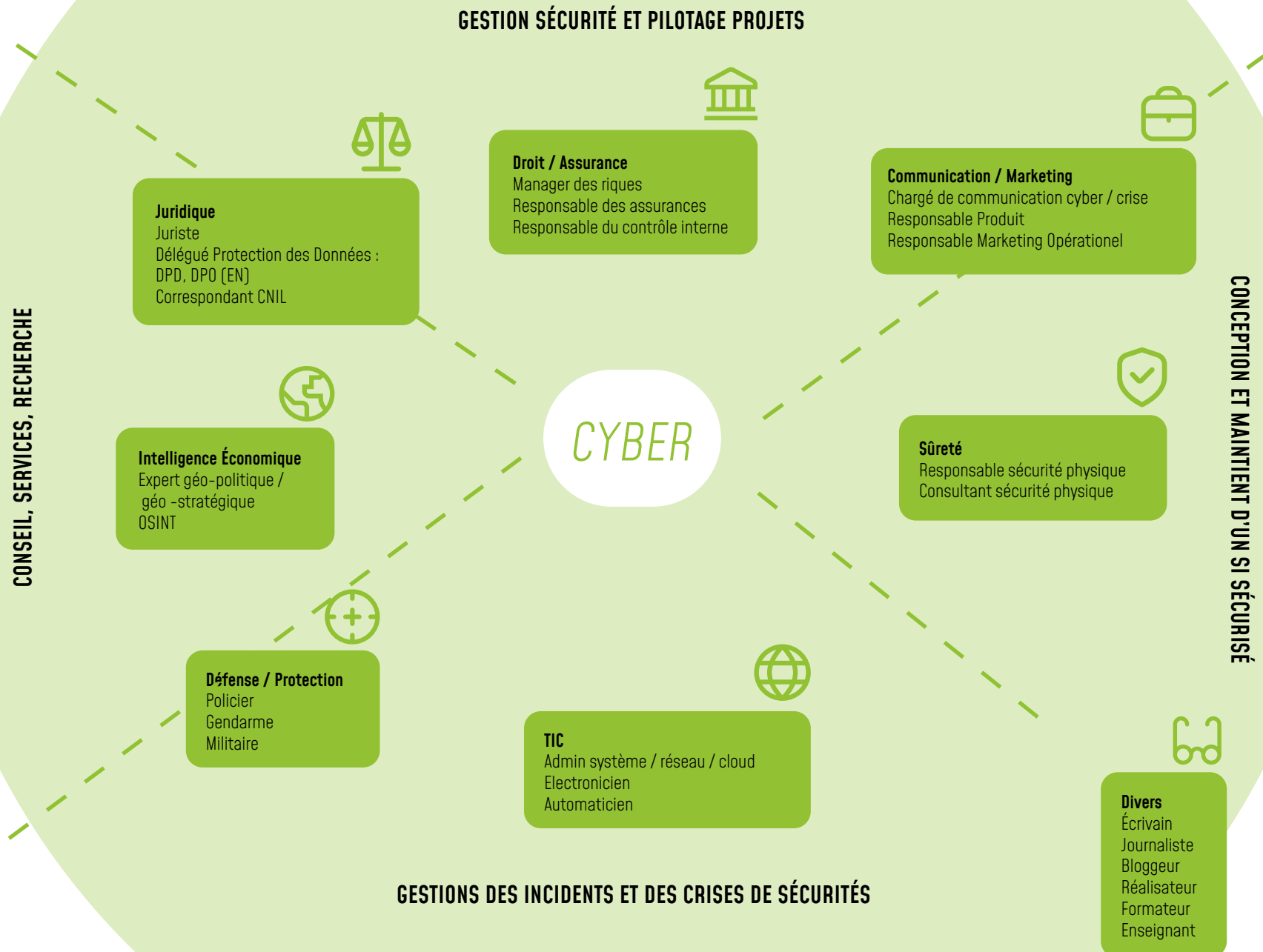
CONSEIL, SENSIBILISATION, AUDIT,  
RIQUES, CONFORMITÉ, RECHERCHE

Gestions des incidents et des crises de sécurité

Responsable du SOC  
Analyste SOC  
Responsable du CERT / CSIRT  
Analyste Réponses aux incidents de sécurité  
Analyste de la menace cybersécurité

DÉTECTION, TRAITEMENT, ANALYSE,  
GESTION DE CRISE

La cybersécurité ce sont aussi des métiers dans les domaines suivants :



## Compétences recherchées savoir-faire

### Compétences générales

Informatique, système, réseau, développement

### Compétences méthodologiques

Analyse, rédaction, organisation, animation

### Compétences technique cyber

Crypto, dev, reverse, admin, éval...

### Double compétences

Telecom, automaticien, électronicien, IA, BigData...

## Compétences recherchées savoir-être

Autonomie

Travail en équipe

Prise d'initiatives

Curieux, innovant

Goût du travail bien fait

Appétence à l'apprentissage permanent

Motivations

Équilibre vie pro / vie perso

# QUELQUES LIENS POUR EN SAVOIR PLUS ET COMMENCER À SE FORMER

## Pour en savoir plus sur les métiers

Guide des métiers de l'ANSSI : la référence

[Les profils de la cyber](#)

[Métiers de la cyber](#)

[Cartographie des métiers du numérique](#)

[Référentiel des compétences des métiers de la cybersécurité du Campus cyber](#)

[Etude APEC](#)

[Découverte des métiers de la cybersécurité « Demain spécialiste cyber »](#)

[PEC Pôle Excellence Cybersécurité](#)

[BDI](#)

[Portrait du numérique en Bretagne](#)

[GREF Bretagne](#)

[Plateforme IDEO](#)

[Exploratoire](#)

## Pour apprendre et commencer à se former

[MOOC ANSSI](#)

[PIX](#)

Kit Microsoft : GitHub - microsoft/Cybersecurity-jobs-skills-workshop:

Ce kit pédagogique a pour but de présenter aux participants quelques enjeux de la cybersécurité et de découvrir les métiers qui y sont associés.

# SE FORMER EN CYBERSÉCURITÉ : UNE DIVERSITÉ DE FORMATIONS ET DE PARCOURS

Des formations de bac à Bac + 5 / 8

Des formations accessibles en Formation Initiale, en alternance et par la voie de la formation continue.

## Formation initiale

Correspond à celle suivie en lycée / université  
Statut de lycéens ou d'étudiants  
Inclu période de stage

## Formation en alternance

Correspond aux formations en apprentissage ou contrat de professionnalisation  
Formations en Centre de formation et en entreprise  
Statut de salarié

## Formation continue

Correspond aux formations à destination de personnes en reconversion ou à la recherche d'une qualification supérieure  
Permet de conforter, améliorer ou acquérir des connaissances  
Statut de stagiaire de la formation professionnelle

# DES FORMATIONS LABELLISÉES SECNUMÉDU



L'objectif de **SecNumedu** est d'apporter aux personnes recherchant une formation et aux employeurs l'assurance qu'une formation spécialisée en cybersécurité répond à un certain nombre de critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine (établissements d'enseignement supérieur, industriels, etc.).

[Liste des formations labellisées SecNumedu accessible.](#)

## Des diplômes et des titres inscrits au RNCP (Répertoire Nationale des Certifications Professionnelles [RNCP])\*

- Les **diplômes nationaux** et les titres professionnels délivrés par l'État (bac pro, BTS, master, etc.) qui y sont **enregistrés de droit** ;

- Les **titres à finalité professionnelle** proposés par des CCI (chambres de commerce et d'industrie), des CMA (chambres de métiers et de l'artisanat), des organismes de formation publics ou privés, des ministères... Ces titres sont enregistrés après instruction du projet par la CCP (Commission de la certification professionnelle), **à la demande de ces organismes**.

La certification est accordée pour une durée précise, de **1 à 5 ans**, après examen d'un dossier de candidature.

[Lien article ONISEP Les titres enregistrés au RNCP](#)

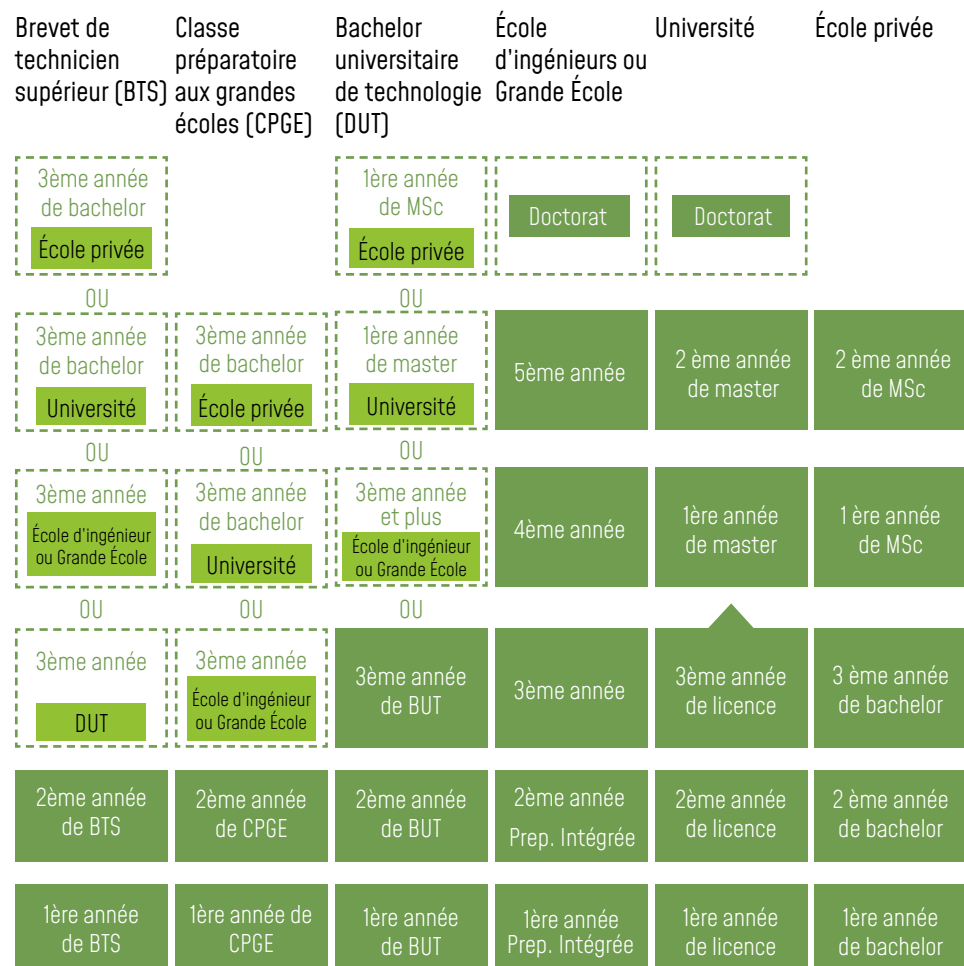
# DES PASSERELLES POSSIBLES

“L’enseignement supérieur français offre diverses possibilités de parcours permettant aux étudiants d’adapter leur parcours académique et professionnel en fonction de leurs aspirations et de leurs projets, incluant des passerelles entre les établissements privés et publics. Si la transition des diplômes publics vers les privés se fait sans problème, l’inverse (comme passer d’un Bachelor privé à un Master universitaire) nécessite une attention particulière. Les Bachelors privés, souvent axés sur des formations pratiques, diffèrent des Masters universitaires, qui se concentrent sur des modules théoriques et des recherches approfondies. Deux défis principaux se posent :

- la sélection compétitive pour entrer en Master
- l’adaptation académique nécessaire pour les étudiants issus de formations pratiques.

Les passerelles existent pour ceux souhaitant diversifier leur parcours, et le succès repose sur une analyse de faisabilité du parcours, une préparation rigoureuse et une bonne compréhension des exigences académiques, ainsi qu’une forte motivation.”

# PARCOURS POSSIBLES



## Baccalauréat

**Baccalauréat général**, spécialités : Mathématique, Physique Chimie, Numérique et Sciences Informatiques (NSI) et/ou Science de l’ingénieur

**Baccalauréat technologique** Sciences et Technologies de l’industries et du Développement Durable (STI2D)

**Baccalauréat professionnel** Cybersécurité, Informatique et réseaux, Electronique (CIEL)

# LISTE DES ÉTABLISSEMENTS DE FORMATIONS

FORMATION Niveau 4 / Bac

FORMATION Niveau 5 / Bac +2

FORMATION Niveau 6 / Bac + 3

FORMATION Niveau 7 / Bac + 5

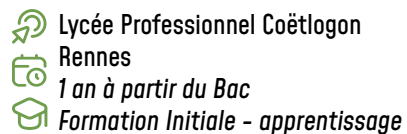
FORMATION Niveau 4 / Bac

## Mention complémentaire Cybersécurité

Formation post-bac en 1 an sous statut lycéen ou apprenti

Certification délivrée par Ministère éducation Nationale et de la Jeunesse

RNCP : 37488 [2028]



[Site Web Lycée Coëtlogon](#)

[Lien vers la page de la formation](#)

### PRÉSENTATION

Cette mention complémentaire vise à former des techniciennes et techniciens capables d'intervenir sur l'installation, l'exploitation et la maintenance des réseaux informatiques notamment dans un environnement industriel. Le technicien ou la technicienne participe à la sécurisation des données, des applications, des infrastructures numériques, des produits et des équipements. Il ou elle contribue à la gestion des incidents, à l'audit des installations et systèmes, ainsi qu'à la diffusion d'une culture d'hygiène informatique.

#### PRÉREQUIS

Bac professionnel SN, Bac technologique STI2D, Bac général (spécialités scientifique, numérique et SI), Titulaire d'un Bac autre, sur positionnement en fonction de l'expérience professionnelle.

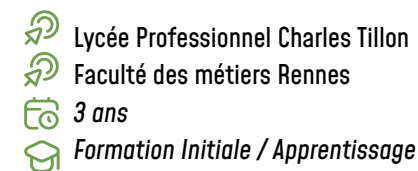
#### DÉBOUCHÉS

Intégrateur ou intégratrice de solutions de sécurité, opérateur ou opératrice en cybersécurité, Technicien.ne de maintenance en informatique, installateur.trice de réseaux informatique.

## Bac Pro Cybersécurité, Informatique et Réseaux, Electronique (CIEL)

Diplôme niveau 4 délivrée par Ministère de l'Éducation Nationale et de la Jeunesse

RNCP : 37489 [2028]



[Site internet Lycée Charles Tillon](#)

[Lien vers la page de la formation](#)

### PRÉSENTATION

Le baccalauréat professionnel C.I.E.L a pour objet de former des techniciennes et des 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.

#### PRÉREQUIS

Ouvert aux élèves issus de 3ème générale, 3ème Prépa-Métiers et seconde générale ou technologique qui souhaitent se réorienter.

#### DÉBOUCHÉS

Poursuite d'études en BTS  
Les emplois les plus couramment exercés par le ou la titulaire du baccalauréat professionnel « Cybersécurité, Informatique et réseaux, Électronique » couvrent les domaines de la réalisation, de la production, de l'intégration, de la maintenance de produits électroniques ainsi que la mise en œuvre de réseaux informatiques, la valorisation de la donnée et la cybersécurité.




## FORMATION Niveau 5 / Bac +2

## BTS CIEL

*BTS CIEL Cybersécurité, Informatique et réseaux, Electronique (CIEL) – Option A informatique et réseau Diplôme délivré par Ministère de l'Enseignement supérieur et de la recherche.*

RNCP : 37489 [2028]


**Lycée Professionnel Bréquigny**  
**Hélène Bach**  
**Rennes YNOV campus**  
**AFTEC Rennes**  
**2 ans à partir du Bac**  
**Formation Initiale – apprentissage**

[Lien vers la page de la formation](#)

## PRÉSENTATION

Le BTS CIEL a pour objectif de former de futurs professionnels aptes à intervenir sur la cybersécurité, la mise en place et la maintenance des applications, des réseaux et des systèmes électroniques et informatiques.

L'option A du BTS CIEL est principalement axée sur les systèmes informatiques organisés en réseaux et sur les langages de programmation. Cette option du BTS CIEL permet de développer des compétences spécifiques dans les pôles d'activités suivants :

- Étude et conception de réseaux informatiques
- Exploitation et maintenance de réseaux informatiques
- Valorisation de la donnée et cybersécurité

## PRÉREQUIS

Bac pro SN, Bac général, Bac technologique SII2D, étudiants en réorientation

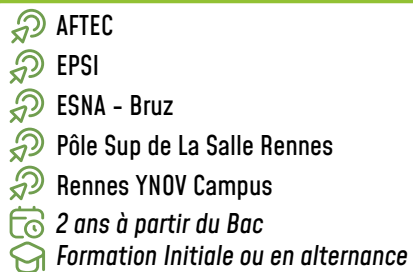
## DÉBOUCHÉS

Poursuite d'études : licence informatique, licence pro, école ingénieur, BUT 3ème année Bachelor Technicien ou technicienne en maintenance / Analyste en sécurité des systèmes télécoms, réseaux et informatique/ Développeur ou développeuse en informatique / Analyste de données / Technicien ou technicienne télécoms et réseaux / Administratrice ou administrateur systèmes, réseaux

# BTS SIO – SLAM Prépa intégrée Cybersécurité

Diplôme délivré par Ministère de l'Enseignement supérieur et de la recherche et de l'Innovation

RNCP : 35340 [2025]



[Site internet de l'AFTEC](#)

[Lien vers la formation ESNA](#)

[Lien vers la formation Rennes YNOV Campus](#)

[Lien vers la formation EPSI](#)

[Lien vers la formation Pôle Sup de La salle](#)

[Autres formations BTS SIO SLAM](#)

## PRÉSENTATION

Le BTS SIO option solutions logicielles et applications métiers (SLAM) a pour objectif de former un.e alternant.e à développer, à adapter et à maintenir des solutions applicatives. Le technicien.ne informatique dialogue en permanence avec les informaticiens de l'entreprise et les collaborateurs extérieurs (fournisseurs de matériel, prestataires de services...). Il-elle exerce des fonctions d'interface entre les utilisateurs, le service informatique central, les gestionnaires et les décideurs.

### PRÉREQUIS

BAC général, STI2D, STMG ou d'un BAC PRO (systèmes numériques)

### DÉBOUCHÉS

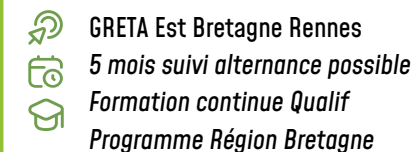
Poursuite d'études en BTS

**Les exemples de métiers :** Développeur d'applications informatiques, chargé d'études informatiques, Technicien en informatique ou cybersécurité. Attention sur certains postes, nécessité d'avoir une habilitation (avec procédure allant de 6 à 8 mois). Passerelles possibles à l'ESNA : TSCP Drones – Technicien.ne Supérieur.e Spécialité Drone – ESNA (Niveau 6) /- Poursuites possibles : Bachelor – Systèmes Réseaux et Cybersécurité – ESNA (Niveau 6) / Titre BAC +5 MSIR ROB – Manager de systèmes informatique spécialité Robotique d'innovation (Niveau 7)

# Technicien Veilleur de Cybersécurité

Certification délivrée par Ministère des Armées

Validation de 2 blocs de compétences dans le cadre de QUALIF EMPLOI de la Région Bretagne / puis possibilité de poursuivre en alternance



RNCP : 36164 [2027]

[Lien vers la page de la formation](#)

## PRÉSENTATION

La formation "technicien veilleur de cybersécurité" vise à former des professionnels capables de renforcer la résilience des organisations contre les menaces, de surveiller et protéger les systèmes informatiques, les données et la vie privée, de sensibiliser les utilisateurs et de maintenir une sécurité efficace dans un environnement numérique en constante évolution.

### PRÉREQUIS

Avoir un niveau 4 [niveau bac] validé dans le domaine informatique et/ou une expérience professionnelle dans le domaine de l'informatique / Avoir des connaissances technologiques en informatique.

### DÉBOUCHÉS




**Métiers :** Analyste en cybersécurité / Technicien en sécurité des systèmes d'information/ Analyste en renseignement sur les menaces/ Administrateur de la sécurité réseau /Responsable de la conformité en cybersécurité

**Poursuites d'études :** Coursus Bachelor universitaire de technologie « Réseaux et télécommunication en cybersécurité » / Coursus universitaire : licence Sciences et ingénierie Cybersécurité défensive / Responsable en ingénierie informatique et cybersécurité / Coursus « Ecole d'ingénieur » / Ingénieur Cyberdéfense ENSIBS Vannes.

# Technicien supérieur Systèmes et Réseaux spécialisation Analyste Cybersécurité

Titre professionnel Technicien Supérieur  
Systèmes et Réseaux du Ministère du travail  
du plein emploi et de l'insertion.

RNCP : 37682 (2026)

 **Simplon Rennes**  
 **Formation intense de 399 h**  
 **Suivi d'alternance sur 12 mois**

[Lien vers la page de la formation](#)

## PRÉSENTATION

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.

### PRÉREQUIS

Aucun prérequis technique, très forte motivation, à démontrer lors du parcours de candidature. Avoir compris le métier visé par la formation, Vouloir travailler en équipe et collaborer autour de projet, Connaître les principaux métiers et domaines du numérique.





### DÉBOUCHÉS

Administrateur systèmes, réseaux et sécurité / Technicien déploiement / Technicien d'infrastructure / Technicien d'intégration / Technicien réseau / Technicien système / Technicien télécom / Ingénieur systèmes / Ingénieur réseaux.

# Technicien supérieur Systèmes et Réseaux

Titre professionnel Technicien Supérieur  
Systèmes et Réseaux du Ministère du travail  
du plein emploi et de l'insertion.

RNCP : 37682 (2026)

 **ENI Rennes**  
 **AFTEC**  
 **Formation en continu sur 8 mois**  
 **(6 mois de cours/2 mois de stage)  
ou 2ans en alternance**

[Site internet de l'AFTEC](#)

[Site internet de l'ENI](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

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 et guide les utilisateurs dans l'utilisation de leurs différents équipements numériques et les informe des bonnes pratiques de sécurité.

### PRÉREQUIS

Jeunes diplômés d'un titre de niveau Bac en informatique.

Demandeurs d'emploi ayant un niveau Bac en informatique. Demandeurs d'emploi de niveau Bac+2 hors informatique (domaines : commercial, gestion, comptabilité, secrétariat...) désirant s'orienter vers les métiers du support aux utilisateurs. Demandeurs d'emploi ayant déjà une première expérience professionnelle en informatique (assistance technique, technicien maintenance, ...) et désirant s'inscrire dans les métiers du support aux utilisateurs. Demandeurs d'emploi ayant déjà une première expérience dans un domaine de l'informatique.

### DÉBOUCHÉS

**Métiers** : Technicien support, Technicien informatique, Technicien d'exploitation, Technicien systèmes et réseaux.

[Lien vidéo Youtube BTS SIO Pôle Sup de La Salle](#)




## **Témoignage de Romina, cursus TSSR Bac+2 à l'ENI**

*«J'ai effectué une formation continue Bac +2 'Technicienne supérieure en Systèmes et Réseaux' après avoir été Commerciale et Technicienne Back Office. A l'issue de mon diplôme bac +2, j'ai pu poursuivre en alternance sur le Bac +4 Administratrice système et réseau. J'ai ensuite été embauchée par l'entreprise AUB Santé en Alternance pour poursuivre vers le Bac +5 ESD, où je suis restée 4 ans en tant que RSSI.»*

FORMATION Niveau 6 / Bac + 3

## BUT Réseaux et Télécommunications

Diplôme délivré par Ministère de l'Enseignement supérieur et de la recherche et de l'Innovation.  
Formation labellisée SecNumedu. délivré par l'ANSSI

 **IUT SAINT MALO**  
 **3 ans à partir du Bac**  
 **Formation initiale ou en apprentissage**

RNCP : 35455 – 35511 – 35458 (2026)

[Site internet de l'IUT de Saint-Malo](#)

[Lien vers la page de la formation](#)

### PRÉSENTATION

L'objectif du BUT R&T est de former des experts spécialisés dans l'installation, la configuration, la supervision et la sécurisation des réseaux informatiques et de télécommunications. Les connaissances acquises permettent aux diplômés d'exploiter les équipements, les systèmes et les logiciels qui composent un système d'information d'entreprise tout en garantissant le niveau de sécurité adéquat. Ils savent gérer, surveiller et sécuriser les systèmes et services aussi bien virtualisés que conteneurisés dans le cloud.

#### PRÉREQUIS

Bac Général / Bac Technologique STI2D

#### DÉBOUCHÉS




Métiers : Administrateur Systèmes et réseaux. Administrateur d'infrastructure de réseaux et télécommunications. Dans les emplois notamment spécialisés en cybersécurité : intégrateur de solution, auditeur, analyste SOC, Responsable de la sécurité Informatique au sein d'une petite structure. Administrateur Data Center, Intégrateur infrastructure Cloud, technicien sécurité des systèmes cloud (DevSecOps).

Poursuites d'études possibles : en école d'ingénieur et en Master en alternance. Possibilité d'entrée en BUT 3 : BTS CIEL, BTS SIO, DUT informatique ou GEII.

## Administrateur d'Infrastructures Sécurisées

Titre professionnel d'administrateur d'infrastructures sécurisées délivré par le Ministère du Travail

RNCP : 37680 (2026)

 **AFPA Rennes**  
 **10 mois inscrit dans Qualif**  
**Programme de la Région Bretagne**  
**Rennes**  
 **Formation Initiale – apprentissage**

[Site internet de l'AFPA](#)

[Lien vers la page de la formation](#)

### PRÉSENTATION

L'administrateur d'infrastructures sécurisées (AIS) met en œuvre, administre et sécurise les infrastructures informatiques locales et dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision. Il participe à la gestion de la cybersécurité en analysant les menaces et en mettant en place des mesures de sécurité et de réaction en cas d'incident.

#### PRÉREQUIS

Maîtrise des fondamentaux systèmes, réseaux et environnements virtualisés, de préférence attestée par un diplôme ou une certification informatique de niveau 5, ou expérience significative équivalente aux prérogatives d'un technicien supérieur [technicien systèmes réseaux]. Un niveau d'anglais technique est également requis à l'entrée en formation.

#### DÉBOUCHÉS


Administrateur cybersécurité, administrateur d'infrastructures et cloud ; administrateur infrastructures, administrateur réseaux (et sécurité), administrateur systèmes et réseaux (et sécurité), administrateur systèmes (et sécurité), responsable infrastructure systèmes et réseaux.

# Bachelor Sécurité Informatique

Titre niveau 6 (Bac +3)

CHEF DE PROJET LOGICIEL ET RESEAU ET SECURITE, Titre de niveau 6 reconnu par l'Etat, enregistré au RNCP délivré sous l'autorité ANAPIJ.

RNCP : 34568 [2025]

 CFA de La Salle – Rennes  
 1 an à partir du Bac +2  
 Formation en alternance  
 Contrat d'apprentissage /  
 Contrat de professionnalisation

[Site internet Pôle Sup de La salle](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Formation conçue pour répondre aux besoins des professionnels de l'IT en matière de sécurité. Elle permet de développer les compétences suivantes : coordonner un projet informatique, Concevoir – administrer et sécuriser le système informatique.

### PRÉREQUIS

Cette formation est ouverte à tous les titulaires d'une certification de niveau 5 (Bac +2) de l'enseignement supérieur dans le domaine de l'administration logiciel et réseau/ de l'informatique ainsi que du domaine du développement (ex : BTS SIO/ SNIR, BUT2 Info & Cyber, titre de niveau 5 Technicien Supérieur en informatique).

### DÉBOUCHÉS

**Métiers** : Chef(fe) de projet SI / Consultant(e) informatique / Administrateur(rice) Systèmes et Réseaux / Auditeur(rice) sécurité Informatique / Consultant(e) sécurité.  
**Poursuite d'études** : Poursuites possibles vers un titre de niveau 7 dont Mastère Sécurité Informatique.

# Bachelor Systèmes Réseaux et Cloud

Certification professionnelle « Coordinateur de projets informatiques (infrastructures cloud, applicatives ou data) » de niveau 6 délivrée par Sup de Vinci

RNCP : 38478 [2028]

 Sup de Vinci à Rennes  
 12 mois en alternance  
 Contrat d'apprentissage ou  
 professionnalisation

[Site internet Sup de Vinci](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Le Bachelor vous permet d'apprendre à maîtriser les compétences nécessaires pour travailler avec des infrastructures hétérogènes, que ce soit en mode cloud, hybride ou local. La formation se concentre sur l'orchestration et la professionnalisation des infrastructures informatiques, en utilisant des outils pour automatiser des tâches complexes et améliorer la productivité des serveurs, tout en assurant leur sécurité. Ce Bachelor vous prépare à travailler en collaboration avec les architectes infrastructure, dans le but de concevoir et de mettre en place des architectures informatiques fiables, performantes et sécurisées.

### PRÉREQUIS

Admission en Post-bac avec les deux premières années en initial et choix de la spécialisation en 3ème année Admission en Post-bac avec les deux premières années en initial et choix de la spécialisation en 3ème année

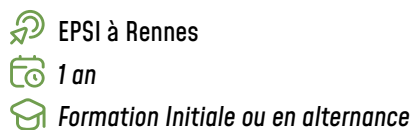
### DÉBOUCHÉS

**Métiers** : administrateur systèmes et réseaux / Responsable informatique PME/PMI / Administrateur cloud.  
**Poursuite d'études** : Mastère en 2 ans avec 1 spécialisation à choisir parmi 5 : Big Data & IA / Cybersécurité / DevOps, Infrastructure & Cloud / Chef de projet IT / Développement Fullstack.

# Bachelor IT Concepteur Intégrateur SysOps

Certification de niveau 6 « Administrateur systèmes, réseaux et bases de données » délivrée par l'IGS

RNCP : 35594 [2026]



[Lien vers la page de la formation](#)  
[Site internet de l'EPSSI](#)

## PRÉSENTATION

L'administrateur systèmes réseaux et bases de données assure l'installation, l'administration et la surveillance des équipements informatiques tant physiques que virtuels. Il veille à la cohérence et à la qualité des données. Il est le garant de la bonne exploitation des ressources informatiques dans un objectif de qualité, de productivité, de disponibilité, et de sécurité.

**Compétences :** Administrer et concevoir une infrastructure, automatiser les tâches et les environnements, gérer des données et un projet selon une approche sysops, Assurer une veille technologique.

### PRÉREQUIS

Posséder une certification professionnelle de niveau 5 ou un diplôme bac+2 en informatique OU une certification professionnelle de niveau 4 ou un diplôme de niveau bac avec expérience minimum de 1 ans dans l'informatique. Dans le cas où un.e candidat.e ne disposerait pas des prérequis, il a la possibilité de déposer un dossier qui sera examiné par une commission.

### DÉBOUCHÉS

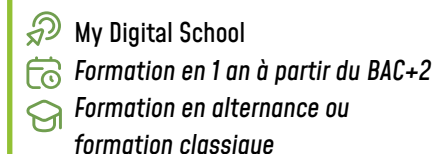
**Métiers :** Administrateur systèmes et réseaux et sécurité / Administrateur systèmes / Administrateur réseaux / Administrateur Cloud / Administrateur des systèmes d'informations.

**Poursuite d'études :** Msc expert en informatique et système d'information / Msc expert en ingénierie des données  
Msc expert en cybersécurité et sécurité informatique/ Mastère.

# Bachelor Cybersécurité et Administrateur Réseau

Titre professionnel « Administrateur d'Infrastructures Sécurisées » de Niveau 6 enregistré au RNCP délivré par le ministère du travail

RNCP : 37680 [2026]



## PRÉSENTATION

Le Bachelor Cybersécurité et Administrateur Réseau se charge de la conception, de la réalisation du réseau informatique de son entreprise ou de ses clients. Il assure le maintien en condition opérationnelle, corrige les éventuels problèmes survenant sur le réseau, préconise les évolutions nécessaires pour que l'infrastructure informatique réponde aux besoins des utilisateurs. Il met également l'accent sur la sécurité des systèmes, des réseaux et des données. Il surveille constamment les signaux faibles et réagit rapidement aux incidents de sécurité.

En combinant savoir-faire technique et vision stratégique, le Bachelor Cybersécurité et Administrateur Réseau œuvre pour édifier un rempart inviolable contre les cybermenaces.

### PRÉREQUIS

Être titulaire d'un Bac+2 : BTS, DUT OU 120 crédits ECTS dans le domaine de l'informatique Système et Réseau (BTS SIO option SISR, Titre TSSR, BUT Informatique...)

### DÉBOUCHÉS

**Métiers :** Administrateur systèmes, réseaux et sécurité  
Administrateur réseaux, Chef de projet, Responsable informatique, Analyste en sécurité réseaux, Consultant cybersécurité

**Poursuite d'études :** MBA Cybersécurité et Architecture Réseau (Niveau 7)

# Administrateur Système et Réseaux ENI

Titre Professionnel reconnu par l'Etat, de Niveau III enregistré au RNCP et délivré par l'ENI - Ecole informatique

RNCP : 35587 [2026]



ENI Rennes

2 ans à partir du Bac +2

Formation en alternance

[Lien vers la page de la formation](#)

[Site internet de l'ENI](#)

## PRÉSENTATION

L'Administrateur Système et Réseau conçoit, planifie et met en œuvre des infrastructures réseaux et/ou des systèmes d'information. Au terme de la formation il est en capacité: Administrer les systèmes serveurs dans le contexte d'une entreprise, Administrer et sécuriser les réseaux informatiques du système d'information de l'entreprise, Concevoir et structurer un système d'information sécurisé, Analyser, définir et programmer les projets d'évolution du système d'information.

### PRÉREQUIS

Jeune diplômé en informatique Bac +2 / Informaticien expérimenté.

### DÉBOUCHÉS

**Métiers :** Administrateur système et réseau, Administrateur système ou administrateur réseau spécialiste système et réseau.

# Bachelor Informatique spécialisation Cybersécurité et Réseaux en 3ème année (sur Paris)

Certification professionnelle de « Administrateur d'infrastructures sécurisées » délivrée par le Ministère du Travail du Plein Emploi et de l'Insertion, Certification délivrée par le Ministère du Travail

RNCP : 37680 [ 2026]



OMNES Education

ECE Rennes

1 an à partir du Bac +2

Formation en alternance ou formation classique

[Site internet d'OMNES Education](#)

[Lien vers la page de la formation](#)

[Site internet de l'ECE](#)

## PRÉSENTATION

L'administrateur d'infrastructures sécurisées (AIS) met en œuvre, administre et sécurise les infrastructures informatiques locales et dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision. Il participe à la gestion de la cybersécurité en analysant les menaces et en mettant en place des mesures de sécurité et de réaction en cas d'incident.

### PRÉREQUIS

Être titulaire Bac+2 : BTS / BUT / Licences (admissions hors parcoursup)

### DÉBOUCHÉS

**Métiers :** Administrateur systèmes et réseaux, Administrateur d'infrastructures, Administrateur Cybersécurité.

Risk Manager, Architecte Réseaux et SI au sein d'entreprises de services numériques,

**Poursuite d'études possible :** en alternance avec le programme hybride « Expert en Cybersecurité » (titre RNCP de niveau 7) ou en classique avec le programme sur Paris « Manager de la Cybersécurité » (MSc labellisé par Conférences des Grandes Ecoles).



# Opérateur de solutions de sécurité Cloud et hybride

Ecole MICROSOFT by SIMPLON

Titre professionnel

"Administrateur d'infrastructures sécurisées" AIS

Trois certifications Microsoft Azure :

"Principes fondamentaux de la sécurité, de la conformité et de l'identité de Microsoft"

"Technologies de sécurité Microsoft Azure"

"Administrateur d'identités et d'accès Microsoft"



Simplon Rennes

Formation intense de 399 h

Suivi d'alternance sur 16 mois

RNCP : 37680

## PRÉSENTATION

L'opérateur·trice de solutions de sécurité Cloud et hybride est chargé·e de mettre en œuvre les services et les contrôles de sécurité dans les environnements Cloud et hybride. Il/elle doit assurer la configuration et l'exploitation des services déployés en appliquant les règles de sécurité. Il/elle intervient sur la configuration et l'exploitation des solutions de sécurité pour défendre son organisation contre les menaces (ransomwares et phishing) et protéger les données et les applications. Enfin il/elle participe à la diffusion des bonnes pratiques de sécurité dans l'utilisation des outils et services au sein de l'organisation, dans le but de limiter les risques liés à d'éventuelles attaques.

### PRÉREQUIS

Pas de prérequis de diplôme. Maîtrise des compétences numériques fondamentales :

- Savoir utiliser un ordinateur
- utilisation du système de fichiers Windows [ou autre] et d'une suite bureautique
- installation et désinstallation d'applications, navigation web
- utilisation d'un service de messagerie instantanée et d'un service d'e-mail

### DÉBOUCHÉS

Administrateur systèmes et/ou réseaux (et sécurité)  
 Administrateur infrastructures  
 Administrateur d'infrastructures et cloud  
 Administrateur cybersécurité  
 Responsable infrastructure systèmes et réseaux

## TÉMOIGNAGES

### Témoignages de Najib, Bachelor Systèmes, Réseaux & Cloud - Sup de Vinci

« C'est une super école avec des intervenants très compétents. Les membres de l'administration sont toujours à l'écoute des élèves. À noter également que l'école a un service dédié pour aider les étudiants à trouver une alternance. Le programme Bachelor Systèmes & Réseaux est riche en contenu et permet d'approfondir nos connaissances. »

### Témoignage de Paul, 2ème année IUT R&T St Malo en alternance

« Ce parcours vise à donner aux étudiants un socle de compétences solides en sécurité informatique. Les compétences développées incluent, la mise en place et supervision d'infrastructures sécurisées, la réponse à incident, les bases de la cryptographie, et les méthodologies du pentesting. »

### Témoignages de Aurélien, cursus ASR Bac+4 à l'ENI

« Cette formation m'a permis d'aborder un très large éventail de connaissances. Le fait d'être encadré par des professionnels du secteur est un véritable atout pour la formation. Cela m'a permis d'apprendre avec des exemples tirés de faits réels et parfois obtenir certaines astuces liés à leurs expériences terrain. Je ne peux que recommander ce cursus. »




### Témoignage de Luc, Bachelor Concepteur Intégrateur SysOps - EPSI

« Durant ma formation en Bachelor Concepteur Intégrateur SysOps, j'ai particulièrement apprécié les modules liés à la cybersécurité et les retours d'expérience des formateurs. Ces notions m'intéressent particulièrement car je suis en alternance chez Vivalto Santé et la gestion des risques cyber est un enjeu important dans le domaine de la santé. »

Témoignage disponible [ici](#)

# Master Informatique parcours Cybersécurité

Diplôme National Universitaire délivrée par  
Université de Rennes  
Formation labellisée SecNumedu.  
Délivrée par l'ANSSI

 **Université de Rennes - ISTIC**  
 **2 ans à partir de la licence**  
 **Formation Initiale**

RNCP : 34126 (2024)

[Site internet de l'ISTIC](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Ce master forme des spécialistes dans le domaine de la sécurité, capables d'assurer la conduite des projets de sécurisation des infrastructures de système d'information, de concevoir des applications sécurisées, de réaliser des missions d'audit technique en sécurité, etc. À l'issue des deux années, les étudiant.e.s sont capables de concevoir, coder, valider et gérer de nouvelles architectures sécurisées ou d'évaluer et corriger des architectures existantes pour les protéger des cybermenaces.

### PRÉREQUIS

Être titulaire d'une Licence Informatique ou d'une Licence Maths-Info ou d'une Licence Génie électrique et électronique.

### DÉBOUCHÉS




**Métiers :** Auditeur Technique (Pentester) / Consultant Cyber / Développement logicielle de sécurité / Spécialiste de la sécurité des IoT / Spécialiste en sécurisation des infrastructures de Système d'information.

**Poursuite d'étude** possible en Mastère spécialisé ou doctorat .

# Master Informatique parcours Responsable Sécurité des Systèmes d'Information (RSSI)

Diplôme National Universitaire délivrée par  
Université de Rennes

RNCP : 34126 (2024)

 **Université de Rennes - ISTIC**  
 **2 ans à partir de la licence ou BUT**  
 **Formation en alternance**

[Site internet de l'ISTIC](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Ce Master prépare les étudiants à la place de politiques de sécurité de l'information dans les organisations afin d'assurer le bon fonctionnement et la pérennité de celles-ci. Ce parcours forme aux métiers liés au management de la sécurité des systèmes d'information. A l'issue des deux années en alternance, les étudiants acquièrent des compétences techniques, juridiques, sectorielles et fonctionnelles.

### PRÉREQUIS

Être titulaire d'une Licence Informatique ou d'un BUT Réseaux Télécommunications option cybersécurité.

### DÉBOUCHÉS




**Métiers :** RSSI / Consultant cybersécurité / Auditeur organisationnel / Consultant GRC (Gouvernance, Risques et Conformité) Spécialiste en sécurisation des infrastructures de Système d'information.

# Master mathématiques et applications parcours mathématiques de l'information, Cryptographie

Diplôme National Universitaire délivrée par  
Université de Rennes

Formation labellisée SecNumedu. délivré  
par l'ANSSI

RNCP : 34 274 (2024)

 **Université de Rennes UFR  
Mathématiques**  
 **2 ans à partir de la licence**  
 **Formation Initiale apprentissage**

[Site internet de l'UFR mathématiques](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Ce master forme des ingénieurs-experts mathématiciens, pour devenir des experts en protection des informations numériques. Les étudiants acquièrent les connaissances théoriques nécessaires pour une bonne compréhension de la cryptographie moderne et de la théorie de l'information, ainsi que des connaissances pratiques pour une application efficace dans la vie réelle. Ils apprennent les fondements mathématiques de la modélisation et le traitement de l'information numérique pour maîtriser les mathématiques et les algorithmes comme l'algèbre, la géométrie, la combinatoire, les probabilités.

### PRÉREQUIS

Être titulaire d'une Licence Mathématiques ou licence Maths-Info.




### DÉBOUCHÉS

**Métiers :** Ingénieur R&D en sécurité de l'information, Cryptographe, Ingénieur en développement de logiciels sécurisés, Ingénieur R&D en sécurité informatique.  
**Poursuite d'étude** possible en doctorat.

# Master Cybersécurité

Diplôme national de l'enseignement supérieur délivré par le CNAM, Conservatoire national des arts et métiers, spécialité Informatique « Master Informatique »

RNCP : 34126 [2024]

 **ESNA –Rennes**  
 **2 ans à partir de la licence**  
 **En alternance**

[Site internet de l'ESNA](#)

## PRÉSENTATION

Au terme de la formation les apprenants sont capables

Gérer un système d'information après compromission / Élaborer la maquette du dossier d'architecture technique / Élaborer l'architecture d'un système d'information sécurisé / Définir un plan de reprise d'activités informatiques / Auditer la sécurité du système d'information / Superviser le système d'information / Sensibiliser les utilisateurs à l'hygiène informatique et aux risques liés à la cybersécurité.

### PRÉREQUIS

Être titulaire d'un Bac +3 / Adaptation possible du parcours selon les prérequis.

### DÉBOUCHÉS

Spécialiste en gestion de crise cyber , Chef de projet sécurité, Expert en cybersécurité, Pentester, Auditeur, Expert en sécurité des systèmes d'information, Investigateur numérique.




Cette formation a pour premier objectif l'insertion professionnelle.

*\*Formation également proposée par le CNAM à distance*

# Ingénieur Cyberdéfense

Titre Ingénieur diplômé du CNAM, reconnu par la CTI

RNCP : 37357[2024] et 38105 [2026]

 **ESNA Rennes**  
 **2 à 3 ans**  
 **Formation en alternance**

[Site internet de l'ESNA](#)

## PRÉSENTATION

A l'issue de cette formation, les apprenants devront être capable de : Analyser un cahier des charges d'un système d'information / Élaborer la maquette du dossier d'architecture technique / Élaborer l'architecture d'un système d'information sécurisé / Définir un plan de reprise d'activités informatiques / Auditer la sécurité du système d'information / Gérer la sécurité du système d'information / Gérer un système d'information après compromission / Superviser le système d'information / Sensibiliser les utilisateurs aux risques liés à la cybersécurité.

### PRÉREQUIS

Pour entrer en formation Bac+3 : Être titulaire d'un Bac+2 Informatique (BTS, BUT...)  
 Pour entrer en formation Bac+5 :v Être titulaire du diplôme Licence informatique parcours cybersécurité.

### DÉBOUCHÉS




L'ingénieur cyberdéfense occupe une grande variété d'emplois liés à la sécurité des systèmes d'information. Il exerce dans diverses structures, publiques comme privées, sujette à d'éventuels incidents de sécurité informatique ou de cyber-attaques.

**Métiers :** Spécialiste en gestion de crise cyber / Chef de projet sécurité / Expert en cybersécurité / Pentester (Testeur d'intrusion), Expert Forensique (Investigateur numérique), Consultant en organisation de la Sécurité des Systèmes d'Information, Responsable de la sécurité des systèmes d'information (RSSI )

# Ingénieur Informatique Mention Cybersécurité

Titre ingénieur délivré par Centrale Supélec

RNCP : 34751 (2024)

 **Centrale Supélec à Rennes**  
 **3 ans, temps plein ou alternance, à partir du Bac+2**  
 **Cours en cybersécurité : en 3ème année**

[Site internet Centrale Supélec Rennes](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

La formation d'ingénieur de Centrale Supélec se déroule sur 3 ans. Les étudiants effectuent deux premières années généralistes et suivent notamment des cours du domaine informatique (cours SIP, cours d'algorithmique, Sécurité & Réseaux...).

En troisième année, la formation se décline en 4 mentions : 'Systèmes', 'Intelligence artificielle', 'Science du logiciel' et 'cybersécurité'. La mention cybersécurité apporte les clés nécessaires au succès de la sécurisation du système d'information, via une formation couvrant cryptologie, prévention et détection des intrusions et logiciels malveillants, ainsi que divers aspects de l'ingénierie de la sécurité.

### PRÉREQUIS

Avoir validé une Classe préparatoire scientifique aux Grandes Écoles. CPGE




### DÉBOUCHÉS

**Métiers** : Chef de projet (cyber), Architecte sécurité, Consultant, Auditeur cyber, Ingénieur R&D de sécurité, Gouvernance en sécurité, conseils et audit.

# Ingénieur spécialité informatique, réseaux, télécommunications

Certification délivrée Titre Ingénieur de l'IMT Atlantique spécialité réseaux et télécommunications

RNCP : 38637 (2027) / 38322

 **IMT Atlantique Rennes**  
 **3 ans, temps plein, à partir de bac +2**  
 **En alternance et FI**

[Site internet de l'IMT Atlantique Rennes](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Ce cursus par apprentissage d'IMT Atlantique vise à former des ingénieurs diplômés de haut niveau, opérationnels et à large spectre technique couvrant l'informatique, les réseaux et les télécommunications. Il prépare aux métiers d'architecture et d'ingénierie des systèmes et réseaux d'information et de communication, ainsi qu'aux fonctions managériales et à l'international.

### PRÉREQUIS

Être titulaire de l'un des diplômes suivants : BUT Réseaux et Télécommunications - BUT Informatique - BUT génie électrique et informatique industrielle (GEII) - BUT Mesures Physiques - BTS Systèmes numériques - L3 Scientifique - D'une Classe préparatoire adaptation technicien supérieur (ATS) - D'une Classe préparatoire technologie et sciences industrielles (TSI) - D'une Classe préparatoire physique et technologie (PT)

### DÉBOUCHÉS




**Métiers** Chef de projet (cyber), Architecte sécurité, Consultant / Auditeur cyber, Ingénieur R&D de sécurité, Responsable de la Sécurité des Systèmes d'Information, Formateur / Chercheur.

**Poursuite d'étude** possible Mastère Spécialisé ou Doctorat.

# Ingénieur Informatique Option Sécurité

Titre ingénieur - Ingénieur diplômé de l'Institut national des sciences appliquées de Rennes, spécialité informatique

RNCP : 4189 (2025)

 **INSA – Rennes**  
 **3 ans, temps plein, à partir de bac +2**  
 **Formation Initiale**

[Site internet de l'INSA Rennes](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Après un socle commun en informatique permettant d'acquérir des connaissances nécessaires à la maîtrise des aspects génie logiciel, réseaux, système, architecture et de domaines aussi divers que les systèmes d'information, le traitement de données ou l'aide à la décision. Les étudiants se spécialisent à la sécurité des systèmes informatiques et électroniques [cryptologie, programmation sécurisée, sécurité des réseaux, confiance, détection d'intrusions]. La formation est ponctuée de cours, travaux dirigés, travaux pratiques, stages et projets.

### PRÉREQUIS

Prépa INSA : via la plateforme Parcoursup (Dossier et Entretien de motivation) / En 3<sup>ème</sup> année : via la plateforme MonMaster (Dossier et Entretien de motivation) / En 4<sup>ème</sup> année : via la plateforme de candidature de l'Université de Rennes.




### DÉBOUCHÉS

Chef de projet (cyber), Ingénieur d'affaires, Consultant cyber, Ingénieur R&D, DevOps, chargé du développement logiciel et de l'administration des systèmes informatiques au sein d'environnements très variés : Entreprise de Services du Numérique (ESN), éditeurs de logiciels, sociétés de conseil, start-up, laboratoires de R&D publics ou privés, services informatiques de grandes sociétés ou administrations.

# École Supérieur d'Ingénieur de Rennes

Titre ingénieur - Ingénieur diplômé de l'Institut national des sciences appliquées de Rennes

RNCP : 39292

 **ESIR – Université Rennes**  
 **3 ans à partir de bac +2**  
 **Formation Initiale**

[Site internet ESIR - École Supérieur d'Ingénieur de Rennes](#)

## PRÉSENTATION

Le Programme Grande École, accessible post-bac, se déroule en 5 ans et forme des experts en informatique. En cybersécurité, sur les trois premières années, les étudiants découvrent notamment les vulnérabilités liées au développement d'applications via des CTF sur des machines présentant des failles diverses (JWT, SQLi, injection de commande...). La 4<sup>e</sup> année s'effectue à l'international dans des universités partenaires, qui offrent des spécialisations en cybersécurité. La 5<sup>e</sup> année se déroule en grande partie en entreprise et les étudiants peuvent suivre des modules techniques (Cryptographie, Web Security, Reverse engineering...).

### PRÉREQUIS

Admission post-bac (GEIPI)  
 CPGE (Concours E3A-Polytech)  
 BUT ou L2/3 scientifique (dossier)

### DÉBOUCHÉS

**Métiers** : Ingénieur R&D, Ingénieur expert, Ingénieur conseil, Administrateur de Systèmes Informatiques, Chef de Projet.  
**Poursuite d'études** : Oui, en doctorat.

# Expert en Technologies de l'Information Programme Grande École

Certifications délivrées

Diplôme d'Expert(e) en Technologies de l'Information –

Visa du Ministère de l'Enseignement supérieur et de la Recherche / Titre Expert(e) en Ingénierie Logicielle d'EPITECH

RNCP : 37985[2026]



[Lien vers la page de la formation](#)

[Site internet EPITECH](#)

## PRÉSENTATION

Le Programme Grande École, accessible post-bac, se déroule en 5 ans et forme des experts en informatique. En cybersécurité, sur les trois premières années, les étudiants découvrent notamment les vulnérabilités liées au développement d'applications via des CTF sur des machines présentant des failles diverses (JWT, SQLi, injection de commande...). La 4e année s'effectue à l'international dans des universités partenaires, qui offrent des spécialisations en cybersécurité. La 5e année se déroule en grande partie en entreprise et les étudiants peuvent suivre des modules techniques (Cryptographie, Web Security, Reverse engineering...).

### PRÉREQUIS

Baccalauréat toutes filières.

### DÉBOUCHÉS

**Métiers :** Développeur Informatique/Ingénieur Logiciel, Expert/Consultant Technique, Chef de Projet MOA/MOE, Ingénieur de recherche, CTO, Directeur Technique, Data Scientist, Architecte Informatique, Data Analyst, Auditeur Cybersécurité, Administrateur Sécurité, Développeur IoT, Pentester, Responsable Systèmes et Réseaux, Devops, Chef de Projet Informatique.

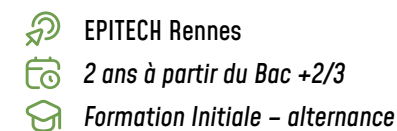
**Poursuite d'étude** possible en doctorat ou autre Master.

# MSc Pro Cybersécurité

Certifications délivrées

Titre Architecte de Systèmes d'Information et Titre Expert(e) en Management des Systèmes d'Information

RNCP : 38114 [2026]/ 35284 [2026]



[Lien vers la page de la formation](#)

[Site internet EPITECH](#)

## PRÉSENTATION

Les titulaires d'un Bac +2/3, avec une appétence prouvée dans l'informatique et le développement, peuvent rejoindre les MSc Pro d'Epitech. Ces parcours s'effectuent en alternance jusqu'au Bac +5 (RNCP de niveau 7), Les apprenants MSc Pro ont la possibilité de choisir une spécialisation en cybersécurité. Les objectifs de cette spécialité sont de leur apprendre l'ensemble des méthodes, techniques, technologies de détection, de défense et d'évolution des systèmes. Ils apprennent à maîtriser les techniques de sécurisation d'un réseau par PENTEST, à créer des failles de sécurité White Hat, à protéger un système informatique dans le respect des normes en vigueur, à maîtriser les techniques de protection des données (RGPD, CNIL...)

### PRÉREQUIS

Bac +2 toutes filières ou 120 crédits ECTS pour intégrer au niveau Bac +3 (appelé Pré-MSc) ou Bac +3 informatique pour intégrer au niveau Bac +4

### DÉBOUCHÉS

**Métiers :** Développeur web et mobile, Data Analyst, Concepteur de Systèmes Autonomes Intelligents, Expert en Réalité Virtuelle, Expert en Réalité Augmentée, Développeur IoT, Ingénieur en Systèmes Embarqués, Data Scientist, Data Miner, Responsable Sécurité des Systèmes d'Information, Auditeur Cybersécurité, Pentester, Administrateur Sécurité, Responsable Infrastructure Cloud, Responsable Système, Réseaux et Télécoms, Responsable de Projet, Chef de Projet, Responsable de la Transformation Digitale...

Les titulaires de l'un des Bac +5, s'ils le souhaitent, peuvent postuler à d'autres master qui seraient complémentaires ou partir sur un Doctorat.

**Poursuite d'étude** possible en doctorat ou autre Master.

# MSc Data Protection Officer

Certification délivrée titre

« Délégué à la protection de données (DPO) »

par ECOLE PRIVÉE DES SCIENCES INFORMATIQUES

RNCP : 36448 [2025]



WIS Rennes



2 ans à partir du Bac +3



Formation en alternance

[Site internet WIS Rennes](#)

[Lien vers la page de la formation](#)

[Data Protection Officer Track - BAC+5](#)

[| WIS Écoles \[wis-ecoles.com\]](#)

## PRÉSENTATION

Cette certification a comme objectif de répondre à un besoin croissant en compétences dans le domaine de la protection des données. Au terme de la formation, vous avez des compétences pour : Élaborer le cadre juridique RGPD et protection, accompagner les directions métiers et les collaborateurs dans la mise en œuvre de la stratégie de protection des données, déployer une stratégie de protection des données et manager un projet de protection de données. Vous développez aussi des compétences transversales et en communication.

### PRÉREQUIS

Être titulaire d'une certification de niveau 6 ou bac+3 en informatique ou en sécurité de l'informatique ou en droit informatique/ droit en propriété intellectuelle.

### DÉBOUCHÉS

**Métiers** : Data Protection Officer, Délégué.e à la protection des données, Data protection manager/specialist, Responsable conformité RGPD, Consultant.e RGPD, Consultant.e données à caractère personnel, Relais informatique et libertés.

# MSc Expert cyber et sécurité informatique

Certification Titre Expert en cybersécurité et sécurité informatique, délivrée par l'EPSI

RNCP : 36924 [2025]



EPSI Rennes



2 ans à partir du Bac 2/3



Formation en alternance

[Site internet de l'EPSI](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Au terme de la formation, vous avez les compétences pour déployer une architecture fonctionnelle et technique en vue de renforcer la sécurité du S.I et de faire face aux cybermenaces. Vous êtes en mesure d'assurer la supervision, l'audit et la gestion de la sécurité informatique et des cyberattaques. Vous pourrez concevoir la stratégie de sécurité du S.I et conseiller la gouvernance, mais aussi piloter le projet de déploiement de la stratégie de sécurité informatique et cybersécurité en mobilisant une démarche agile et innovante.

### PRÉREQUIS

Être titulaire d'une certification professionnelle de niveau 6 ou d'un diplôme bac+3 en informatique [développement d'applications, réseaux informatiques, infrastructures et systèmes] Ou Être titulaire d'une certification de niveau 5 ou d'un diplôme bac+2 en informatique avec une expérience professionnelle d'au moins un an dans un métier de l'informatique.

### DÉBOUCHÉS

**Métiers** : Responsable de la Sécurité des Systèmes d'information (RSSI), Architecte SSI, Conseiller(ère) en SSI, Consultant.e en cybersécurité, Analyst SOC.






# MSc Data Manager

Certification Titre

«Expert en ingénierie des données» délivrée par EPSI

RNCP : 36921 [2025]

 **WIS Rennes**  
 **2 ans à partir du Bac 2 ou 3**  
 **Formation Initiale –alternance**

[Site internet WIS Rennes](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Avec cette certification, l'EPSI souhaite répondre au besoin croissant en compétences liées à l'ingénierie des données, et proposer aux entreprises des profils de certifiés d'un niveau technique informatique élevé et dotés d'une expertise pointue en data. Au terme de la formation, les apprenants sont capables d'analyser et définir la stratégie Big Data alignée avec la stratégie « business » de l'entreprise en collaboration avec la DSI et les experts métiers. Ils peuvent piloter un projet de développement d'une plateforme Big Data, en assurer l'administration et la supervision. Ils préparent et mettent également à disposition les données aux équipes utilisatrices.

### PRÉREQUIS

Être titulaire d'une certification de niveau 6 ou bac+3 en informatique OU Être titulaire d'une certification de niveau 5 ou bac+2 en informatique avec une expérience d'au moins un an dans les métiers informatiques (développement d'applications ou data).

### DÉBOUCHÉS

Expert(e) en ingénierie des données, Data Engineer/Ingénieur, Ingénieur de données, Ingénieur Big Data.




# Expert en Sécurité Digitale

Certification délivrée

Titre professionnel reconnu par l'État, de Niveau 7 (Niveau Bac +5) et enregistré au RNCP.

Certificateur du titre : ASTON Institut

RNCP : 36399 [2027]

 **ENI Rennes**  
 **1 à 2 ans à partir du Bac+3**  
 **Formation en alternance**

[Site internet de l'ENI](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Formation en 1 an : Lead Pentester, Techniques de hacking avancées, Test Intrusion avec Python, Wargame, Cyberdéfense, SOC Security manager, Investigation Numérique – Réseau et Windows, Fondamentaux de l'analyse de malware, Gestion de projets et juridique, Gestion des risques SI avec ISO 27005 et EBIOS 2010/RM, Intégration SMSI avec ISO 27001, Plan de continuité (PCA) avec ISO 22301, DevOps Security Manager, Préparation Jury »

### PRÉREQUIS




En 1 an d'alternance après un Bac+4 Administrateur Système et Réseau / En 2 ans d'alternance après un Bac+3 en informatique.

### DÉBOUCHÉS

**Métiers** : Expert en sécurité digitale, Consultant.e en sécurité des systèmes d'information, Auditeur.rice en sécurité des systèmes d'information, Assistant.e RSSI, Risk Manager.euse (Junior), Administrateur.rice système réseau et sécurité.

## Mastère Expert en Cybersécurité

Titre d'Expert en cybersécurité délivré par YNOV, NSF 326, de niveau 7 enregistré au RNCP par décision du Directeur Général de France Compétences en date du 19/07/2023 Label SecNumEdu de l'ANSSI pour le programme d'Expert en Cybersécurité (obtenu à Paris et Bordeaux, dossier en cours à Rennes).

 Rennes YNOV Campus  
 Parcours en 2 ans.  
 Formation initiale - alternance

RNCP : 37832 [2025]

[Lien vers la page de la formation](#)

[Site internet YNOV](#)

### PRÉSENTATION

Ce Mastère va faire de vous des innovateurs qui façonnent, et façonneront, le futur de la sécurité numérique. Ceux qui peuvent lire entre les lignes de code, déchiffrer les menaces et construire des solutions robustes pour le monde numérique de demain.

Vous disposez d'un programme vous préparant à relever les défis majeurs, réels et futurs, de la cybersécurité : assurer la sécurité des systèmes et réseaux, protéger l'intégrité et la confidentialité des données, garantir la continuité des services...

#### PRÉREQUIS

Être titulaire d'un titre ou diplôme de niveau 6 validé dans le domaine de l'informatique  
 OU Avoir validé les 3 premières années d'une formation qui vise un titre ou diplôme de niveau 7 dans le domaine de l'informatique  
 OU à défaut, signature de la dérogation au prérequis à la certification

#### DÉBOUCHÉS




**Métiers :** Ingénieur cybersécurité, Consultant en cybersécurité, Auditeur sécurité des systèmes d'informations, Architecte sécurité des systèmes d'information, Expert en sécurité des systèmes d'information, Spécialiste en cybersécurité, analyste SOC Security Operations Center, Pentester, Chef de projet en sécurité des systèmes d'information.

## Mastère Spécialisé Cybersécurité

Certification délivrée par Centrale Supélec et l'IMT Atlantique

+ certification ISO27007 Lead Auditor

Le mastère spécialisé® cybersécurité bénéficie du label SecNumedu.

 Centrale Supélec  
 IMT Atlantique Rennes  
 Durée : 1 an, temps plein, à partir de bac +4 / bac+5  
 Formation initiale ou continue

RNCP : 28224

[Lien vers la page de la formation](#)

### PRÉSENTATION

L'objectif de la formation est l'acquisition de compétences permettant la conception, le déploiement et l'exploitation d'un système d'information en respectant les contraintes de sécurité inhérentes à un environnement dédié (ingénierie de la cryptographie, audit, supervision). Cette formation de haut-niveau apporte également les compétences spécifiques pour réagir aux incidents de sécurité (intrusions réseau et web). Le mastère spécialisé Cybersécurité permet d'acquérir les savoir-faire académiques et techniques prisés par les entreprises et ouvre aux métiers d'experts en sécurité.

#### PRÉREQUIS

Cette formation s'adresse à un public de professionnels ou de jeunes diplômés, ayant ou non une expérience professionnelle, désirant acquérir une compétence en sécurité des systèmes d'information.  
 BAC+5 (CTI ou DNU) / BAC+4 avec 3 ans d'expérience / RNCP 7 ou 8.

#### DÉBOUCHÉS

**Métiers :** Responsable Sécurité des Systèmes d'Information, Chef de projet (cyber), Architecte sécurité, Consultant GRC, Auditeur sécurité technique, Auditeur sécurité organisationnelle, Ingénieur R&D de sécurité, Gouvernance en sécurité.

# Mastère Sécurité Informatique

Expert en Architectures systèmes-réseaux et en Sécurité Informatique, Titre de niveau 7 (Bac +5) reconnu par l'Etat, enregistré au RNCP et délivré sous l'autorité ANAPIJ.

RNCP : 36296 (2027)



**CFA de La Salle – Rennes**  
**2 an à partir du Bac +3**  
**Formation en alternance**  
**Contrat d'apprentissage /**  
**Contrat de professionnalisation**

[Site internet Pôle Sup de La salle](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

L'expert en architectures systèmes-réseaux et en sécurité informatique peut mener les activités suivantes : L'analyse et la conception des infrastructures techniques, systèmes et réseaux s'appuyant sur une veille technique et stratégique et en réponse à des besoins identifiés. Le management de projets informatiques complexes, en maîtrisant toutes les étapes nécessaires à la mise en production d'une solution informatique. La supervision et l'amélioration des infrastructures déployées en s'assurant d'une évolutivité des solutions informatiques et de leurs usages en condition réelle. L'identification des risques et la définition de la politique de sécurité informatique propre à une structure.

### PRÉREQUIS

Formation ouverte à tous les titulaires d'une certification de niveau 6 et ayant validé une 3e année dans l'enseignement supérieur dans le domaine de la sécurité informatique (logicielle et/ou matérielle) : Bachelor en Sécurité Informatique, Bac + 3 informatique avec une couche sécurité prononcée (ex : L3 info sécu, BUT3 info réseaux télécom option cybersécurité.)...

### DÉBOUCHÉS

**Métiers** : Architecte des systèmes d'information, Architecte sécurité, Consultant(e) en sécurité des systèmes d'information, Directeur(rice) des services informatiques (après expérience), RSSI (Responsable Sécurité du Système d'Information), Auditeur(rice)...

# Mastère Cybersécurité

Certification délivrée par Partner formation  
 « Expert en Systèmes d'Information » + CEH,  
 PaloAlto, Cisco, AWS, TOEIC, SPLUNK, ELASTIC

RNCP : 34471 (2025)



**Sup de Vinci Rennes**  
**2 ans à partir du Bac +3**  
**Formation en alternance**

[Site internet Sup de Vinci Rennes](#)

[Lien vers la page de la formation](#)

## PRÉSENTATION

Sup de Vinci forme aux nouvelles technologies de la cybersécurité tout en étoffant le background technique transverse de ses étudiants au travers du réseau, des systèmes informatiques et de la sécurisation. Demande de rançons, vol de données, espionnage industriel : la protection des données et des systèmes informatiques est devenue indispensable pour faire face à ces menaces en hausse constante. Les métiers de la sécurité informatique peuvent être classés en deux catégories : les attaquants (Red Team) et les défenseurs (Blue Team). La spécialité Red Team, se concentre dans l'attaque de systèmes d'information afin d'améliorer leur sécurité, tandis que la spécialité Blue Team, se focalise dans la surveillance de l'état de santé d'un réseau à l'aide d'outils permettant de détecter et signaler des anomalies. Ce Mastère vous permettra d'acquérir les compétences essentielles en cybersécurité pour choisir votre Team !

### PRÉREQUIS

Bac +3 validé (Niveau 6) en informatique.

### DÉBOUCHÉS

**Métiers** : Responsable Sécurité des SI, Consultant en cybersécurité, Chef de projet en sécurité informatique, Analyste SOC (security operation center), Ingénieur réseaux, Pentester

# TÉMOIGNAGES

## Témoignage de Julien, Programme Grande Ecole, Promo 2022

« La cybersécurité a une place toute particulière au sein d'Epitech, avec une présence tout au long des cinq années sur des projets dédiés mais pas uniquement ! Ces expériences enrichissantes sont combinées à une dimension compétitive mais accueillante, et favorisent une compréhension approfondie des enjeux cyber tout en stimulant l'apprentissage continu et l'esprit d'équipe. »

## Témoignage de Kévin en formation MSc Pro Cyber, Promo 2025

« Des intervenants de l'écosystème cyber breton couplés à la pédagogie par projets d'Epitech permettent d'acquérir des compétences techniques pratiques, qui mettent les apprenants en situation quasi réelle. Nous apprenons des notions de gestion de crise et de management d'équipe avec un fort aspect cyber. »

## Témoignage de Morgan, Programme Grande École, Promo 2027

« Le format CTF d'Epitech est très intéressant sur le plan pédagogique. Il permet de mettre en pratique nos connaissances dans des situations plus ou moins proches de la réalité, tout en ajoutant un aspect compétitif qui pousse chacun à apprendre continuellement de nouvelles notions. De plus, il permet à chacun d'interpréter et de comprendre des concepts de cybersécurité avec ses propres termes. »

## Témoignage de Mounir, cursus ESD Bac+5 à l'ENI

« Chauffeur routier avec un rêve d'intégrer le monde de l'informatique, j'ai trouvé chez l'ENI un accompagnement dynamique et humain qui m'a permis de dépasser mes objectifs de reconversion. Après les titres de Développeur Web (DWW) et de Concepteur d'Application (CDA), l'ENI m'a aidé à développer mes compétences en Systèmes et Réseaux pour décrocher le titre d'Expert en Sécurité Digitale (ESD) avec les félicitations du jury. Merci à toute l'équipe de l'ENI ! »

## Témoignage de François Demay, Analyse SOC EDF - Promotion Mastère Sécurité Informatique 2022, Pôle sup de La Salle

« La formation cyber proposée au Pôle Supérieur De La Salle allie un enseignement de qualité et travaux pratiques au goût du jour, encadré par des formateurs experts dans leur domaine. Durant ce cursus, j'ai eu l'occasion d'acquérir des compétences pointues, prêtes à être appliquées dans le monde professionnel. Cette formation constitue une porte d'entrée idéale vers des carrières passionnantes et en constante évolution dans le secteur de la sécurité informatique. »

# TÉMOIGNAGES

## Témoignage de Thomas, cursus ESD Bac+5 à l'ENI

« Ma formation de développeur logiciel à l'ENI a été le point de départ de ma carrière en cybersécurité, car j'ai pu travailler sur un outil spécialisé en cybersécurité, ce qui m'a permis de me familiariser avec les enjeux de la sécurité dès le développement. Par la suite, j'ai évolué vers des rôles d'auditeur de code et de pentesteur, où mes compétences en développement m'ont permis d'identifier et de corriger des vulnérabilités. Cette double expertise en développement et cybersécurité est aujourd'hui un atout clé pour apporter des solutions sécurisées et innovantes. »

## Témoignage d'Anne-Sophie : cursus ESD (Bac+5) à l'ENI

« Infirmière, je travaillais au bloc opératoire. Une opportunité m'a souri lorsque, suite aux cyberattaques sur des établissements de santé en 2021 je me suis rendue sur le site de l'ANSSI et j'ai vu qu'il existait des métiers et des formations permettant de prendre part à la défense (numérique) des hôpitaux. J'ai donc entrepris une démarche de reconversion professionnelle et un parcours de 2 ans de formation : une première année pour acquérir les bases nécessaires en systèmes et réseaux puis j'ai intégré le cursus Expert en Sécurité Digitale (ESD) à l'ENI de Rennes. A 50 ans, je suis cheffe de projets cybersécurité au Groupement régional e-Santé Bretagne et contribue activement à la protection de nos établissements sanitaires et médico-sociaux ! C'est un métier passion qui requiert une appétence pour la technique mais aussi (surtout) un bon relationnel car il faut expliquer, fédérer, convaincre en permanence. »

## Témoignage de Vincent, Bachelor Cybersécurité et Réseaux de l'ECE

« Le Bachelor Cybersécurité et Réseaux de l'ECE m'a offert une formation technique solide, me permettant d'acquérir des compétences pointues en sécurité informatique, pentests, et gestion des réseaux. Cette formation m'a donné la confiance nécessaire pour intégrer le cursus ingénieur de l'ECE. Grâce à mon alternance et à l'expérience que j'ai acquise en autodidacte, j'ai pu rapidement me spécialiser et décrocher un poste d'ingénieur en cybersécurité défensive. Aujourd'hui, je veille à maintenir un haut niveau d'exigence sécuritaire pour l'ensemble des datacenters du Groupe Asten, en collaboration directe avec notre RSSI. »

## AUTRES FORMATIONS

D'autres formations dans les domaines suivants sont également appréciées des employeurs de la cybersécurité

Electronique

Electronique embarquée

Test logiciel

Intelligence artificielle

Data

Juridique / droit

Gestion de crise ..

La cybersécurité étant un domaine en constante évolution, il est important de continuer à se former tout au long de son parcours professionnel. Des formations courtes sont proposées par différents opérateurs.

[PENSEZ ÉGALEMENT À LA VALIDATION DES ACQUIS D'EXPÉRIENCE !!](#)



Pour toutes questions dans le cadre d'une reconversion professionnelle, n'hésitez pas à contacter par mail Stéphane Szymanski – référent du Syndicat Initiative Cyber mis en place par Rennes Métropole  
stephane.szymanski@univ-rennes.fr

## Liste des établissements de formations

### ETABLISSEMENTS

AFPA

AFTEC

CENTRALE SUPÉLEC Rennes \*

CyberSchool

ECE (Omnes Education )

ENI

EPITECH

EPSI

ESIR \*

ESNA

GRETA

Groupe St-Jean (Pôle Sup De La Salle)

IMT Atlantique \*

INSA Rennes \*

IUT de St Malo, UR \*

LYCEE Bréquigny

LYCEE Charles Tillon

LYCEE Coëtlogon

LYCEE Hélène Bach

SIMPLON

Sup de Vinci

UNIVERSITE DE RENNES \*

YNOV Campus

WIS

### SITES INTERNET

[afpa.fr](http://afpa.fr)

[aftec.fr](http://aftec.fr)

[centralesupelec.fr](http://centralesupelec.fr)

[cyberschool.univ-rennes.fr](http://cyberschool.univ-rennes.fr)

[ece.fr](http://ece.fr)

[eni-ecole.fr](http://eni-ecole.fr)

[epitech.eu](http://epitech.eu)

[epsi.fr](http://epsi.fr)

[esir.univ-rennes.fr](http://esir.univ-rennes.fr)

[esna.bzh](http://esna.bzh)

[greta-bretagne.ac-rennes.fr](http://greta-bretagne.ac-rennes.fr)

[groupe-saintjean.fr](http://groupe-saintjean.fr)

[imt-atlantique.fr](http://imt-atlantique.fr)

[insa-rennes.fr](http://insa-rennes.fr)

[iut-stmalo.univ-rennes.fr](http://iut-stmalo.univ-rennes.fr)

[lycee-brequigny.fr](http://lycee-brequigny.fr)

[lyceecharlestillon.fr](http://lyceecharlestillon.fr)

[lycee-coetlogon.ac-rennes.fr](http://lycee-coetlogon.ac-rennes.fr)

[lycee-basch.fr](http://lycee-basch.fr)

[simplon.co](http://simplon.co)

[supdevinci.fr](http://supdevinci.fr)

[univ-rennes.fr](http://univ-rennes.fr)

[ynov.com](http://ynov.com)

[wis-ecoles.com](http://wis-ecoles.com)

\* Établissements membres du programme **CyberSchool**. Programme porté par France 2030 qui vise à développer les formations cybersécurité sur le territoire breton.

# REMERCIEMENTS

Ce document est le fruit d'un travail porté par un collectif d'acteurs impliqués dans la feuille de route de Rennes Métropole sur la filière cybersécurité :

- opérateurs de formations,
- acteurs de l'emploi,
- employeurs privés et publics..

Il s'inscrit dans le cadre de la démarche de Gestion Prévisionnelle des Emplois et des Compétences Territoriale.

Démarche co-pilotée par WE KER qui bénéficie dans ce cadre d'un financement de l'Etat, de Rennes Métropole et du soutien de l'Union Européenne.



Cofinancé par  
l'Union européenne

Ce document a été réalisé gracieusement par l'agence de communication **Solatypic**, agréée Entreprise Adaptée, en partenariat avec l'**Institut Solacroup**, centre de formation d'excellence pour des publics porteurs de handicap invisible.

Ce document constitue une photographie des formations en cybersécurité proposées en présentiel sur le territoire de Rennes Métropole en 2024. Il a vocation à faire l'objet d'une mise à jour annuelle.

Si vous constatez que votre formation n'apparaît pas dans le catalogue ou que des erreurs se sont glissées, n'hésitez à contacter : [rdiverres@we-ker.org](mailto:rdiverres@we-ker.org)



Cofinancé par l'Union européenne

Édition et conception graphique réalisées par l'agence web adaptée

# solatypic



Institut Solacroup