Cybersécurité

Une palette de métiers et de formations

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

2025

Document réalisé en janvier 2026, porté par le GT opérateurs formation cyber et partenaires emplois coordonné par We Ker dans le cadre de sa mission GPEC-T sur la filière cybersécurité et inscrit dans la feuille de route cyber de Rennes Métropole.

Cofinancé par l'Union européenne

EDITO

« La cybersecurité 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. »

Sébastien SEMERIL

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

SOMMAIRE

C'EST QUOI LA CYBERSÉCURITÉ ?

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.

Le secteur 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, du régiment de cyberdéfense, 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 numériques en tant qu'Architecte sécurité, en prévention ou en défensive et en gestion des risques cyber ou encore choisir des métiers plus transverses comme celui de juriste spécialisé 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 en cybersécurité, c'est aussi s'engager pour défendre les intérêts de tous face aux menaces des attaques informatiques : les menaces sont diverses, allant des ransomwares aux logiciels malveillants sur ordinateurs et téléphones mobiles, en exploitant les failles de sécurité détectées dans différents systèmes et applications (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 organismes publiques ou entreprises privése, 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 constante évolution

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 continus, 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 la gouvernance, le management et 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 MÉTIERS 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. Tous 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 !!

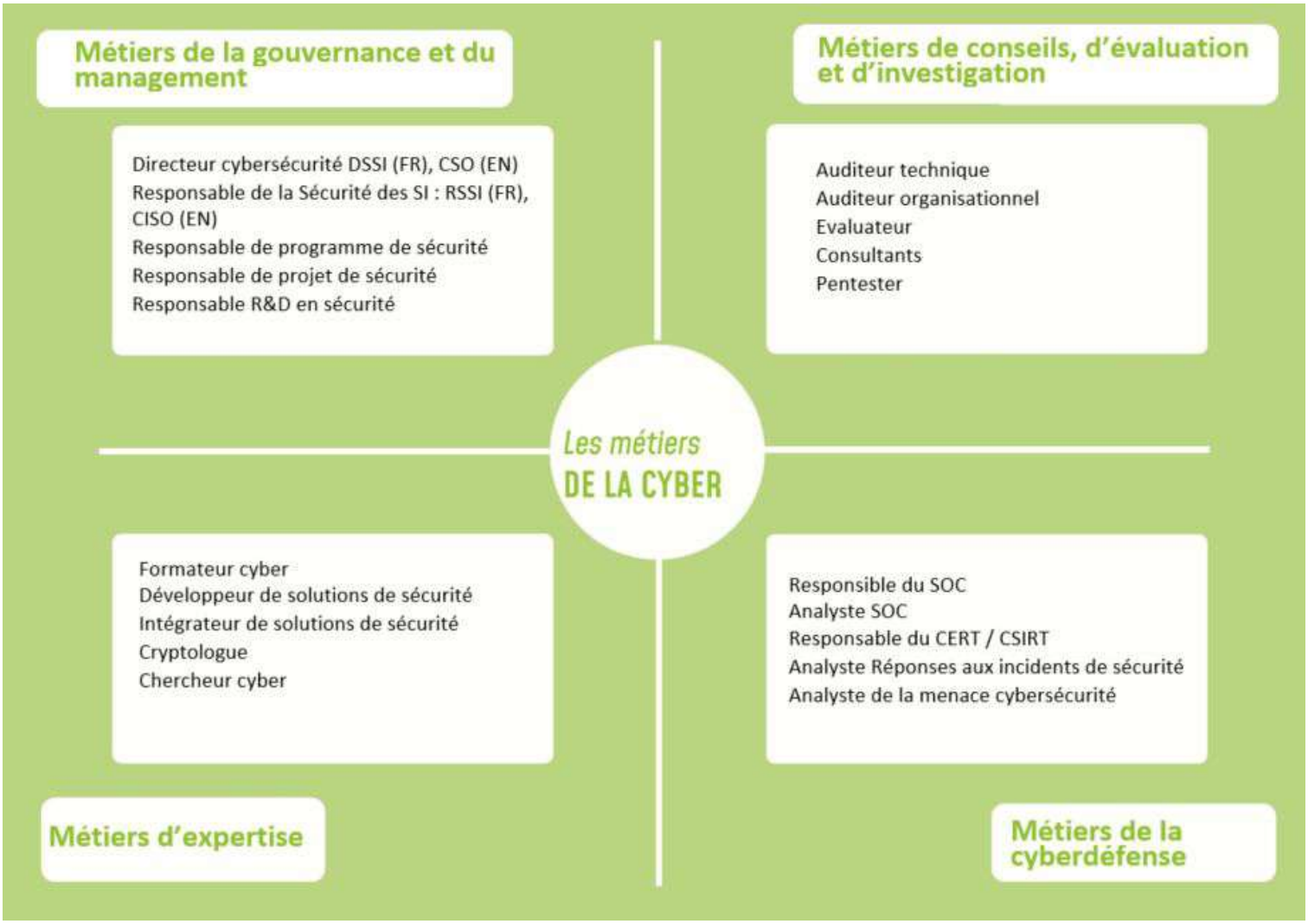
Les domaines de la Cybersécurité

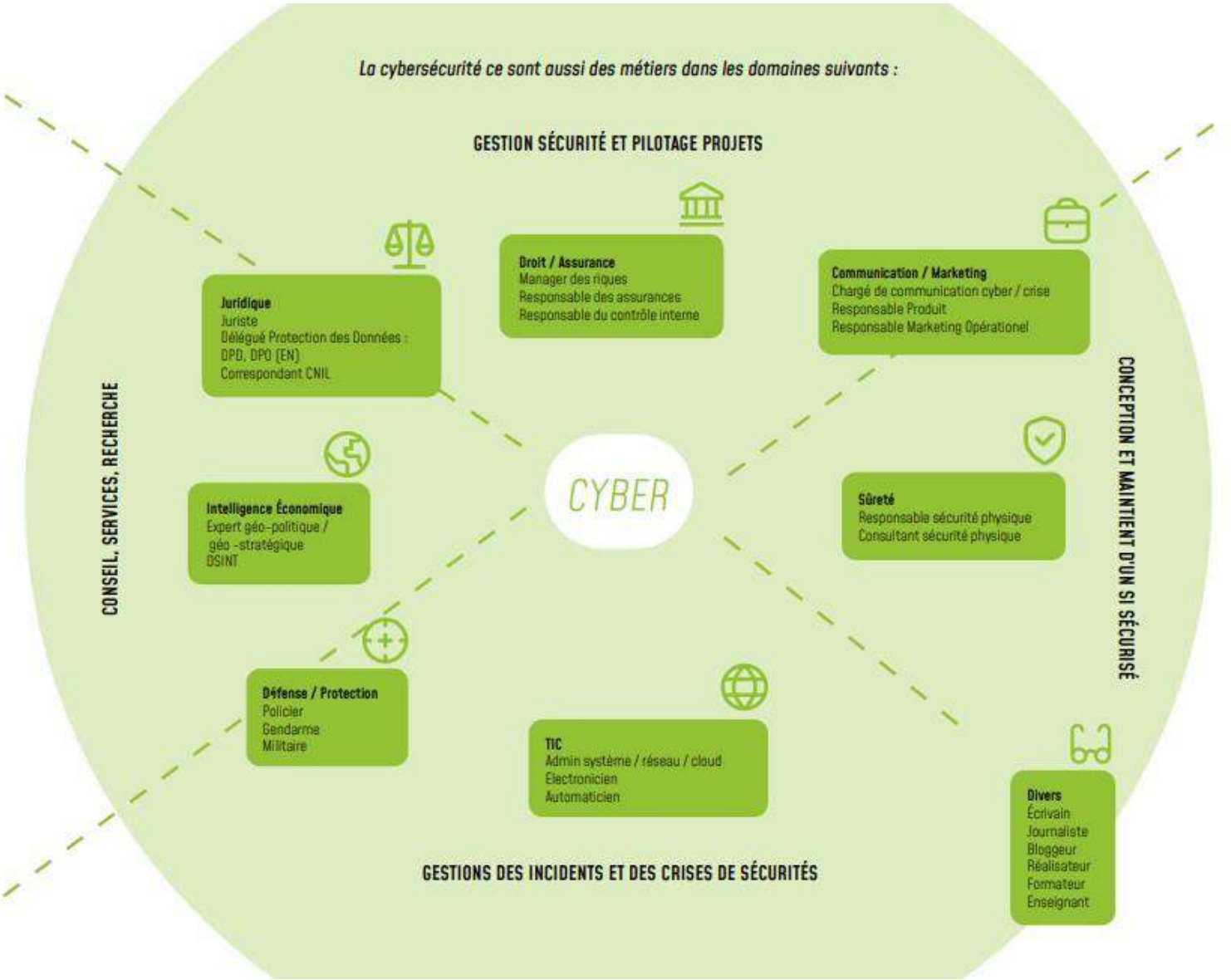
Cybersécurité & Business
Prestations de services cyber
(Entreprise Service du Numérique)
Ventes / Développement de produit de sécurité
(Logiciel / Matériel / Réseau / Cloud…)
Surveillance / Défense interne de l'entreprise

Cybersécurité étatique
Inter Ministériel (ANSSI)
Ministère des Armées : (DGA,COMCYBER, Régiment de cyberdéfense (Armées de terre)
Autres ministères : police, gendarmerie, douanes…
Service de renseignement (DGSE, DGSI…)

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

POUR DES ILLUSTRATIONS DE PARCOURS CONSULTEZ LE DERNIER CATALOGUE DE L'ONISEP DANS LEQUEL VOUS DÉCOUVRIREZ DES PARCOURS INSPIRANTS : de RSSI, ARCHITECTE CYBER, GESTIONNAIRE DE CRISE, ANALYSTE SOC…Publication : Les métiers de la cybersécurité - Onisep


Métiers de la gouvernance et du management
Directeur cybersécurité DSSI (FR), CSO (EN)
Responsable de la Sécurité des SI : RSSI (FR), CISO (EN)
Responsable de programme de sécurité
Responsable de projet de sécurité
Responsable R&D en sécurité
Métiers de conseils, d'évaluation et d'investigation
Auditeur technique
Auditeur organisationnel
Evaluateur
Consultants
Pentester
Les métiers
DE LA CYBER
Formateur cyber
Développeur de solutions de sécurité
Intégrateur de solutions de sécurité
Cryptologue
Chercheur cyber
Responsible du SOC
Analyste SOC
Responsable du CERT / CSIRT
Analyste Réponses aux incidents de sécurité
Analyste de la menace cybersécurité
Métiers d'expertise
Métiers de la cyberdéfense


La cybersécurité ce sont aussi des métiers dans les domaines suivants :
GESTION SÉCURITÉ ET PILOTAGE PROJETS
Juridique
Juriste
Délégué Protection des Données : DPD, DPO (EN)
Correspondant CNIL
Droit / Assurance
Manager des risques
Responsable des assurances
Responsable du contrôle interne
Communication / Marketing
Chargé de communication cyber / crise
Responsable Produit
Responsable Marketing Opérationel
CONSEIL, SERVICES, RECHERCHE
CYBER
CONCEPTION ET MAINTIENT D'UN SI SÉCURISÉ
Intelligence Économique
Expert géo-politique / géo -stratégique
OSINT
Sûreté
Responsable sécurité physique
Consultant sécurité physique
Défense / Protection
Policier
Gendarme
Militaire
TIC
Admin système / réseau / cloud
Electronicien
Automaticien
Divers
Écrivain
Journaliste
Blogueur
Réalisateur
Formateur
Enseignant
GESTIONS DES INCIDENTS ET DES CRISES DE SÉCURITÉS

LES MÉTIERS de CONSEILS, D'ÉVALUATION et d'INVESTIGATION

Les objectifs 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

Ces métiers s'appuient sur la connaissance des menaces potentielles et les méthodes utilisées par les attaquants afin de garder une longueur d'avance et limiter les angles morts.

Exemples de métiers :

L'auditeur.trice 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 cyber attaquants. L'auditeur.trice 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'actions concrets pour corriger les vulnérabilités mises en lumière par ses tests et les scénarios utilisés au cas par cas.

L'Évaluateur.trice sécurité des systèmes et produits informatiques joue un rôle crucial dans la protection des infrastructures numériques.

- Analyse et évalue les risques de sécurité des systèmes et produits informatiques, réalise des audits de sécurité pour identifier les vulnérabilités et les failles.
- Propose des solutions pour renforcer la sécurité et prévenir les attaques informatiques
- Effectue des tests d'intrusion pour évaluer la robustesse des systèmes face aux tentatives d'effraction
- Documente les procédures de sécurité et forme les utilisateurs aux bonnes pratiques de sécurité
- Collabore avec les équipes de développement pour intégrer la sécurité dès la conception des produits

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.
Les métiers du SOC vont fortement évoluer avec l'arrivée de l'IA. Elle rend le travail moins monotone et plus efficace, Grâce à l'automatisation, le métier d'analyste se redessine. Les pros n'ont plus à traiter des tâches chronophages et ont désormais du temps pour se concentrer sur d'autres tâches à plus forte valeur ajoutée.
Comment l'IA a révolutionné le SOC ? | EPSI
Exemples de métiers de la cyberdéfense :

Le.la Sécurity Opérator
Ce professionnel surveille 24h/24h et 7J/7 les alertes qui remontent dans le SOC. Il.elle 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.elle priorise, trie et corrèle les alertes qui pourraient nuire à un système d'information selon leur degré de criticité. Il.elle 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.la manager SOC
Il agit de l'alter ego du RSSI (le Responsable de la Sécurité des Systèmes d'Information) sur la partie opérationnelle. Il.elle 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.elle travaille en étroite collaboration avec les Analystes sécu pour limiter au maximum les risques de crise. Il.elle a un rôle de conseiller et oriente les clients sur la meilleure stratégie de sécurité à adopter

LES MÉTIERS DE LA GOUVERNANCE et du MANAGEMENT CYBER

Dans le secteur de la cybersécurité, la gouvernance regroupe les protocoles, outils, méthodologies et procédures à suivre pour protéger et défendre les organisations contre les attaques numériques et plus particulièrement en cas de crise. Avec pour objectif d'assurer la continuité de ces activités.
Les métiers de la cybersécurité et plus particulièrement de la gouvernance cyber peuvent inclure plusieurs expertises

Le.la RSSI

Le.la Responsable de la sécurité des systèmes d'information (RSSI) assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation. Il.elle définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience,remédiation) et veille à son application. Il.elle assure un rôle de conseil,d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction de son périmètre.
Il.elle s'assure de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des systèmes d'information. Selon la taille de l'organisation, il.elle joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI ou encadre une équipe.

Coordinateur.trice sécurité

Le.la coordinateur.trice sécurité assure un appui au pilotage des actions de sécurité des SI sur un périmètre de l'organisation (sur une entité ou bien en lien avec une thématique : par exemple, coordination des actions de sécurité sur les environnements Cloud, coordination de la mise en conformité à une réglementation, etc.). Il.elle apporte un support aux équipes opérationnelles pour la réalisation des actions de sécurité et assure le suivi des plans d'actions.

LES MÉTIERS DE LA 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.la Chef-fe de projet Cyber

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.la PMO (ou Project Management Officer)

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

L'Architecte de sécurité

L'architecte sécurité des SI s'assure que les choix techniques et techno-logiques des projets IT et métiers respectent les exigences de sécurité de l'organisation. Il.elle constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation.

Le responsable de la communication cyber

Il.elle sensibilise les équipes. Il peut par exemple **créer des supports de formations** sous des formats originaux pour rappeler les bonnes pratiques cyber pour rendre les salariés plus attentifs.

LES MÉTIERS DE CONSEILS CYBER

Ce domaine englobe les activités de conseils et de recherche, axées sur l'innovation et le développement de solutions de sécurité.

Le.la consultant.e cyber

Le.la consultant.e en cybersécurité intervient au sein d'une société de services ou du pôle de conseil interne d'une organisation. Il propose, à partir d'un diagnostic, des solutions, méthodes, outils. qui répondent aux enjeux posés. Il mobilise pour ce faire des éléments issus de son expertise et de son expérience ainsi que des outils développés en interne.Il anticipe les évolutions du contexte de cybersécurité, apporte un retour d'expérience et une vision des pratiques du marché. Il peut contribuer à la définition de la stratégie de cybersécurité de l'organisation et à la mise en œuvre des solutions de cybersécurité. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.

Le.la chercheur.se en sécurité des systèmes d'information

Il.elle se consacre à la recherche sur les nouvelles menaces et le développement de solutions innovantes.

Le.la consultant.e conformité

Spécialisé.e 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.elle s'assure que la sécurisation des informations sensibles respecte le RGPD et les préconisations de la CNIL en lien avec le DPO (Le délégué à la protection des données (DPO) | CNIL)Il.elle 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).

Une partie des éléments cités ci-dessus provienne du site de ADVENS avec leur accord
https://www.advens.com/travailler-dans-la-cybersecurite/

Quelques métiers connexes

Ces rôles complémentaires jouent également un rôle crucial dans la cybersécurité.

Le.la Risk Manager
Évalue et gère les risques liés à la cybersécurité, en assurant une protection adéquate des données.

Le.la Délégué.e à la Protection des données
Veille à la conformité des organisations avec les réglementations sur la protection des données, comme le RGPD.

Le.la Juriste spécialisé.e en cybersécurité
Conseille les entreprises sur les aspects légaux liés à la cybersécurité, notamment en matière de protection des données, de conformité réglementaire et de gestion des risques juridiques.

Ces rôles complémentaires jouent également un rôle crucial dans la cybersécurité.

POUR DES ILLUSTRATIONS DE PARCOURS CONSULTEZ LE DERNIER CATALOGUE DE L'ONISEP DANS LEQUEL VOUS DÉCOUVRIREZ DES PARCOURS INSPIRANTS : de RSSI, ARCHITECTE CYBER, GESTIONNAIRE DE CRISE, ANALYSTE SOC…Publication : Les métiers de la cybersécurité - Onisep

CARTOGRAPHIE DES MÉTIERS DE LA CYBERSÉCURITÉ – RÉFÉRENCE ANSSI

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.

Compétences recherchées

Compétences recherchées - Savoir-faire

- Compétences générales

Informatique - système, réseau - anglais

- Compétences méthodologiques

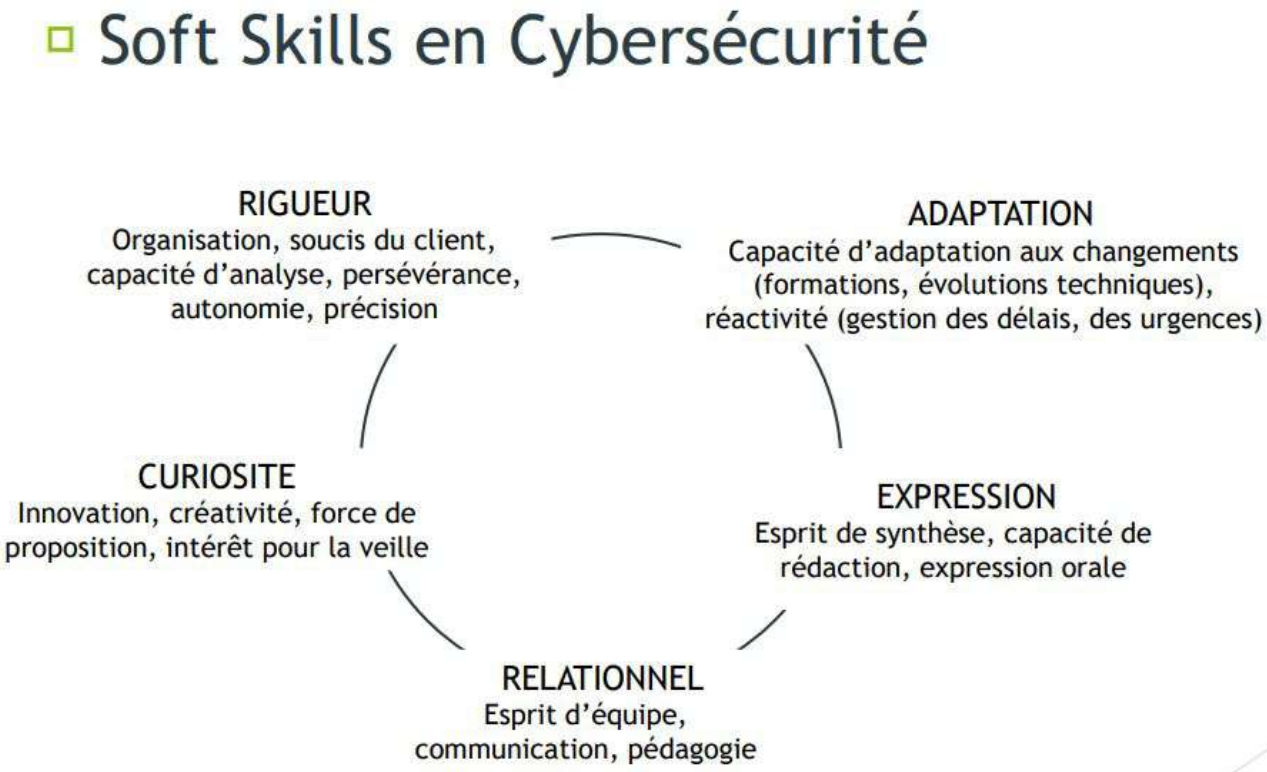
Analyse, rédaction, organisation, animation

- Compétences spécifiques cyber

Cryptologie, rétro-ingénierie, investigation numérique

- Double compétence

Télécom, automaticien, électronicien, IA, BigData, droit, communication



Quelques liens pour en savoir plus et commencer à se former

Le Pôle d'Excellence cyber : Recherche, Formation, Développement Industriel - Pôle d'excellence cyber

Le ComCyber : Le Commandement de la cyberdéfense (COMCYBER) | Ministère des Armées et des Anciens combattants

ANSSI : Agence nationale de la sécurité des informations : l'ANSSI

Cybermalveilance : cybermalveillance : les bonnes pratiques

CNIL : CNIL

Stratégie cybersécurité Nationale 2026-2030 : Stratégie nationale de cybersécurité 2026-2030 | SGDSN

Cybersécurité : Un défi citoyen et stratégique - Cadettes de la cyber PEC : Publications - Pôle d'excellence cyber

Pour en savoir plus sur les métiers et les compétences recherchées

- Les profils de la cybersécurité ANSSI : Les profils de la cybersécurité | ANSSI
- Les métiers de la cybersécurité ANSSI : Panorama des métiers de la cybersécurité | ANSSI
- Cahier ONISEP fév 2026 - Publication : Les métiers de la cybersécurité - Onisep
- Cartographie des métiers du numérique OPIEC : https://www.opiiec.fr/cartographie-des-metiers
- Référentiel des compétences des métiers de la cyber : Référentiel des compétences des métiers de la cyber - Campus Cyber
- Découverte de la cybersécurité et des métiers : DemainSpécialisteCyber
- Campus CYBER Evolution : https://evolution.campuscyber.fr/ - une plateforme pour découvrir les métiers, les formations, les challenges, jeux et différentes ressources
- Etude APEC- Emploi cadre cybersécurité : Cybersécurité, un marché de l'emploi cadre diversifié et de plus en plus porteur
- Replay cybesécurité, on hacke les clichés : Actualités - Replay. Cybersécurité : on hacke les clichés ! Le point sur les enjeux et les métiers
- Fiches métiers France travail - métiersscope : https://candidat.francetravail.fr/metierscope/fiche-metier/M1856/expert-experte-en-cybersecurite

Pour en savoir plus sur la cybersécurité à Rennes et plus globalement en Bretagne

- La cybersécurité à Rennes , un secteur stratégique : La cybersécurité à Rennes, un secteur stratégique
- Portrait du numérique - Gref Bretagne : Actualités - Portrait du numérique en Bretagne
- Plateforme Idéo Bretagne : 6 métiers pour travailler dans la cybersécurité | Ideo
- Agence next - cybersécurité en Bretagne : Cybersecurité en Bretagne - BDI
- Campus Bretagne Cyber Alliance : https://www.cyberalliance.bzh/

Quelques liens pour en savoir plus et commencer à se former

Quelques moocs pour commencer à se former

Niveau débutant

1 - SecNumAcadémie (ANSSI - Agence nationale de la sécurité des systèmes d'information) (Attention : le 28 février 2026, le MOOC SecNumAcadémie fermera temporairement pour une refonte.)

🔗 Découvrir le MOOC : SecNumacadémie

2 - Mooc Cyber Malveillance - sensibilisation cyber - Comprendre les menaces et adopter les bonnes pratiques

🔗 Découvrir le MOOC : SensCyber: Apprendre et tester vos connaissances - Assistance aux victimes de cybermalveillance

3 - L'atelier RGPD (CNIL)
Idéal pour s'initier à la protection des données ou approfondir ses connaissances.
🔗 Découvrir le MOOC :Atelier RGPD

4 - MOOC : qu'est-ce que l'OSINT (Open Source INtelligence)

🔗 Découvrir le MOOC :Cours : 🎓 MOOC OSINT-FR - Qu'est-ce que l'OSINT

5 - Initiez-vous à

- PYTHON : Apprenez les bases du langage Python - OpenClassrooms
- LINUX : Initiez-vous à Linux - OpenClassrooms
- JAVASCRIPT : Apprenez à programmer en Java - OpenClassrooms

6 - Plateformes de Capture the Flag

- RootMe : Root Me
- Pico CTF : picoCTF
- Passe ton Hack d'abord (inscription auprès des enseignants) : Passe ton hack d'abord 2026 | Ministère des Armées et des Anciens combattants

Quelques liens pour en savoir plus et commencer à se former

Quelques moocs pour commencer à se former

NIVEAU Intermédiaire

1 - Administrer un système Linux : Administrez un système Linux - OpenClassrooms

2 - Gérez votre serveur Linux et ses services : Gérez votre serveur Linux et ses services - OpenClassrooms

3 - Sécurisez les accès Wi-fi : Sécuriser les accès Wi-Fi | ANSSI

NIVEAU Expert

1- Introduction à la méthode EBIOS Risk Manager

Un parcours structuré en 10 modules pour apprendre à gérer les risques cyber
🔗 Découvrir le MOOC : Introduction à la méthode EBIOS Risk Manager

2- Guide de la continuité d'activité – Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)
Anticiper les situations de crise, structurer un plan de continuité et garantir la résilience de vos services essentiels.
🔗 Découvrir le MOOC : Guide de la continuité d'activité -

3- SenCy-Crise – Commandement de la cyberdéfense (COMCYBER)
Se préparer à la gestion d'une crise cyber : adopter les bons réflexes avant, pendant et après un incident.
🔗 Découvrir le MOOC :Bienvenue dans SenCy-Crise - Assistance aux victimes de cybermalveillance

Des formations labellisées

Formations labellisées SecNumedu

L'objectif de **SecNumedu** est d'apporter aux étudiants 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.).
A noter, ce sont les établissements de formation qui doivent déposer un dossier pour obtenir la labeliisation auprès de l'ANSSI.

Lien pour accéder aux formations labellisées : Formations en sécurité informatique

- Des diplômes et des titres inscrits au RNCP (Répertoire Nationale des Certifications Professionnelle)
  Les diplômes nationaux et les titres professionnels délivrés par l'Etat (Bac pro, BTS, master..) 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 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.

Financer ses études grâce à l'armée

L'allocation financière spécifique de formation (AFSF) est une bourse qui permet aux étudiants et étudiantes de financer leurs études en informatique et en cyber jusqu'à 15 000€ par an selon l'armée d'appartenance et le niveau d'étude sous condition de s'engager ,à l'issue de l'obtention de leur diplôme, à servir l'armée pour un premier contrat.

La bourse proposée par les armées, aussi appelé Allocation financière spécifique de formation (AFSF), s'adresse aux étudiants qui se forment dans des domaines stratégiques pour la défense du pays, notamment dans la cybersécurité et l'informatique. Après la terre, la mer, l'air et l'espace, le cyberespace s'impose aujourd'hui comme le cinquième champ de bataille.

Pour en savoir plus :

Financer ses études grâce à l'armée : tout savoir sur la bourse informatique et cyber

Des passerelles possibles

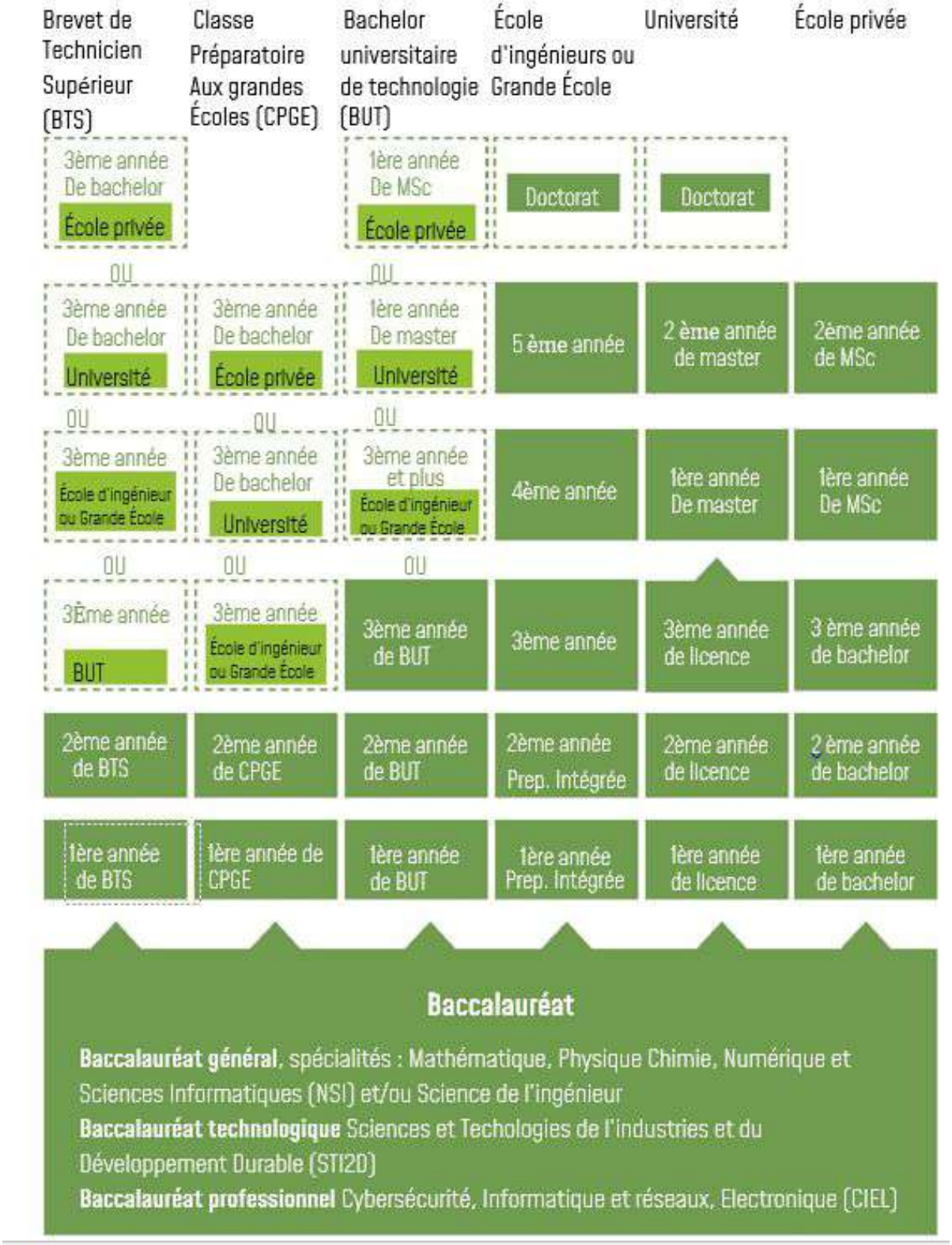
"L'enseignement supérieur français offre diverses possibilités de parcours permettant aux étudiants d'adapter leur parcours académique et professionnel en fonction de leurs aspirations et de leurs projets, incluant des passerelles entre les établissements privés et publics. Si la transition des diplômes 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."

A noter en fonction des formations, la dominante cybersécurité peut correspondre à différents niveaux. Un travail mené par le Gref Bretagne fait état des niveaux suivants :

Parcours possibles



Liste des formations par niveau

Pour travailler dans le domaine de la cybersécurité, il existe différents parcours possibles avec des formations dédiées à la cybersécurité et des formations tournées vers le numérique, présentées dans ce catalogue.

Ce catalogue n'est pas exclusif. Il existe d'autres formations notamment pour les métiers transverses à la cybersécurité comme en droit, communication…

FORMATION Niveau 4 / Bac

FORMATION Niveau 5 / Bac+2

FORMATION Niveau 6 / Bac+3

FORMATION Niveau 7 / Bac+5

A noter la possibilité de poursuivre au delà du Bac +5, notamment dans le cadre de doctorat porté par les universités

FORMATION Niveau 4 / Bac

FORMATION Niveau 4 / Bac

Bac pro Cybersécurité, Informatique et Réseaux, Électronique (CIEL)

Diplôme niveau 4 délivrée par Ministère de L'education Nationale et de la Jeunesse

RNCP : 37489 (2028)

★ Lycée Professionnel Charles Tillon et Coëtlogon
★ CMA FORMATION RENNES BRUZ

3 ans

Formation Initiale ou en apprentissage

Lien formation site RNCP

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, Electronique" couvrent les domaines :

- de la réalisation de la production,
- de l'intégration, de la maintenance de produits électroniques
- de la mise en oeuvre de réseaux informatiques, la valorisation de la donnée et de la cybersécurité.

FORMATION Niveau 4 / Bac

Certificat de spécialisation Cybersécurité

Formation post Bac en 1 an sous statut lycéen ou apprenti

Certification délivrée par Ministère de L'education Nationale et de la Jeunesse

RNCP : 37488(2028)

Lycée Coëtlogon Rennes

1 an à partir du Bac

Formation Initiale ou en apprentissage

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

DÉBOUCHÉS

Poursuite possible en BTS

Métiers

- Intégrateur.trice de solutions de sécurité.
- Opérateur ou opératrice en cybersécurité.
- Technicien.ne de maintenance informatique.
- Installateur.trice de réseaux informatiques.

FORMATION Niveau 5 / Bac+2

FORMATION Niveau 5 / Bac + 2

BTS CIEL

BTS CIEL Cybersécurité, Informatique et réseaux, Électronique (CIEL) - Option A informatique et réseau Diplôme délivré par Ministère de l'Enseignement supérieur et de la recherche et de l'Innovation

- ★ Lycée Professionnel Bréquigny
- ★ Rennes YNOV Campus
- ★ AFTEC Rennes

2 ans à partir du Bac

Formation Initiale ou en alternance

RNCP : 37391(2028)

Lien vers formation-RNCP

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 sytèmes 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 :

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

PRÉREQUIS

Bac professionnel SN, Bac technologique STI2D , Bac général, étudiants en réorientation

DÉBOUCHÉS

Poursuite d'études : licence informatique, licence pro, école ingénieur, BUT 3ème année Bachelor

Métiers

- 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

FORMATION Niveau 5 / Bac + 2

BTS SIO - Option B

SLAM Prépa intégrée Cybersécurité

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

- ★ AFTEC Rennes
- ★ EPSI
- ★ Pôle Sup de La Salle
- ★ Rennes YNOV Campus
- ★ *My Digital School.*

2 ans à partir du Bac

Formation Initiale ou en alternance

RNCP : 40792 (2028)

Lien vers formation-RNCP

PRÉSENTATION

Le BTS SIO option solutions logicielles et applications métiers (SLAM) a pour objectif de former les apprenant.e.s à développer, à adapter et à maintenir des solutions applicatives.
Le- la 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 professionnel SN, Bac technologique STI2D , Bac général (spécialités scientifique, numérique et SI) , étudiants en réorientation

DÉBOUCHÉS

Poursuite d'études : Tecnicien.ne Supérieur.e Spécialité Drone, licence, école ingénieur, BUT 3ème année, Bachelor systèmes Réseaux et cybersécurité

Métiers

- Développeur d'applications informatiques,
- Chargé d'études informatiques
- Technicien en informatique ou cybersécurité
- Testeur.euse en einformatique

Attention sur certains postes, nécessité d'avoir une habilitation (avec procédure allant de 6 à 8 mois).

FORMATION Niveau 5 / Bac + 2

BTS SIO - Option A - SISR

Brevet de Technicien Supérieur - Service Informatiques aux Organisations - Solutions d'Infrastructure, Systèmes et Réseaux

Diplôme délivré par le Ministère de l'enseignement supérieur et de la recherche

RNCP : 40792 (2028)

- ★ AFTEC Rennes
- ★ EPSI
- ★ ESNA
- ★ Pôle Sup de La Salle
- ★ Rennes YNOV Campus
- ★ *My Digital School*.
- ★ CMA FORMATION RENNES BRUZ

2 ans

Formation en alternance

Lien vers RNCP 40792

PRÉSENTATION

Le BTS SIO option solutions d'infrastructure, systèmes et réseaux (SISR) a pour objectif de former l'alternant•e à **assurer la sécurité, la maintenance et l'installation des réseaux et équipements informatiques**. A l'issue de cette formation, les apprenants devront être capables de :

- Gérer un système d'information après compromission
- Élaborer la maquette du dossier d'architecture technique
- Superviser le système d'information
- Se situer dans un environnement organisationnel réel
- S'immerger dans des contextes professionnels variés
- Sensibiliser les utilisateurs aux risques liés à la cybersécurité.

PRÉREQUIS

- Être titulaire d'un baccalauréat : BAC général, STI2D, STMG ou d'un BAC PRO (Systèmes Numériques ou Cybersécurité, Informatique et réseaux, ÉLectronique (CIEL)…)
- Satisfaire au process de recrutement

DÉBOUCHÉS

Poursuite d'études : Bachelor et Mastère Sécurité Informatique, Licence informatique à l'université, BUT Technico-commercial, BUT Développement d'applications Web, École d'ingénieur

Métiers

- Administrateur.rice réseaux
- Technicien.ne de maintenance
- Technicien support

FORMATION Niveau 5 / Bac + 2

Technicien Veilleur 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

★ Eni en partenariat avec le Greta Est Bretagne Rennes

5 mois poursuite en alternance possible

Formation continue Qualif Programme Région Bretagne

RNCP : 36164 (2027)

Lien vers formation-RNCP

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 de l'informatique et/ou une expérience professionnelle dans le domaine de l'informatique / Avoir des connaissances technologiques en informatique.

DÉBOUCHÉS

Poursuites d'études :

Cursus Bachelor universitaire de technologie « Réseaux et télécommunication en cybersécurité »,

Cursus universitaire : licence Sciences et ingénierie Cybersécurité défensive

Responsable en ingénierie informatique et cybersécurité

Cursus « École d'ingénieur » / Ingénieur Cyberdéfense ENSIBS Vannes.

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

FORMATION Niveau 5 / Bac + 2

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 continue sur 8 mois (6 mois de cours / 2 mois de stage) - ENI
Formation en 11 mois en initial ou 18 mois en alternance - AFTEC

Formation continue - Initiale- Alternance

Lien vers formation-RNCP

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

Poursuite d'étude : Bac+3 Administrateur Système DevOps, Bac+3 Administrateur Système et Réseau en 1 an ou Bac+4 Administrateur Système et Réseau en 2 ans, Bac+5 Expert en Sécurité Digitale possible à l'ENI.

Métiers

- Technicien .ne support
- Technicien.ne informatique
- Technicien.ne d'exploitation
- Technicien.ne systèmes et réseaux.

FORMATION Niveau 6 / Bac+3

FORMATION Niveau 6 / Bac +3

BUT Réseaux et Télécommunications

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

Formation labellisée SecNumedu délivrée par l'ANSSI

IUT de Saint Malo

3 ans à partir du Bac

Formation Initiale ou en apprentissage

RNCP : 35455 - 35511 - 35458 (2026)

Lien vers formation-RNCP

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

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.

Métiers

- Administrateur Systèmes et réseaux.
- Administrateur d'infrastructure de réseaux et télécommunications.

Dans les emplois notamment spécialisés en cybersécurité :

- Intégrateur.se de solution,
- Auditeur.trice
- analyste SOC,
- Responsable de la sécurité Informatique au sein d'une petite structure
- Administrateur.trice Data Center,
- Intégrateur.trice infrastructure Cloud,
- Technicien.ne sécurité des systèmes cloud (DevSecOps)
- Technico-commercial cyber.

FORMATION Niveau 6 / Bac +3

Administrateur Infrastructures sécurisées

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

★ AFPA Rennes

10 mois inscrit dans Qualif Programme de la Région Bretagne

Formation initiale - apprentissage

RNCP : 37680 (2026)

Lien vers formation-RNCP

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

Métiers

- Responsable infrastructure systèmes et réseaux.
- Administrateur.trice
  - cybersécurité
  - d'infrastructures et cloud
  - systèmes et réseaux (et sécurité),

FORMATION Niveau 6 / Bac +3

Bac +3 - Sécurité Informatique

CHEF DE PROJET

SYSTEMES, RESEAUX et SECURITE

Titre de niveau 6 reconnu par l'Etat, enregistré au RNCP délivré sous l'autorité de Sciences-U Lyon.

RNCP : 39115

CFA de La Salle - Rennes

1 an à partir du Bac + 2

Formation en alternance :

Contrat d'apprentissage ou contrat de professionnalisation

Lien vers le titre RNCP

CFA DE LA SALLE -

BAC +3 CHEF DE PROJET SYSTEMES - RESEAUX & SECURITE

PRÉSENTATION

Formation conçue pour répondre aux enjeux actuels de la cybersécurité. Cette formation de niveau 6 prépare des professionnels capables de concevoir des solutions systèmes et réseaux durables, de sécuriser et de faire évoluer les infrastructures et de conduire des projets informatiques responsables.

PRÉREQUIS

Cette formation s'adresse à toute personne titulaire d'une certification de niveau 5 (Bac+2) dans le domaine de l'administration des réseaux, de l'informatique ou du développement.

Exemples de diplômes ou titres acceptés : BTS SIO/CIEL, BUT2 Informatique, BUT Réseaux & Télécommunications, Titre de niveau 5 « Technicien Supérieur en Informatique » ou tout autre titre RNCP équivalent en informatique.

DÉBOUCHÉS

Poursuite d'études : Formation de niveau 7 en Sécurité informatique (CFA de La Salle) / formation Ingénieur Informatique / Master informatique à l'université

Métiers

- Administrateur.trice système - réseaux - infrastructure
- Analyste d'exploitation informatique
- Technicien.ne système et réseaux & sécurité
- Technicien.ne de maintenance système informatique
- Chef.fe de projet IT et sécurité

Bachelor Cybersécurité

Bachelor Cybersécurité délivré par l'EPITA

★ EPITA - Rennes

3 ans POST-BAC

Formation initiale (années 1 et 2) + alternance ou stage (année 3)

RNCP 41285 (échéance d'enregistrement : 31/08/2028)

Lien vers le site https://www.epita.fr/formation-cybersecurite-rennes/

PRÉSENTATION

Fondée en 1984, l'EPITA est une école de référence en informatique et en numérique. Forte d'une expertise reconnue, notamment en cybersécurité, elle a conçu le Bachelor Cybersécurité pour former en 3 ans des profils opérationnels, capables de répondre aux besoins d'un secteur qui recrute massivement.

Présente sur sept campus en France, EPITA s'appuie sur ses équipes de recherche et d'innovation pour nourrir une pédagogie concrète et connectée aux enjeux réels. Ce Bachelor bénéficie de cet écosystème et prépare à des opportunités de carrière dans tous les secteurs, en France comme à l'international, au sein d'un réseau de près de 10 000 diplômés présents dans plus de 2 000 entreprises.

PRÉREQUIS

Terminales générales avec au moins une spécialité scientifique.
Terminales STI2D ou Bac pro CIEL.

DÉBOUCHÉS

Métiers visés

- Analyste SOC
- analyste cybersécurité,
- pentester
- incident responder,
- consultant cybersécurité
- DevSecOps
- Administrateur systèmes et réseaux orienté sécurité
- Aanalyste forensic
-

Poursuite d'études possible: MSc Gouvernance de la Cybersécurité (EPITA), MSc in Computer Science, avec spécialisation cybersécurité (Computer Security), autres MSc EPITA (informatique, IA, data).

FORMATION Niveau 6 / Bac +3

Bachelor Cybersécurité

Certification délivrée

Titre Concepteur Développeur d'Applications d'EPITECH

★ EPITECH Rennes

3 ans , à partir du Bac

Formation initiale - alternance

RNCP : 37873 (2026)

Lien vers formation-RNCP

Epitech Rennes - Bachelor Cyber

PRÉSENTATION

Le Bachelor d'Epitech, accessible post-bac, se déroule en 3 ans (Bac +3) et forme des experts opérationnels sur les métiers émergents. Il offre 5 spécialités et la possibilité de personnaliser son parcours : international, alternance, stage ou entrepreneuriat. Côté cyber sont notamment traitées la sécurité offensive (Pentest, OSINT, Forensic), l'IA en cyber ainsi que la gouvernance des systèmes d'information. La 1re année aborde plusieurs langages de programmation, l'algorithmie, l'administration système et les bases de données. En 2e année sont approfondis les techniques de protection des systèmes d'information, l'Ethical Hacking, la cryptographie et l'IA appliquée à la cybersécurité.
En 3e année, l'expertise en cybersécurité s'affine à travers des projets avancés directement appliqués en entreprise.

PRÉREQUIS

Baccalauréat toutes filières

DÉBOUCHÉS

Métiers

- Pentester,
- SOC
- OSINT Analyst
- Responsable Sécurité des Systèmes d'Information,
- Data Protection Officer
- Ingénieur en Sécurité Informatique…

Poursuite d'étude possible en Master of Science ou MBA à Epitech, en Master, au sein du Programme Grande École d'Epitech (en 3e année) d'Epitech

Bachelor Cybersécurité et Administrateur Réseaux

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

RNCP : 37680 (2026)

★ My Digital School

Formation sur 1 an à partir du Bac +2

Formation initiale ou en alternance

Lien vers formation-RNCP

My Digital School - Bachelor Cybersécurité et Administration Réseau

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.trice systèmes, réseaux et sécurité
- Administrateur.trice réseaux
- Chef.fe de projet
- Responsable informatique
- Analyste en sécurité réseaux
- Consultant.e cybersécurité

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

Bachelor Systèmes Réseaux et Bases de données

Certification Administrateur système, réseaux et bases de données" délivrée par l'IGS

★ EPSI Rennes

12 mois

Formation initiale ou en alternance

RNCP : 35594 (2026)

Lien vers formation-RNCP

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.trice systèmes et réseaux et sécurité
- Administrateur.trice systèmes
- Administrateur.trice réseaux
- Administrateur.trice Cloud
- Administrateur.trice des systèmes d'informations.

Poursuite d'études :
Msc expert en informatique et système d'information
Msc Expert en Cybersécurité

Bachelor Systèmes Réseaux et Cloud

Certification professionnelle "Coordinateur de projet informatiques - Infrastructures -cloud - applicatives ou data - de niveau 6 délivrée par Association Sup de Vinci

★ Sup de Vinci Rennes

12 mois en alternance

Contrat d'apprentissage ou de professionnalisation

RNCP : 38478 (2028)

Lien vers formation-RNCP

Bachelor Cybersécurité, Système & Réseau et Cloud - Sup de Vinci

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 .

Ce bachelor t'apprend à connecter, sécuriser et faire évoluer les systèmes et les serveurs, sur site ou dans le cloud. En un an, tu deviens un professionnel opérationnel grâce à l'alternance, et mets en application la théorie vue en cours avec de réels enjeux de performance et sécurité.

PRÉREQUIS

Pour faire acte de candidature, il faut être en cours d'obtention ou titulaire d'un Bac+2 minimum - Niveau 5 (BTS,L2) reconnu par l'Etat ou 120 crédits ECTS

1 /Admission en Post-bac avec les deux premières années en initial + choix de la spécialisation en 3ème année en alternance
2/ Intégration de la 3eme Année en admission parallèle après validation d'un BAC + 2 (160 crédits Ects) niveau 5

DÉBOUCHÉS

Métiers

- Administrateur.trice systèmes et réseaux
- Responsable informatique PME/PMI
- Administrateur.trice 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.

FORMATION Niveau 6 / Bac +3

Bachelor Développeur Data et Intelligence Artificielle

Certification professionnelle de « Développeur En Intelligence Artificielle » délivrée par le Ministère du Travail du Plein Emploi et de l'Insertion, Certification délivrée par le Ministère du Travail

RNCP : 37827 (2028)

★ OMNES ECE Rennes

12 mois à partir du Bac +2

Formation initiale ou en alternance

Lien vers formation-RNCP

PRÉSENTATION

La spécialisation Développeur Data et Intelligence Artificielle en troisième année de Bachelor offre une formation complète aux technologies de pointe dans le domaine de la data et de l'intelligence artificielle. Conçue pour répondre aux besoins croissants du marché, cette spécialisation prépare les étudiants à devenir des experts en collecte, stockage et exploitation de données dans des projets innovants d'IA.

PRÉREQUIS

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

DÉBOUCHÉS

Métiers

- Développeur.se IA
- Développeur.se Machine Learning
- Data Développeur
- Développeur.se Web et Mobile
- Analyste Programmeur Informatique
- Architecte Réseaux et SI au sein d'entreprises de services numériques

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

FORMATION Niveau 7 / Bac+5

FORMATION Niveau 7 / Bac +5

Master cybersécurité parcours Sécurité logicielle et matérielle

Diplôme National Universitaire délivré par l'Université de Rennes.

La formation bénéficie du Label SecNumedu délivré par l'ANSSI.

★ Université de Rennes - ISTIC

2 ans à partir de la licence

Formation initiale

RNCP : 34126 (2024)

Lien vers formation-RNCP

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 étudiants 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'études possible en Mastère spécialisé ou doctorat .

FORMATION Niveau 7 / Bac +5

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

Diplôme National Universitaire délivré par l'Université de Rennes.

La formation bénéficie du Label SecNumedu délivré par l'ANSSI.

RNCP : 34274 (2024)

★ Université de Rennes - UFR Mathématiques

2 ans à partir de la licence

Formation initiale

Lien vers formation-RNCP

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.

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'études possible en doctorat.

FORMATION Niveau 7 / Bac +5

Master cybersécurité parcours Responsable de la Sécurité des Systèmes d'Information (RSSI)

Diplôme National Universitaire délivré par l'Université de Rennes.

★ Université de Rennes - ISTIC

2 ans à partir de la licence ou du BUT

Formation en alternance

RNCP : 34126 (2024)

Lien vers formation-RNCP

PRÉSENTATION

Ce Master prépare les étudiants à la mise en 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 Électronique
Être titulaire d'un BUT Réseaux Télécommunications option cybersécurité ou d'un BUT informatique

DÉBOUCHÉS

Métiers

- RSSI
- Consultant.e cybersécurité
- Auditeur.trice organisationnel
- Consultant.e GRC (Gouvernance, Risques et Conformité)
- Spécialiste en sécurisation des infrastructures de Système d'information.

FORMATION Niveau 7 / Bac +5

Ingénieur spécialité Systèmes Numériques et Réseaux

Titre D'ingénieur délivré par l'École Supérieure d'Ingénieurs de Rennes.

★ ESIR Université de Rennes

3 ans, à partir du bac +2

Formation en alternance.

RNCP : 39292 (2027)

Lien vers formation-RNCP

PRÉSENTATION

La spécialité Systèmes Numériques et Réseaux forme des ingénieurs en alternance pour répondre aux besoins des entreprises dans les domaines de l'électronique, de l'informatique et des réseaux. À compter du second semestre de la deuxième année, un parcours est à choisir : "Systèmes Numériques sans fil" cible plus spécifiquement les métiers de conception et de caractérisation de systèmes électroniques haute fréquence et embarqués et "Clouds, Réseaux et Cybersécurité (CRC)" cible quant à lui les métiers en lien avec le développement des Clouds, des réseaux et de la cybersécurité pour améliorer l'efficacité et la sécurité des systèmes et des réseaux.

PRÉREQUIS

- Un BTS Cybersécurité, Informatique et réseaux, Electroniques (CIEL), Systèmes Numériques (SN) ou Assistance Technique d'Ingénieur (ATI)
- Un BUT 2 ou 3 Génie Électrique et Informatique Industrielle (GEII) ou Réseaux & Télécommunications (R&T)
- Une licence 2 ou 3 Sciences pour l'ingénieur / réseaux / électronique
- Un cycle préparatoire de l'Esir

DÉBOUCHÉS

Métiers

- Ingénieur R&D en électronique numérique
- Ingénieur Tests et mesures
- Ingénieur R&D en électronique radio fréquence
- Ingénieur avant-ventes
- Ingénieur de déploiement de réseaux de télécom
- Administrateur de réseaux informatique
- Architecte de réseaux informatiques
- Ingénieur Cloud/Virtualisation
- Responsable Sécurité des Systèmes d'Information (RSSI)

FORMATION Niveau 7 / Bac +5

Ingénieur mention Cybersécurité

Titre d'ingénieur délivré par CentraleSupélec.

★ CentraleSupélec Rennes

3 ans, à partir du Bac + 2

Formation en alternance. Cours en cybersécurité en 3ème année

RNCP : 39502 (2025)

Lien vers formation-RNCP

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. 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

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 Audits

FORMATION Niveau 7 / Bac +5

Ingénieur en Informatique
Parcours Cybersécurité

Titre D'ingénieur diplômé du Conservatoire National des Arts et Métiers (CNAM) - spécialité Informatique, parcours cybersécurité

reconnu par la CTI

RNCP : 38461 (2028) ,38105 et 39126 (2026)

★ ESNA Rennes / EiCnam

1 an (pour 38105) à 3 ans

Formation en alternance

Lien vers RNCP 38461

Lien vers RNCP 38105

Lien vers RNCP 39126

PRÉSENTATION

L'ingénieur cybersécurité sera en mesure :

- De déployer tout ou partie des architectures de sécurité des systèmes d'informations. Des datacenter aux IoT, réseaux de capteurs/actionneurs intelligents sécurisés, systèmes embarqués ou tout objet communicant sécurisé.
- D'intégrer, mettre en oeuvre, configurer tous les dispositifs visant la protection de ces composants de sécurité, leurs architectures et protocoles.
- De mettre en oeuvre un service de veille et de renseignement et d'intelligence de la menace (CTI)
- D'approfondir ses connaissances et d'acquérir par lui-même une expertise technique élevée
- D'auditer la sécurité d'un système d'information en constante évolution, de le corriger et l'optimiser par l'application de contre mesures adaptées.
- Enfin face aux situations d'incidents de sécurité, il sera en mesure de comprendre la menace, de manager des équipes opérationnelles, de les conduire sur les opérations tecnhiques en situation de crise et de les conduire à capitaliser sur leurs expériences.

PRÉREQUIS

- Etre titulaire d'un BAC+2 ou Bac+3 Informatique : BTS CIEL ou SIO, BUT ⅔ (R&T, INFO,...) Licence générale ou professionnelle, ou titre RNCP de niveau 5)
- Satisfaire au process de recrutement

DÉBOUCHÉS

Métiers

- Ingénieur en sécurité opérationnelle, expert des SOC, il conçoit, applique et maintient les mesures et contre-mesures de sécurité en contextes défensif et offensif. Référent en analyse de sécurité (vulnérabilités, forensic, détection d'intrusions), il pilote la remédiation, la CTI et la modélisation des menaces pour l'analyse des risques cyber.
- Ingénieur en conception et innovation de produits et solutions de cybersécurité, conformes aux normes de certification, en soutien à l'innovation et au développement industriel.
- Ingénieur en développement d'application cybersécurité : expert du génie logiciel, il accompagne le process de production de services et applications sécurisés "by design"
-

Poursuite d'études possible en doctorat, Masters spécialisés

FORMATION Niveau 7 / Bac +5

Ingénieur spécialité informatique, réseaux, télécommunications (FIP)

Certification Titre D'ingénieur délivré par l'IMT Atlantique spécialité réseaux et télécommunications

RNCP : 38637 (2027)

★ IMT Atlantique Rennes

3 ans, à partir du Bac + 2

Formation en alternance

Lien vers formation-RNCP

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. La formation est organisée selon 4 grandes thématiques : Informatique, réseaux et télécommunications / Sciences sociales et de gestion / Sciences de l'ingénieur / Projet Personnel et Professionnel, formation à l'international.

PRÉREQUIS

- 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.fe de projet (cyber)
- Architecte ou expert en exploitation informatique
- Ingénieur d'affaires ou avant-vente
- Ingénieur d'études en systèmes d'information
- Ingénieur Réseaux et Télécommunications.

FORMATION Niveau 7 / Bac +5

Ingénieur spécialité cybersécurité

Titre d'ingénieur délivré par CentraleSupélec.

★ CentraleSupélec Rennes

3 ans, à partir du Bac +2

Formation en initiale (ou en alternance la 3ème année).

RNCP : 39502 (2025)

Lien vers formation-RNCP

PRÉSENTATION

Le cursus d'ingénieur de spécialité Cybersécurité de CentraleSupélec forme des experts capables de combiner une expertise scientifique et technique approfondie avec une compréhension globale des enjeux liés à leur domaine. Les élèves apprennent à analyser les problèmes de sécurité, à concevoir des solutions solides et innovantes, et à les appliquer dans des environnements complexes et multidisciplinaires. Ils développent également des compétences en communication, travail en équipe et apprentissage autonome, leur permettant de s'adapter à l'évolution rapide du domaine et de prendre des décisions face à des systèmes de plus en plus complexes.

PRÉREQUIS

Classe préparatoire scientifique aux Grandes Écoles (CPGE).

DÉBOUCHÉS

Métiers

- Ingénieur en sécurité des systèmes d'information
- Analyste de la menace et des risques
- Consultant en cybersécurité
- Responsable de la sécurité des systèmes d'information (RSSI)
- Expert en tests d'intrusion et audit de sécurité.

FORMATION Niveau 7 / Bac +5

Ingénieur spécialité informatique

Titre D'ingénieur délivré par l'École Supérieure d'Ingénieurs de Rennes.

★ ESIR Université de Rennes

3 ans, à partir du Bac + 2

Formation initiale

RNCP : 39292 (2027)

Lien vers formation-RNCP

PRÉSENTATION

La formation d'ingénieur spécialité informatique vise à former des ingénieurs avec les compétences nécessaires à l'audit, à la conception, au développement, à la maintenance, et à l'évaluation de systèmes logiciels complexes. Les trois derniers semestres de formation sont organisés en trois options, dont 2 options en lien avec la cybersécurité : Systèmes d'Information (SI), qui a pour mission de former des ingénieurs de haut niveau dans le domaine des technologies innovantes de l'informatique ; et IoT, sécurité et ville intelligente (IoT), qui forme des ingénieurs ayant une forte appétence dans les Sciences et technologies de l'information et de la communication (STIC).

PRÉREQUIS

Cycle préparatoire ESIR
BUT ou Licence 2/3 scientifique

DÉBOUCHÉS

Métiers

- Ingénieur R&D
- Ingénieur expert
- Ingénieur conseil
- Administrateur.trice de Systèmes Informatiques
- Chef.fe de Projet.

Poursuite d'études possible en doctorat.

FORMATION Niveau 7 / Bac +5

Ingénieur généraliste thématique d'approfondissement cybersécurité

Certification Titre D'ingénieur délivré par l'IMT Atlantique.

★ IMT Atlantique Rennes

3 ans, à partir du bac +2

Formation en initiale. Cours en cybersécurité en 2ème et 3ème année.

RNCP : 38322 (2027)

Lien vers formation-RNCP

PRÉSENTATION

La thématique d'approfondissement « cybersécurité » forme des ingénieurs en sécurité applicable tant en technologies de l'information que dans les technologies industrielles. En réponse aux problématiques de sécurité, les étudiants développent des compétences en cyber protection et en cyberdéfense et sont dotés d'un bagage scientifique et technique solide, nécessaire aux besoins du marché de la filière cybersécurité. Outre ces compétences fondamentales, les nouveaux usages en termes de communication et de traitement de l'information sont également pris en compte dans les formations cybersécurité (ex. cloud computing, IoT, bigdata, systèmes industriels).

PRÉREQUIS

- Une Classe Préparatoires aux Grandes Écoles pour un cursus de 3 ans
- Une licence scientifique (L3) pour une entrée en 1ère ou 2ème année selon votre diplôme universitaire
- Un master scientifique (M1) pour une entrée en 1ère ou 2ème année selon votre diplôme universitaire

DÉBOUCHÉS

Métiers

- Architecte sécurité
- Développeur.se de sécurité
- Évaluateur.trice ou Auditeur.trice (produit, logiciel, matériel) de sécurité
- Intégrateur.trice
- Consultant.e
- Opérateur.trice
- Responsable de la Sécurité des Système d'information (RSSI)
- Formateur.trice ou Instructeur.trice

FORMATION Niveau 7 / Bac +5

Ingénieur Informatique, option sécurité

Titre D'ingénieur délivré par l'Institut National des Sciences Appliquées de Rennes, spécialité informatique

★ INSA Rennes

3 ans, à partir du Bac + 2

Formation initiale

RNCP : 38637 (2025)

Lien vers formation-RNCP

PRÉSENTATION

La formation s'articule autour d'un socle commun, axé sur la conception et la réalisation de logiciels, et d'options permettant d'acquérir des compétences complémentaires. L'option Sécurité est consacrée à la sécurité des systèmes informatiques et électroniques. Elle a pour objectif de sensibiliser les étudiants aux problèmes de protection de l'information, des dispositifs physiques et des implémentations logicielles. Les thématiques portent aussi bien sur la construction de mécanismes de sécurité (cryptologie, programmation sécurisée, sécurité des réseaux, confiance, détection d'intrusions) que sur la conception de nouvelles méthodes d'attaque.

PRÉREQUIS

1er cycle de l'INSA
Bac +2 (Licence 2, CPGE) ou Bac + 3 (Licence 3)
D'un Bac +4 (master 1 ou équivalent) pour l'entrée en 4ème année

DÉBOUCHÉS

Métiers

- Chef.fe de projet (cyber)
- Ingénieur d'affaires
- Consultant.e cyber
- Ingénieur R&D
- DevOps
- Chargé.e du développement logiciel et de l'administration des systèmes informatiques.

FORMATION Niveau 7 / Bac +5

Ingénieur Informatique

Titre Ingénieur diplômé EPITA, reconnu par la CTI

★ EPITA - Rennes

5 ans après le bac (2 ans de cycle préparatoire + 3 ans de cycle ingénieur)

Formation initiale

RNCP N°40531 (échéance d'enregistrement : 31/08/2028)

Site internet de https://www.epita.fr/

PRÉSENTATION

Fondée en 1984, l'EPITA est une École d'ingénieurs en informatique et en numérique, leader dans son domaine. Elle forme des étudiantes et étudiants dans 8 domaines technologiques tels que l'intelligence artificielle et la cybersécurité. Dans sa démarche d'innovation permanente, l'École poursuit une approche pédagogique inédite et associe avec excellence enseignement et recherche. L'EPITA se déploie sur sept campus en France avec ses équipes de recherche et d'innovation pour apporter des réponses innovantes et concrètes aux grands défis technologiques, industriels, économiques et sociétaux.

PRÉREQUIS

Bac général : mathématiques obligatoires, avec une spécialité scientifique.
Après une CPGE : intégration dans le cycle ingénieur
Admissions parallèles : intégration possible à partir de Bac+1 (BTS, BUT, Licence ou équivalent), en informatique ou domaine proche.

DÉBOUCHÉS

Métiers visés

- Ingénieur logiciel
- Développeur full stack,
- Ingénieur systèmes,
- Ingénieur réseaux, ingénieur cloud,
- DevOps,
- Ingénieur cybersécurité,
- Analyste SOC
- Pentester
- SecDevOps
- Ingénieur data,
- Data engineer,
- Architecte SI
- Ingénieur IA
- Chef.fe de projet technique
- Consultant.e IT
- Ingénieur embarqué

Poursuite d'études possible: Doubles diplômes, parcours recherche, doctorat (R&D)

FORMATION Niveau 7 / Bac +5

Expert en Sécurité Digitale

Titre Professionnel de niveau 7 enregistré au RNCP par l'ENI - Ecole Informatique Administrateur systèmes et réseaux

★ ENI Rennes

Formation en 2 ans après Bac +2 ou en 1 an après Bac+3

Formation en alternance

RNCP : 35 587 (2026)

Lien vers formation-RNCP

PRÉSENTATION

La formation *Expert en Sécurité Digitale* vise à former des professionnels de haut niveau capables de protéger, auditer et sécuriser les systèmes d'information des organisations face aux menaces numériques actuelles. Elle couvre des domaines avancés tels que la gestion des risques, la cryptographie, la sécurité des réseaux, la protection des données, la réponse aux incidents et l'audit de systèmes. Au terme de la formation, vous serez en mesure de concevoir des politiques de sécurité, déployer des mesures de défense efficaces et piloter la sécurité organisationnelle dans des environnements complexes.

PRÉREQUIS

Cette formation s'adresse aux personnes titulaires d'un diplôme de niveau 6 (Bac +4) en informatique, idéalement avec des compétences en administration systèmes et réseaux. La sélection se fait sur dossier, test de connaissances et entretien professionnel.

Ou informaticien expérimenté.

DÉBOUCHÉS

Métiers

- Expert.e en sécurité digitale
- Consultant.e en sécurité des systèmes d'information
- Auditeur.trice en cybersécurité
- Assistant.e RSSI
- Risk Manager (junior)
- Administrateur.trice systèmes, réseaux et sécurité

FORMATION Niveau 7 / Bac +5

Mastère Cybersécurité

Expert en architectures sécurisées des systèmes d'information Titre RNCP niveau 7 délivré par ASSOCIATION SUP DE VINCI

Formation labellisée SecNumedu délivrée par l'ANSSI

RNCP 40165

★ Sup De Vinci Rennes

2 ans à partir du Bac +3

Formation en alternance et alternance progressive/initiale

RNCP40165 - Expert en architectures sécurisées des systèmes d'information

PRÉSENTATION

Avec de plus en plus de données à défendre (donc plus de risques), des attaques qui se perfectionnent (donc plus de risques aussi), le développement de la sécurité informatique à tous les niveaux des cycles de vie, l'IA pour optimiser les réponses, les process face aux cyberattaques qui se développent et industrialisent, le DevSecOps qui apparaît en réponse face à un renforcement de la sécurité informatique, ... notre certification a pour objectif de permettre une employabilité durable sur le marché du travail avec des compétences attestées relatives aux besoins actuels et à venir en termes d'architectures sécurisées des systèmes d'information.

En te formant à la cybersécurité chez **Sup de Vinci,** tu développes des compétences techniques immédiatement applicables en entreprise, recherchées par tous les acteurs du marché. Tu apprends à anticiper, détecter et contrer les cybermenaces qui touchent aussi bien les TPE que les grands groupes, grâce à une pédagogie orientée terrain et à l'alternance.
Encadré par des experts et équipé d'outils et méthodes cyber, tu gagnes en autonomie et en confiance. C'est l'opportunité d'allier ta curiosité à un métier d'impact, au cœur d'un secteur qui ne cesse d'évoluer.

PRÉREQUIS

Etre titulaire d'un Bac +3 validé (niveau 6) en informatique

DÉBOUCHÉS

Métiers

- Responsable Sécurité des SI
- Consultant.e en cybersécurité
- Chef.fe de projet en sécurité informatique
- Analyste SOC (security operation center),
- Ingénieur réseaux,
- Pentester

FORMATION Niveau 7 / Bac +5

MBA Data, Protection & Sécurité

Certification délivrée

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

★ EPITECH Rennes

2/3 ans, à partir du Bac +2/3

Formation initiale - alternance

RNCP : 35284 (2026)

Lien vers formation-RNCP

PRÉSENTATION

Les titulaires d'un Bac +2/3, avec une bonne compréhension des fondamentaux du développement Web, de l'expérience digitale et/ou en gestion de projet, peuvent rejoindre les MBA d'Epitech. Ces parcours s'effectuent en alternance jusqu'au Bac +5 (RNCP de niveau 7), Les apprenants peuvent choisir une spécialisation Data, Protection & Sécurité. Les objectifs sont de former des experts en matière de protection et de sécurité des données, avec des connaissances approfondies sur les technologies de sécurité des données, en gestion de projet, en gestion des risques ou encore gestion de la conformité. Côté cyber sont au programme : Sécurité des SI, Risk Management, Bases de données et protection des données, Data Science & Cybersécurité, Cryptologie et code, Hébergement & Sécurité…

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

- Consultant.e RGPD
- Expert.e en Protection des Données Personnelles
- Chef.fe de projet cybersécurité
- Formateur.trice Cybersécurité
- Consultant.e Sécurité
- Spécialiste en gestion de crise cyber
- Data Protection Officer
- Communicant.e de Crise…

Poursuite d'étude possible en doctorat ou autre Master qui serait complémentaire.

Epitech Rennes - MBA Data, Protection & Sécurité

FORMATION Niveau 7 / Bac +5

Bac +5 - 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

CFA De La Salle - Rennes

2 ans à partir du Bac +3

Formation en alternance :
Contrat d'apprentissage ou contrat de professionnalisation

RNCP : 36296

Lien vers le titre RNCP

CFA DE LA SALLE - BAC +5 -

Expert en architectures systèmes-réseaux et en sécurité informatique

PRÉSENTATION

L'expert en architecture 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, 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 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) : Titre de niveau 6 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.trice des services informatiques (après expérience)
- RSSI (Responsable Sécurité du Système d'Information),
- Auditeur.trice…

FORMATION Niveau 7 / Bac +5

Mastère Spécialisé Cybersécurité

Certification délivrée par Centrale Supélec et IMT Atlantique + certification ISO27007 Lead Auditor.

La formation bénéficie du Label SecNumedu délivré par l'ANSSI.

★ CentraleSupélec / IMT Atlantique

1 an, à partir du Bac +4/+5

Formation initiale ou continue

RNCP : 39837(2027)

Lien vers formation-RNCP

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
- Développeur.se Sécurité
- Architecte Sécurité
- Intégrateur.trice Sécurité
- Analyste SOC
- Consultant.e sécurité organisationnelle
- Consultant.e sécurité technique
- Évaluateur.trice de produit de sécurité

FORMATION Niveau 7 / Bac +5

Expert en Technologie de l'Information Programme Grande Ecole

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) / NOR : ESRS2334763A

★ EPITECH Rennes

5 ans , à partir du Bac

Formation initiale

Lien vers le bulletin officiel MESR

Lien vers formation-RNCP

Epitech Rennes - Programme Grande École

PRÉSENTATION

Le Programme Grande École, accessible post-bac, se déroule en 5 ans et forme des experts en informatique (Bac +5). 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 suivent des modules techniques (Cryptographie, Web Security, Reverse engineering…).

PRÉREQUIS

Baccalauréat toutes filières

DÉBOUCHÉS

Métiers

- Développeur.se Informatique
- Ingénieur Logiciel,
- Expert.e/Consultant.e Technique
- Chef.fe de Projet MOA/MOE
- Ingénieur de recherche
- CTO
- Directeur.trice Technique
- Data Scientist
- Architecte Informatique
- Data Analyst
- Auditeur.trice Cybersécurité,
- Administrateur.trice Sécurité
- Développeur.se IoT
- Pentester
- Responsable Systèmes et Réseaux
- Devops
- Chef.fe de Projet Informatique
- Analyste en IA
- Architecte de Solutions…

Poursuite d'étude possible en doctorat ou autre Master.

FORMATION Niveau 7 / Bac +5

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 25/06/2025 Label SecNumEdu de l'ANSSI pour le programme d'Expert en Cybersécurité (obtenu à Paris, Toulouse et Bordeaux, dossier en cours à Rennes).

★ Rennes YNOV Campus

Parcours en 2 ans

Formation initiale - alternance

RNCP : 40897 (2028)

Lien vers formation-RNCP

PRÉSENTATION

Ce mastère fera de vous un expert qui façonnera le futur de la sécurité numérique des entreprises. Ceux qui peuvent lire entre les lignes de code, anticiper et détecter les menaces, 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.e en cybersécurité,
- Auditeur.trice sécurité des systèmes d'informations,
- Architecte sécurité des systèmes d'information,
- Expert.e en sécurité des systèmes d'information
- Spécialiste en cybersécurité
- Analyste SOC Security Operations Center
- Pentester
- Chef.fe de projet en sécurité des systèmes d'information.

FORMATION Niveau 7 / Bac +5

Master of Science Cybersécurité

Certification délivrée

Titre Architecte de Systèmes d'Information

★ EPITECH Rennes

2/3 ans, à partir du Bac +2/3

Formation initiale - alternance

RNCP : 38114 (2026)

Lien vers formation-RNCP

PRÉSENTATION

Les titulaires d'un Bac +2/3, avec une appétence prouvée dans l'informatique et le développement, peuvent rejoindre les Masters of Science d'Epitech. Ces parcours s'effectuent en alternance jusqu'au Bac +5 (RNCP de niveau 7), Les apprenants ont la possibilité de choisir une spécialisation en cybersécurité. Les objectifs de cette spécialité sont de leurs 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

- Responsable Sécurité des Systèmes d'Information
- Auditeur.trice Cybersécurité
- Pentester
- Administrateur.trice Sécurité,
- Consultant.e Sécurité Informatique,
- Analyste en Cybersécurité,
- Ingénieur en Sécurité Réseau,
- Analyste en gestion des risques…

Poursuite d'étude possible en doctorat ou autre Master qui serait complémentaire.

Epitech Rennes - Master of Science Cybersécurité

FORMATION Niveau 7 / Bac +5

Master Sécurité Informatique Cybersécurité et Cybermenaces

Diplôme national de l'enseignement supérieur délivré par le Conservatoire National des Arts et Métiers (CNAM) - spécialité Informatique

« Master Informatique »

RNCP : 39278 (2029)

★ ESNA Rennes en partenariat avec le Cnam Bretagne

Formation en alternance 2 ans

Accessible également en formation 100% à distance avec Cnam Bretagne

Lien vers formation-RNCP

Lien vers formation Master-Esna

Lien vers Master Cnam Bretagne

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 (licence informatique ou BUT 3)
- Satisfaire au process de recrutement

DÉBOUCHÉS

Métiers : ce Master débouche sur l'ensemble des métiers de la sécurité informatique tels qu'ils sont définis dans le panorama des métiers de la cybersécurité et de l'ANSSI :

- Métiers de la Gestion de la sécurité et pilotage de projets de sécurité. : RSSI, SSI, Directeur/coordinateur cybersécurité, ..
- Métiers de la conception et du maintien d'un SI Sécurisé : Architectes sécurité, Auditeur/pentesteur
- Métiers de la gestion des incidents et des crises de sécurité : SOC, SIEM, Analyste forensic, Gestionnaire de crise

**Formation également proposée par le CNAM à distance*

Poursuite d'études possible en doctorat.

FORMATION Niveau 7 / Bac +5

MBA Cybersécurité et Architecture Réseau

Titre professionnel « Expert en Etudes et Développement du Système d'Information » de Niveau 7 enregistré au RNCP délivré par le ministère du travail

★ My Digital School

Formation sur 2 ans à partir du Bac +3

Formation initiale ou en alternance

RNCP N° 40363 (2028)

Lien vers formation-RNCP

My Digital School - MBA Cybersécurité et Architecture Réseau

PRÉSENTATION

Le MBA en Cybersécurité et architecture réseaux, de MyDigitalSchool, forme les futurs experts de la cybersécurité. Les étudiants entament une plongée plus ciblée dans le monde de la **cybersécurité** et de l'architecture de réseaux.

La formation MBA en architecture réseau permet de développer une expertise avancée dans la conception, la gestion et l'optimisation des infrastructures réseau d'entreprises, préparant ainsi les étudiants à des postes de direction stratégique dans le domaine des technologies de l'information.

Les objectifs professionnels sont orientés vers la création et le maintien d'infrastructures réseau fiables, performantes et sécurisées.

PRÉREQUIS

Être titulaire d'un Bac+3, titre de niveau 6 OU 180 crédits ECTS dans le domaine de l'informatique Système et Réseau

DÉBOUCHÉS

Métiers

- Responsable infrastructure systèmes et réseaux,Responsable de la sécurité des systèmes d'information (RSSI)
- Architecte en sécurité réseaux
- Expert.e en système & infrastructures cloud,
- Directeur.trice des systèmes d'information (DSI),
- Chief technical officer (CTO),
- Analyste SOC (Secutity Operations Center)

FORMATION Niveau 7 / Bac +3/5

Parcours Cyb3r Xp

Certification délivrée : titre « Expert en Cybersécurité » par Ynov

★ EPSI Rennes

3 ans , à partir du Bac +2

Formation initiale et/ou en alternance

Lien vers formation-RNCP

RNCP : 40897 (2025)

PRÉSENTATION

Dans la formation Cyb3r Xp vous apprendrez à maîtriser les outils clés de la cybersécurité: systèmes, réseaux, audit de sécurité, pentest, SOC, SIEM, et forensic. Vous développerez vos compétences en défense (Blue Team) et en attaque (Red Team) à travers des mises en situations réalistes. Vous serez formés à l'analyse des menaces, à la gestion des incidents et à la réponse aux crises cyber. Un entraînement spécifique vous préparera aux certifications professionnelles Cisco CCNA, CompTIA Security+ et CompTIA CySA+. Vous serez également accompagnés vers la certification Google Cloud Security Engineer, pour allier cybersécurité et maîtrise du cloud.

PRÉREQUIS

Être titulaire d'une certification de niveau 5 ou bac+2 en informatique ou en sécurité de l'informatique ou en droit informatique/ droit en propriété intellectuelle.

DÉBOUCHÉS

Métiers

- Analyste SOC (Security Operations Center)
- Consultant.e Cybersécurité
- Ingénieur.e sécurité systèmes
- Pentester (testeur d'intrusion),
- Responsable sécurité IT
- RSSI (Responsable de la Sécurité des Systèmes d'information)
- Architecte SSI(I)
- Conseiller.ère en SSI(I)

FORMATION Niveau 7 / Bac +5

MSc Expert en Cybersécurité

Certification Titre Expert en cybersécurité, délivrée par YNOV

★ EPSI Rennes

2 ans , à partir du Bac +2 ou 3

Formation en alternance

Lien vers formation-RNCP

RNCP : 40897 (2025)

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

AUTRES FORMATIONS

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 est 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.

Micro-certifications

Le projet CyberSkills4All va déployer des micro-certifications en cybersécurité accessibles à toutes et tous sur la plateforme FUN, renforçant la formation initiale et continue pour soutenir la souveraineté numérique française.

Dix partenaires se sont regroupés autour de ce projet : Université de Rennes, Université Bretagne Sud (UBS), Pôle d'excellence cyber (PEC), France Université Numérique (FUN), Orange, École nationale supérieure de techniques avancées (ENSTA), Institut National Polytechnique de Bretagne (Bretagne INP), Rennes School of Business (RSB), GIP-FAR, et le CMQe Numérique, Photonique et Cybersécurité de Bretagne.

Cette alliance illustre la capacité de la Bretagne à fédérer universités, écoles et entreprises autour de l'excellence en cybersécurité.

La cybersécurité s'invite sur FUN avec CyberSkills4All dès 2026 - France Université Numérique

PENSEZ EGALEMENT A LA VAE : Validation des Acquis de l'Expérience

La Validation des Acquis de l'Expérience (VAE) offre une 3ème voie d'accès à la certification en France, équivalente à la formation initiale, continue ou en alternance. France VAE

AUTRES FORMATIONS

FORMATIONS PRÉ-QUALIFIANTES aux métiers du numérique - Région Bretagne

Vous avez besoin d'acquérir les bases dans le domaine du numérique, la Région Bretagne propose des formations pré-qualifiantes dans le domaine du numérique.

Construire et sécuriser son parcours d'accès à la formation et à l'emploi vers les métiers du numérique

- Explorer la diversité du secteur et des métiers du numérique
- S'initier aux gestes professionnels de différents métiers du numérique
- Découvrir les opportunités d'emploi sur son territoire et la variété des environnements de travail
- Identifier les offres de formations qualifiantes du niveau 5 au niveau 3 et leurs conditions d'accès
- Formaliser son projet et son plan d'action

https://ideo.bretagne.bzh/formations/pre-qualification-aux-metiers-du-numerique-1

La Région propose et finance chaque année en Bretagne, plus de 22 000 parcours de formation.

Adaptée à chaque situation, l'offre de formation se décline en deux gammes : PRÉPA, pour concrétiser son projet professionnel, et QUALIF pour monter en compétences dans les secteurs d'emploi en Bretagne (agriculture, mer, numérique, industrie, sanitaire et social…).

Vous accompagner vers l'emploi · Région

Numéric'Emploi

Dans le cadre d'une convention signée avec la Branche Bureaux d'Etudes Techniques,l'OPCO Atlas intensifie le déploiement du dispositif Numéric'Emploi sur le territoire national en mobilisant l'ensemble des acteurs de l'emploi et de la formation professionnelle.

4 Piliers : Attractivité, Accompagnement, Formation Recrutement
Numéric'emploi : faciliter le recrutement dans les métiers du numérique | Opco At

Vous souhaitez en savoir plus sur le dispositif en Bretagne et bénéficier d'un accompagnement, contacter Bleuenn JAGAIN : bjagain@opco-atlas.fr

RECONVERSION - TRANSITION PROFESSIONNELLE...

RECONVERSION EN CYBERSÉCURITÉ - Syndicat Initiative Cyber Rennes Métropole

Rennes Métropole, We-Ker et la CyberSchool de Rennes s'associent au sein du Syndicat d'Initiative en Cybersécurité (SIC) pour promouvoir et accompagner la reconversion en cybersécurité sur le territoire.

L'initiative vise à aider les personnes intéressées à se reconvertir avec succès dans ce domaine à la fois complexe mais aussi en constante évolution et qui offre de réelles perspectives d'avenir.

- Nous offrons un accompagnement pour trouver le métier vers lequel vous souhaitez évoluer.
- Nous fournissons toutes les informations pratiques (panorama des métiers, liste des formations, liste et contact des entreprises qui recrutent ...).

Si vous êtes intéressés par une carrière en cybersécurité et que vous avez des questions, contactez-nous par mail pour échanger sur votre projet et ainsi réussir votre transition. Reconversion en cybersécurité - CyberSchool

stephane.szymanski@univ-rennes.fr

Vous êtes salariés, vous avez un projet de transition ou de reconversion professionnelle, vous pouvez bénéficier d'un accompagnement : Avenir Actifs

RECHERCHER UN STAGE - UNE ALTERNANCE

IDEO Région Bretagne - stage élèves 3ème et 2nde : https://stages.ideo.bretagne.bzh/partners

IMMERSION FACILITÉE France Travail : Immersion Facilitée

1 jeune - 1 solution : https://www.1jeune1solution.gouv.fr/apprentissage

Bretagne Alternance: https://www.bretagne-alternance.com/

OPCO Atlas : Atlas de l'Alternance 2022 en Bretagne

SE FORMER

OPCO Atlas : boîte à outils : https://www.opco-atlas.fr/boite-outils.html

Penser à mobiliser votre CPF Inscription / connexion | Mon compte formation

LISTE DES ÉTABLISSEMENTS

AFPA	Afpa
AFTEC	aftec
CENTRAL SUPELEC Rennes *	Campus de Rennes | CentraleSupélec
Chambre des métiers	CMA Bretagne
CNAM Bretagne	Cnam Bretagne
CyberSchool	CyberSchool
ECE (Omnes Education)	ECE
ENI	ENI École Informatique
EPITA	Ecole d'ingénieurs informatique à Rennes - Le campus de l'EPITA
EPITECH	Epitech
EPSI	EPSI
ESIR*	ESIR
ESNA	ESNA
GRETA	GRETA
Groupe St Jean (Pôle Sup De La Salle)	Groupe Saint Jean
IMT Atlantique*	IMT Atlantique
INSA Rennes*	insa-rennes.fr
IUT de St Malo*	iut-stmalo.univ-rennes.fr
Lycée Brequigny	Lycée Brequigny
Lycée Charles Tillon	Lycée Charles Tillon
Lycée Coëtlogon	lycee-coetlogon.ac-rennes.fr
Lycée Hélène Bach	Lycée Victor et Hélène Basch
MyDigital School	Ecole multimédia Rennes - MyDigitalSchool
SIMPLON	simplon.co
Sup De Vinci	Sup de Vinci
Université de Rennes*	Université de Rennes
YNOV	Ynov
WIS	WIS

**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 formation,
- Acteurs de l'emploi
- Employeurs privés et publics

Il s'inscrit dans le cadre de la démarche GPEC-T (Gestion Prévisionnelle des Emplois et Compétences territoriale).
Démarche pilotée par l'association We Ker qui bénéficie dans ce cadre d'un financement de l'Etat, de la Région Bretagne, de Rennes Métropole et du soutien de l'Union Européenne.

Ce document constitue une photographie des formations en cybersécurité proposées en présentiel sur le territoire de Rennes Métropole en 2025. 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,
Si vous n'avez pas trouvé de réponses à vos questions dans ce catalogue
Contacter : rdiverres@we-ker.org

NOTES

NOTES

https://www.entreprendre-rennes.fr/article/cybersecurite/

Catalogue accessible sur le site de Rennes Demain en scannant le QR code