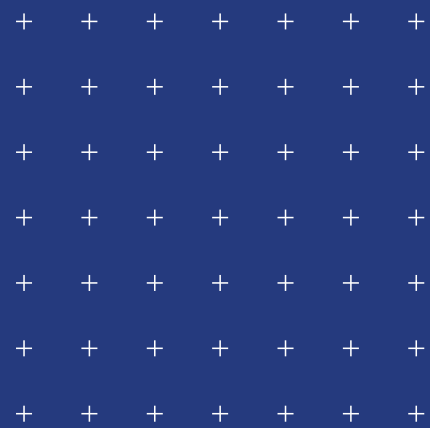


GROUPE  
**INSA**

| CONSCIENCE  
COLLECTIVE



ADMISSIONS 2024

**INGÉNIEUR·E  
ET TELLEMENT +**

**FORMATION EN  
CYBERSÉCURITÉ**



## LES ENJEUX DE LA CYBERSÉCURITÉ

L'usage de l'informatique et des réseaux est devenu incontournable dans notre environnement de travail et dans notre cadre familial.

Cette évolution n'est toutefois pas sans risque car l'omniprésence de l'informatique et son usage dans des applications critiques en font une cible de choix.

Si l'existence d'attaques informatiques n'est pas récente, ce phénomène a pris beaucoup d'ampleur ces dernières années avec le développement de la cybercriminalité, parfois organisée en groupes mafieux, et l'apparition d'attaques étatiques.

Par ailleurs, la menace évolue et cible non seulement les systèmes informatiques classiques mais aussi les objets connectés et les systèmes industriels critiques. Il est urgent de lutter contre ce fléau et de développer la filière de la cybersécurité.

Cela nécessite de former des ingénieurs qui deviendront experts en cybersécurité et de sensibiliser au domaine ceux qui ne feront pas de la cybersécurité leur spécialité.

Le Groupe INSA est un acteur de la transformation numérique et des menaces qui l'accompagnent avec notamment cinq INSA (Centre Val de Loire, Hauts-de-France, Lyon, Rennes et Toulouse) qui proposent aujourd'hui des formations pointues dans le domaine de la cybersécurité.

## CYBERSÉCURITÉ MADE IN INSA

Se former à l'INSA en cybersécurité, c'est acquérir des compétences d'experts bâties sur un cursus théorique et opérationnel et qui permettront de progresser au fil des avancées des connaissances et des technologies.

Se former à l'INSA en cybersécurité, c'est aussi bénéficier d'un environnement de recherche exceptionnel avec des enseignants-chercheurs internationalement reconnus dans les domaines de la sécurité des systèmes et des réseaux, de la cryptographie, de la protection des données personnelles, des méthodes formelles pour la sécurité ou encore de la sécurité des systèmes matériels.

Se former à l'INSA en cybersécurité, c'est également s'offrir un large spectre d'opportunités professionnelles en entreprises, dans les ministères ou agences étatiques ou bien encore dans les organismes nationaux de recherche ou les établissements d'enseignement supérieur et de recherche.

*Bertrand RAQUET,  
Président du Groupe INSA*

# INSA CENTRE VAL DE LOIRE

## DÉPARTEMENT CONCERNÉ

La cybersécurité est au cœur du département STI (Sécurité et Technologies Informatique).

## THÉMATIQUES

Sécurité système, sécurité réseau, sécurité embarquée, développement sécurisé, cryptographie, gestion de crise, sécurité des données et vie privée (RGPD), anonymisation, analyse d'impact sur la vie privée, DevOps, SOC et tests d'intrusion.

## CURSUS

Cette formation, sous statut étudiant ou apprenti, délivre, dès la deuxième année de prépa-intégrée via la pré-spécialisation STI, des enseignements en sécurité tels que sécurité système, sécurité Windows, sécurité réseau, cryptographie ou protection et anonymisation de données. Les étudiants ont la possibilité de choisir en dernière année l'une des trois options suivantes :

- 4AS (Architecture, Administration, Audit et Analyse de Sécurité) ;
- ASL (Architecture et Sécurité Logicielles) ;
- 2SU (Sécurité des Systèmes Ubiquitaires).

En plus des modules théoriques ou techniques en informatique, les étudiants suivent, a minima, 12 modules d'enseignement, soit environ 300h, entièrement dédiés à la cybersécurité et réalisent trois projets orientés sécurité sur une durée de plus de 10 mois au total.

Un module d'Ouverture Scientifique et Technique en 4<sup>e</sup> année permet de plus d'initier les étudiants à la recherche en cybersécurité. Ainsi, de 60 à 70 étudiants de 5<sup>e</sup> année effectuent un stage en entreprise sur une thématique cybersécurité avant d'être diplômés.

La formation est labellisée SecNumEdu de l'ANSSI depuis novembre 2022.



## ÉCOSYSTÈME

Tous les enseignants-chercheurs en informatique du département STI sont des chercheurs en cybersécurité. Cette expertise est renforcée par des professionnels issus d'agences gouvernementales comme l'ANSSI, mais aussi de multiples grands groupes privés tels que Airbus Defence and Space, Amazon, Wavestone, EY, Worldline et Redhat.

De plus, les étudiants participent régulièrement à des challenges ou à des événements liés à la cybersécurité tels que HackTheBox ou le challenge sécurité embarqué CSAW. Ils s'y sont classés plusieurs fois dans le top 5 mondial.

## RECHERCHE

Tous les enseignants-chercheurs en informatique de l'INSA CVL campus Bourges appartiennent à l'équipe Sécurité des Données et Système du Laboratoire d'Informatique Fondamentale d'Orléans. Ils se spécialisent en particulier dans le contrôle d'accès, l'authenticité et la traçabilité des données, les techniques de protection de la vie privée et l'utilisation de méthodes formelles pour la sécurité et la cryptographie.

# INSA HAUTS-DE-FRANCE

## DÉPARTEMENT CONCERNÉ

La cybersécurité est enseignée dans le département informatique.

## THÉMATIQUES

Cryptographie, sécurité des systèmes et des réseaux, sécurité des objets connectés, du cloud et des applications, sécurité offensive, défensive et périmétrique, gouvernance, normes et réglementation.

## CURSUS

Dès la première année de la spécialité ingénieur « informatique et cybersécurité », un solide socle technique et scientifique en informatique est développé, ainsi que la sécurité informatique et la protection des données (p. ex. sensibilisation au RGPD).

Un projet innovation et créativité confronte les étudiants aux problématiques d'autres domaines de l'ingénierie. La cryptographie avancée, les modèles de sécurité ou encore la sécurité de système et programmation sécurisée sont ensuite traités.

En dernière année de spécialité, l'axe cybersécurité forme aux différents contextes de mise en œuvre de la sécurité (cloud, Internet des objets), aux méthodes et outils pour la garantir (sécurité prédictive et proactive), ainsi qu'aux aspects réglementaires.

L'axe systèmes d'information permet des approfondissements en développement mobile, en intelligence artificielle et en conception d'applications complexes. Les cours électifs offrent une ouverture vers d'autres domaines scientifiques.

À terme, cette spécialité accueillera des promotions de 50 étudiants.

## ÉCOSYSTÈME

Près d'un tiers des enseignements de spécialité sont assurés par des intervenants extérieurs, employés de sociétés partenaires ou d'organisations étatiques.

Les deux stages obligatoires intégrés dans le cycle ingénieur aident l'élève à définir son projet professionnel, à acquérir une connaissance du monde industriel et à mettre en œuvre ses compétences techniques.

Un semestre académique à l'étranger est obligatoire durant la scolarité. Il est possible de le suivre dans l'une de nos universités partenaires (Allemagne, Brésil, Canada, Chine, Espagne, Pologne, Grande-Bretagne, Maroc, Italie, Norvège, Pays-Bas, Roumanie, Suède, etc.) et de préparer un double diplôme en passant 18 mois à l'étranger avec une durée supplémentaire de 6 mois par rapport au cursus initial.

## RECHERCHE

Les enseignants-chercheurs qui interviennent dans cette spécialité exercent leurs activités de recherche au sein du Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines (LAMIH). Le LAMIH est une unité mixte de recherche entre l'Université Polytechnique Hauts-de-France (UPHF) et le Centre National de la Recherche Scientifique (CNRS).

# INSA LYON

## DÉPARTEMENTS CONCERNÉS

Les étudiants ont la possibilité d'étudier la sécurité dans le cadre de parcours des formations ingénieur en Télécommunications et ingénieur en Informatique, ainsi que dans le cadre associatif.

## THÉMATIQUES

Cryptographie, sécurité des systèmes, sécurité des infrastructures, protection des données personnelles, gestion de crise.

## CURSUS

Les formations des départements « Informatique » et « Télécommunications » proposent des enseignements en cryptographie, en sécurité des systèmes, en sécurité des infrastructures, en protection des données personnelles et en gestion de crise. L'enseignement de la cybersécurité est réalisé en tronc commun puis les départements « Informatique » et « Télécommunications » proposent chacun un parcours cybersécurité (en 4<sup>e</sup> et 5<sup>e</sup> année en Informatique, et en dernière année en Télécommunications). À la fin de ces parcours, les étudiants sont par exemple capables d'écrire un article sur un événement récent lié à la sécurité, de comprendre le fonctionnement des malwares, d'analyser et déployer une infrastructure de sécurité, ou encore d'effectuer une étude d'impact sur la vie privée d'un système.

Les étudiants participent régulièrement à des événements liés à la cybersécurité tel qu'un challenge d'anonymisation de données ou un exercice de gestion de crise.

Par ailleurs, une association étudiante regroupant des étudiants de différents départements et de toutes les années dès l'admission post-bac, et en liaison avec l'équipe enseignante, organise des réunions hebdomadaires et offre un cadre à ses membres pour qu'ils approfondissent des sujets extrêmement pointus, participent à des compétitions de sécurité et organisent annuellement une conférence et un concours de sécurité dans nos locaux.

## ÉCOSYSTÈME

La formation en cybersécurité de l'INSA Lyon bénéficie d'un riche écosystème composé de grandes entreprises (Orange Cyberdefense, etc.) mais aussi de PME (AlgoSecure, Advens, etc.). On retrouve des anciens élèves dans des acteurs majeurs du domaine : OVH, Synaktiv, Tenable, etc.

De plus, les chercheurs en cybersécurité de l'INSA Lyon sont impliqués dans la structuration et le pilotage de la recherche en sécurité au CNRS et à l'Inria. Ils entretiennent également des liens forts avec la CNIL dans le cadre de la protection des données personnelles.

## RECHERCHE

Les enseignements en cybersécurité à l'INSA Lyon sont donnés par des enseignants-chercheurs des laboratoires de recherche CITI et LIRIS. Ces enseignants-chercheurs sont membres d'équipes adressant les problématiques de la sécurité des systèmes distribués, de la gestion sécurisée de données ou de la protection des données personnelles.

# INSA RENNES

## DÉPARTEMENTS CONCERNÉS

La cybersécurité est essentiellement présente dans le département d'informatique mais il existe également des enseignements qui sont dispensés dans les départements Électronique et Informatique Industrielle (EII) et Électronique et Télécommunications (E&T).

## THÉMATIQUES

Vulnérabilités logicielles, cryptographie, sécurité des réseaux, programmation sécurisée, sécurité à l'interface matérielle/logicielle, sécurité des protocoles de communication, hygiène informatique, sécurité des données multimédias, interceptions matérielles en air libre.

## CURSUS

Le département d'informatique permet aux étudiants de se spécialiser en cybersécurité dès la 3<sup>e</sup> année à travers une « option », c'est à dire une coloration de leur programme qui consiste en 8 unités d'enseignement réparties de la 3<sup>e</sup> à la 5<sup>e</sup> année.

Cette option est complétée par des projets et stages en cybersécurité mais aussi par des enseignements de tronc commun en lien avec la cybersécurité, comme l'hygiène informatique, les réseaux, l'apprentissage automatique, les statistiques, etc.

## ÉCOSYSTÈME

La formation en cybersécurité à l'INSA Rennes bénéficie des compétences du riche écosystème local constitué d'industriels, mais aussi de l'ANSSI, du ministère des Armées, et des chercheurs du CNRS. Les étudiants bénéficient également de la présence sur le campus rennais de la Cyberschool (École Universitaire de Recherche) dont l'INSA Rennes est partenaire et qui permettra prochainement aux étudiants de l'INSA de bénéficier d'un double diplôme ingénieur-master spécialisé en cybersécurité.

Parmi les acteurs majeurs de l'écosystème rennais, on compte de nombreuses entités du ministère des Armées, notamment la DGA-MI, mais aussi des grandes entreprises (Orange Cyberdefense, Thales, Technicolor, etc.) et des PME spécialisées en cybersécurité (Quarkslab, Amosys, Secure-IC, synaktiv, etc.)

Les enseignants-chercheurs et chercheurs rennais en cybersécurité sont également fortement impliqués dans la structuration et le pilotage de la recherche au niveau national, notamment au travers du CNRS, d'Inria et de l'ANSSI.

Enfin, Rennes héberge depuis une vingtaine d'années la conférence francophone SSTIC, référence incontournable dans le paysage français de la cybersécurité.

## RECHERCHE

Les enseignants-chercheurs de l'INSA Rennes qui participent à l'enseignement de la cybersécurité effectuent leurs travaux de recherche au sein des laboratoires rennais IRISA (informatique, pris au sens large) et IETR (électronique et technologies du numérique).



# INSA TOULOUSE

## DÉPARTEMENT CONCERNÉ

La cybersécurité est enseignée dans le département Génie Électrique et Informatique (DGEI).

## THÉMATIQUES

Les principales thématiques enseignées couvrent la sécurité des systèmes logiciels et matériels (analyse de vulnérabilités et contre-mesures) mais aussi la sécurité des réseaux, la cryptographie, la gouvernance et l'écosystème de la sécurité.

Par ailleurs, le contexte local nous permet de proposer un module spécifique sur la sécurité des systèmes aéronautiques.

## CURSUS

La cybersécurité est enseignée dès la 4<sup>e</sup> année avec un cours d'introduction générale à cette problématique, suivi de deux cours plus spécifiques, l'un sur la sécurité du logiciel et l'analyse de vulnérabilités dans les programmes écrits en langage C et l'autre sur la sécurité des réseaux TCP/IP.

En ce qui concerne la 5<sup>e</sup> année, l'INSA Toulouse est à l'origine depuis 2015, en collaboration avec l'ENAC et l'ENSEEIH, d'une formation dédiée à la sécurité informatique, intitulée TLS-SEC. Cette formation de dernière année, d'environ 400 heures, regroupe des étudiants des 3 écoles et aborde les aspects sécurité logicielle, sécurité matérielle, cryptographie, sécurité des réseaux, sécurité des systèmes aéronautique et gouvernance de la sécurité.

Un stage de fin d'études, obligatoirement dans le domaine de la sécurité, vient compléter cette formation. La promotion actuelle compte une quarantaine d'élèves-ingénieurs, dont 18 de l'INSA.

## ÉCOSYSTÈME

Les enseignements de cybersécurité sont bien sûr assurés par les enseignants chercheurs du département Génie Électrique et Informatique mais ils sont également assurés par des intervenants de grands groupes industriels (Airbus, Thalès, Orange), de PME spécialistes de la sécurité mais aussi d'intervenants issus des services de l'état (DGSI, ANSSI, Marine Nationale), qui peuvent ainsi donner une vision métier de la cybersécurité.

Par ailleurs, les enseignants chercheurs du département sont impliqués dans le pilotage et l'organisation d'événements nationaux, tels que la conférence RESSI, mais aussi dans des groupes de travail du GDR sécurité Informatique du CNRS.

## RECHERCHE

Le département Génie Électrique et Informatique de l'INSA Toulouse est adossé au laboratoire de recherche LAAS-CNRS.

Les activités de recherche qui y sont menées dans les équipes Tolérance aux Fautes et Sûreté de Fonctionnement Informatique (TSF) ainsi que Service et Architectures pour Réseaux Avancés (SARA), permettent de nourrir les activités d'enseignement sur la sécurité, notamment dans le domaine de la sécurité du logiciel, des systèmes embarqués critiques, de la sécurité matérielle, de la cryptographie et de la sécurité des réseaux.

# CYBERSÉCURITÉ VIA LA FORMATION CONTINUE

## INSA LYON

La formation Mastère Spécialisé® « Cybersécurité du Numérique » de l'INSA Lyon forme depuis 2010 des experts en cybersécurité avec une double compétence technico-managériale.

Cette formation comporte plus de 500 heures de cours suivies d'une mission en entreprise de six mois. Elle est portée par plus de 70 % d'intervenants professionnels. Elle est labellisée SECNUMEDU par l'ANSSI et intègre 4 certifications professionnelles.

## Contact

Direction Formation Continue INSA Lyon  
dfc@insa-lyon.fr

**Pour plus de détails :** <https://www.insa-lyon.fr/fr/mastere-cybersecurite-numerique>.

## INSA TOULOUSE

L'INSA Toulouse porte, en partenariat avec l'ENAC et l'ENSEEIH, un mastère spécialisé Sécurité Informatique, depuis 2015 également, d'environ 450 heures, et dont la promotion comprend environ une dizaine d'étudiants.

Enfin, l'INSA Toulouse propose également un module de 50 heures dédié à la sécurité des objets connectés dans le cadre du mastère spécialisé MSIOT (Innovative and Secure IoT Systems).

## Contact

Direction Formation Continue INSA Toulouse  
fc@insa-toulouse.fr

**Pour en savoir plus :** <http://forpro.insa-toulouse.fr/fr/formation-diplomante/mastere-specialise.html>

## TÉMOIGNAGES

### Éléonore Carpentier, STI 2014-2019 INSA Centre Val de Loire

« La formation pluridisciplinaire de l'INSA m'a permis d'acquérir des compétences humaines et techniques en cybersécurité.

Celles-ci m'on permises d'avoir un profil attractif pour des entreprises en France ou à l'étranger ainsi que de réussir mon début de carrière ».



### Almamy Touré, 2016-2019 INSA Hauts-de-France

« Le parcours en informatique et cybersécurité que j'ai suivi à INSA Hauts-de-France m'a permis de découvrir de nombreuses facettes des métiers de la sécurité informatique. Grâce aux connaissances et compétences acquises tout au long de ma formation, j'exerce aujourd'hui le métier de spécialiste des menaces (threat expert) dans une grande société internationale, tout en envisageant avec confiance la suite de ma carrière d'ingénieur ».



### Yoan Simiand-Cossin, IF 2016-2021 INSA Lyon

« La formation très complète et pluridisciplinaire que j'ai suivie à l'INSA dans le département informatique m'a offert un large choix de métiers, en particulier dans le monde de la sécurité informatique. Les options proposées m'ont également permis de me spécialiser et d'évoluer dans ce domaine, ce qui m'a amené à exercer le métier d'auditeur en sécurité des systèmes d'information ».



### Mario Timani, IR 2016-2021 INSA Toulouse

« Découvrir la sécurité sous différents prismes est très enrichissant et formateur. À l'issue de la formation TLS-SEC, la qualité de l'enseignement ainsi que l'expertise des intervenants permettent de travailler dans tous les domaines de la sécurité ».



### Louise Treuil, INFO 2018-2023 Double diplôme avec Science Po-Rennes INSA Rennes

« L'option cybersécurité me permet d'acquérir de solides connaissances et compétences techniques en sécurité informatique. Cela est parfaitement complémentaire avec le master de Sécurité-Défense que je suis à l'IEP de Rennes dans le cadre de mon double diplôme ».



## DU CÔTÉ DES RECRUTEURS

**Frédérique Dauvillaire,**  
Thales Avionics, Toulouse

**THALES**  
Building a future we can all trust

« La cybersécurité est un sujet de haute importance au cœur des solutions et projets de Thales. Le savoir-faire de ses employés dans ce secteur est essentiel.

L'existence de la formation TLS-SEC contribue à l'acquisition de ce savoir car elle est très complète en associant enseignements théoriques et pratiques et l'intervention d'enseignants et de professionnels reconnus dans le domaine.

Comme cela fut mon cas, elle peut être suivie par des professionnels en activité et ainsi donner l'occasion d'acquérir ou de renforcer son savoir-faire et expertise en cybersécurité au cours de sa carrière ».

**5 INSA  
PROPOSENT  
UNE FORMATION  
EN CYBERSÉCURITÉ**

## POURSUITE EN THÈSE

Les étudiants diplômés d'un INSA peuvent se spécialiser après l'obtention de leur diplôme d'ingénieur en suivant une formation doctorale de 3 ans qui leur permet d'obtenir le grade et titre de docteur.

Les étudiants qui s'engagent dans une formation doctorale continuent d'être étudiants de l'INSA durant leur trois années de formation doctorale, mais ils sont également salariés et bénéficient des avantages sociaux afférents à ce statut.

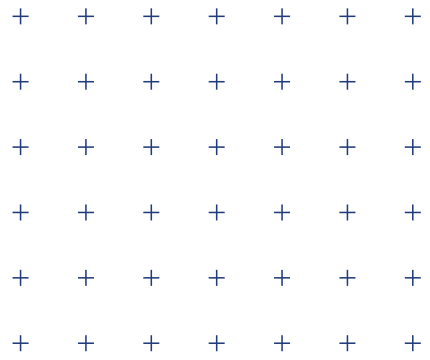
Ils effectuent leurs travaux de recherche au sein d'un laboratoire académique ou d'un département de recherche et développement d'une entreprise privée (le cas échéant, en partenariat avec un laboratoire académique).

Le sujet de thèse est proposé par le directeur de thèse académique (ou éventuellement par l'entreprise dans le cas d'une thèse en milieu industriel) en accord avec l'étudiant.

Le doctorat est un moyen de se former à la recherche et de se spécialiser sur un sujet spécifique (p. ex. « détection d'intrusion dans un réseau à partir d'algorithmes d'apprentissage automatique »).

Les docteurs trouvent un emploi dans le domaine de la cybersécurité sans aucune difficulté et peuvent prétendre directement à des postes d'experts ou de chercheurs.





# CONTACTS

## INSA CENTRE VAL DE LOIRE

Jérémy Briffaut, directeur du département STI  
jeremy.briffaut@insa-cvl.fr

## INSA HAUTS-DE-FRANCE

René Mandiau, directeur du département Informatique  
rene.mandiau@uphf.fr

## INSA LYON

Stéphane Frenot, directeur du département Télécommunications  
stephane.frenot@insa-lyon.fr

Lionel Brunie, directeur du département Informatique  
lionel.brunie@insa-lyon.fr

## INSA RENNES

Gildas Avoine, enseignant-chercheur département Informatique (INFO)  
gildas.avoine@insa-rennes.fr

Maxime Pelcat, enseignant-chercheur  
département Electronique et Informatique Industrielle (EII)  
maxime.pelcat@insa-rennes.fr

## INSA TOULOUSE

Germain Garcia, directeur du DGEI  
germain.garcia@insa-toulouse.fr

## INSA

CENTRE VAL DE LOIRE  
HAUTS-DE-FRANCE  
LYON  
RENNES  
ROUEN NORMANDIE  
STRASBOURG  
TOULOUSE



En savoir plus :

[www.groupe-insa.fr](http://www.groupe-insa.fr)

### Service Admission du Groupe INSA

Campus LyonTech - La Doua | 9 allée du Rhône

69628 Villeurbanne Cedex - France

Tél. : +33 (0)4 72 43 81 25 - [admiss@groupe-insa.fr](mailto:admiss@groupe-insa.fr)