

PROFIL D'ENSEIGNEMENT

Master en Cybersécurité

Le grade de **master 120 en cybersécurité** est décerné aux étudiants qui :

- ont acquis des **connaissances hautement spécialisées et intégrées** et des compétences larges **dans les diverses disciplines des sciences informatiques**, qui font suite à celles relevant du niveau de bachelier en sciences informatiques ou de bachelier en sciences de l'ingénieur, orientation ingénieur civil ;
- se sont **spécialisés** dans le domaine de la **sécurité informatique et des communications**, sous ses différentes composantes (primitives et outils logiciels, gestion du risque et de la sécurité, architecture des systèmes informatiques, réseaux, aspects matériels, gestion des standards, gestions des incidents...), ainsi qu'en **cryptographie, forensique, inférence** et traitement de **mégadonnées** et aux **enjeux légaux et éthiques** associés ;
- sont capables d'appliquer, de mobiliser, d'articuler et de valoriser ces connaissances et ces compétences en vue de contribuer, seuls ou en équipe, **à la conduite et à la réalisation d'un projet d'envergure de développement, d'évaluation et de sécurisation** d'un système d'information et de télécommunication pour le mener à son terme en maîtrisant la complexité, la multidisciplinarité et en tenant compte des objectifs, des ressources allouées et des contraintes qui le caractérisent ;
- sont capables d'organiser et de mener à son terme un **travail de recherche, de développement ou d'innovation** pour appréhender une problématique inédite relevant de leur discipline ;
- sont capables de **communiquer de façon claire, structurée et argumentée**, tant à l'oral qu'à l'écrit, à des publics avertis ou non, leurs conclusions, leurs propositions originales ainsi que les connaissances et principes sous-jacents, le cas échéant dans une langue étrangère ;
- ont développé et intégré un **fort degré d'autonomie** qui leur permet d'acquérir de nouveaux savoirs, de poursuivre leur formation et de développer de nouvelles compétences **pour pouvoir évoluer dans de nouveaux contextes** ;
- ont la capacité de pratiquer une **veille scientifique, technique et technologique**.
- ont la capacité de **mener une réflexion critique** sur l'impact de l'informatique en général et, en particulier, des projets auxquels ils contribuent et y font preuve de **rigueur, d'autonomie, de créativité, d'honnêteté intellectuelle, de sens éthique et déontologique**.

Prérequis

Les études du master en cybersécurité (master en 120 crédits, niveau 7) s'adressent en priorité aux étudiants ayant acquis les compétences générales et spécialisées sanctionnées par les grades académiques de **master en sciences informatiques** ou de **master ingénieur civil en informatique**. Dans ce cas, les étudiants peuvent se voir délivrer le grade académique après suivis et acquis 60 crédits spécifiques du programme, par valorisation de leurs études de 2^e cycle précédentes.

Par ailleurs, les études sont accessibles, moyennant un programme éventuellement adapté, aux étudiants maîtrisant les **compétences générales** des domaines des **sciences (17)** ou des **sciences de l'ingénieur et technologie (19)** et les **compétences spécialisées en informatique** certifiées notamment par un grade de bachelier en sciences informatiques, bachelier en sciences de l'ingénieur, orientation ingénieur civil, ou de bachelier en informatique et système (type court).

Les activités d'enseignement y sont conçues **en continuité** par rapport à celles de ces études et présupposent, notamment, des apprenants

- l'**autonomie** dans leur démarche d'apprentissage et de recherche d'informations, l'**esprit critique** et la **rigueur scientifique** ;
- la maîtrise des **outils mathématiques et formels** en usage dans la discipline ;
- la capacité de s'informer et de s'exprimer en **anglais technique**, tant à l'oral qu'à l'écrit, ou d'acquérir par eux-mêmes cette compétence, les études étant partiellement organisées en anglais ;
- la bonne connaissance des différents **concepts et notions générales de l'informatique**.

Les études comportent environ une moitié d'activités similaires à celles figurant aux programmes des masters qui y donnent directement accès, afin de permettre aux autres étudiants d'acquérir ces compétences communes, générales et spécialisées en informatique.

Si nécessaire, les étudiants peuvent, le cas échéant, compenser leurs lacunes partielles éventuelles par rapport à ces exigences au cours de leurs études de deuxième cycle, de manière autonome ou au sein d'un programme individuel adapté.

Objectifs

Les études de master en cybersécurité ont pour objectif principal de former des **spécialistes** de cette discipline pointue émergente et à répondre ainsi aux **attentes légitimes de la société** de diplômés aptes mettre leurs compétences au bénéfice de tous, notamment dans les **services et organismes publics**.

Les compétences acquises à l'issue de ces études ont pour finalité pour une large majorité des diplômés de former des **universitaires spécialisés en cybersécurité** capables d'assumer leurs **responsabilités** et leur rôle de **citoyen**, de **cadre** et de **professionnel de haut niveau** tout au long de leur vie, ainsi que poursuivre leur formation et de maintenir leurs compétences à jour **de manière autonome**, mais aussi de permettre l'accès direct à la formation doctorale et, au-delà, à la **carrière de chercheur**.

Cet objectif est atteint par quatre axes de formation principaux : une **formation spécialisée** en cybersécurité, un **stage** dans ce contexte particulier, un travail de préparation et de réalisation d'un **mémoire de fin d'études** et une large **formation générale en informatique** et dans les disciplines associées.

Formation spécialisée

Les études de master visent à approfondir les connaissances des étudiants et leurs compétences scientifiques et techniques par une formation spécialisée en lien direct avec les domaines de **recherche scientifique** des enseignants et de leurs équipes dans le domaine particulier de la cybersécurité ou de disciplines associées. De ce point de vue, les études tirent parti de l'**organisation conjointe** où chaque partenaire apporte **les compétences et savoir-faire spécifiques** de ses équipes de chercheurs et d'enseignants.

Ainsi, la majorité des activités d'enseignement du programme du cycle résultent d'un **choix cohérent** de l'étudiant d'enseignements dans les domaines suivants.

- **Cryptologie**, cryptanalyse et sécurité de l'information ;
- **Réseaux**, informatique distribuée et sécurisation des systèmes informatiques ;
- Techniques de gestion et d'exploitation de **mégadonnées** et inférence et fuites d'information ;
- **Forensique** et contrôle d'accès matériels et logiciels ;
- **Management** de la sécurité et mise en œuvre des **normes, audits et politiques de sécurité** ;
- **Aspects légaux**, éthiques et humains de la sécurité ;
- Conception d'**architectures de systèmes** sécurisés et d'outils logiciels spécialisés ;
- Méthodes de génie logiciel et de développement sécurisé.

Stage

Dans le cadre de leurs études, les étudiants sont tenus d'**effectuer un stage** dans une organisation, entreprise, administration ou laboratoire afin d'être mis dans **une situation réelle** d'analyse, d'organisation ou de développement d'une solution de cybersécurité. Pour les étudiants déjà en situation professionnelle, ce stage peut être effectué auprès de leur employeur, pour autant qu'il réponde aux critères attendus.

Ce stage a également pour but de mettre les étudiants **aux contacts d'autres professionnels** actifs dans le domaine. Il est **accompagné et évalué en continu** par l'équipe pédagogique.

Mémoire

Une part importante des compétences attendues d'un diplômé master en cybersécurité sont acquises et évaluées au travers de la réalisation d'un **mémoire de fin d'études**, travail **personnel** d'ampleur significative, la **rédaction d'un document écrit** original et personnel et sa **présentation publique** devant un jury spécialisé.

Ce travail peut être en relation avec le stage effectué.

Formation générale

En complément et de manière intégrée avec les deux objectifs principaux décrits ci-dessus, les études incluent une formation générale **en lien avec la cybersécurité**, notamment en **informatique**, en **sciences**, en **management**, en **droit** et dans d'autres disciplines, qui vise à faire acquérir diverses compétences spécifiques et transversales.

En particulier, le programme comporte des activités destinées à faire acquérir

- des connaissances essentielles et **multidisciplinaires** ;
- une maîtrise des **techniques légales et managériales** générales ;
- la capacité de **conduite et de réalisation de projets**.

Ainsi, les étudiants réalisent également plusieurs **projets collectifs** et **travaux personnels** en lien direct avec la plupart des enseignements. Ces activités constituent une part importante des évaluations associées. Celles-ci s'appuient sur des **rapports structurés, critiques et argumentés** démontrant tant leur maîtrise des compétences transversales informatiques, scientifiques et managériales, que leurs capacités d'acquisition autonome de connaissances et de savoir-faire nécessaires dans des contextes nouveaux et évolutifs.