

MASTER PROFESSIONNEL

MASTER CYBERSECURITE

Personnes à contacter

Référent pédagogique :

Gaetan Richard : gaetan.richard@unicaen.fr

Patrick Lacharme : patrick.lacharme@unicaen.fr

Référente administrative :

Agnès LEBLOND : sciences.fc@unicaen.fr

Sandra LAVIEILLE : sciences.fc@unicaen.fr

UFR DES SCIENCES – Formation Continue

Bâtiment Sciences 3, Campus 2 Côte de Nacre, Bd Maréchal Juin, Caen

Tél : 02 31 56 72 80 – 02 31 56 72 86

Sciences.fc@unicaen.fr

Présentation générale

Le master de cybersécurité propose une formation de deux ans niveau bac + 5 en sécurité informatique, qui permet de découvrir et d'approfondir tous les aspects de la sécurité informatique. Cette formation est co-accréditée entre l'université de Caen Normandie et l'ENSICAEN.

Admission

Le master cybersécurité est ouvert à l'ensemble des personnes ayant des connaissances solides en informatique, mathématiques appliquées, informatiques mathématiques et titulaires d'un BAC + 3 dans ces domaines. La Formation est accessible en initiale et en alternance.

Les modalités de sélection se font sur dossier (qualité du cursus antérieur, motivation, CV...)

Pour l'inscription en alternance : dépôt des candidatures sur les plateformes dédiées :

- Pour une inscription en 1re année, rendez-vous sur MonMaster
- Pour une inscription en 2e année, rendez-vous sur eCandidat

Objectifs de la formation :

- Gérer et piloter la sécurité d'un système d'information sous tous ses aspects (matériel, système, réseau, web, logiciel, information, cloud)
- Connaître les aspects pluridisciplinaires de la cybersécurité, notamment les aspects sociétaux, droit, vie privée et gestion de la sécurité.
- Maîtriser et appliquer les aspects techniques avancés de la sécurité informatique, comme la programmation sécurisée, la biométrie, les blockchains et la forensique.
- Comprendre les aspects théoriques avancés de la cybersécurité, notamment la cryptographie, la cryptanalyse et l'informatique quantique.
- Apprendre le hacking éthique à travers des enseignements orientés vers la sécurité défensive et offensive et des projets basés sur des CTF et des plateformes variés.

Principaux enseignements théoriques :

Au cours des deux ans de formations, le master contient quatre groupes de 5 UE avec des cours magistraux sur les thématiques suivantes, mais également de nombreux travaux pratiques et de challenges de sécurité à réaliser.

- Cryptographie
- Aspects pluridisciplinaires de la sécurité informatique
- Sécurité d'un système d'information
- Fondements informatiques de la sécurité

Ces enseignements théoriques sont complétés d'enseignements pratiques correspondant à une période d'activité en entreprise dans le cadre d'un contrat en alternance correspondant à 40 ECTS.

L'ensemble des enseignements seront évalués dans le cadre de contrôles de connaissances et d'une soutenance.

Programme de formation

Enseignement théorique

Unité d'enseignements	Modules	Heures (CM – TD – TP)
Semestre 1 20 crédits	Anglais et communication	42
	Programmation C/C++ Sécurisée	42
	Mathématique pour la cryptographie	42
	Cryptographie	42
	Introduction à la sécurité	42
Semestre 2 20 crédits	Aspects sociétaux de la sécurité	72
	Linux avancé	42
	Cryptographie avancée	42
	Sécurité web/réseaux	42
	Sécurité système/logicielle	42
Semestre 3 20 crédits	Anglais et communication	42
	Cryptographie post quantique	42
	Biométrie	42
	Sécurité IoT, Cloud, Blockchain	42
	Pentesting et audit sécurité	42
Semestre 4 20 crédits	Droit pour la sécurité et la vie privée	42
	Cryptanalyse quantique et parallélisme	42
	Sécurité des systèmes d'information	42
	Sécurité offensive et défensive	72
	Forensique	42

Organisation temporelle de la formation

- La formation universitaire commence début septembre et se termine après deux années (fin août) par la soutenance des mémoires, pour une durée totale de 907 heures
- Formation organisée en présentiel
- 30 Semaines de formation théorique à l'université de Caen d'enseignements en face à face pédagogique
- 74 semaines de formation pratique en entreprise dans le cadre de l'alternance

Modalités pédagogiques

Le cursus articule et intègre des enseignements théoriques et des enseignements pratiques. Les modalités pédagogiques sont adaptées en fonction des compétences et connaissances visées par l'enseignement. Sont notamment mobilisés les cours magistraux (CM), les travaux dirigés (TD) et/ou les travaux pratiques (TP). Un suivi spécifique en relation avec le tuteur industriel pour les stagiaires est mis en place. Ce dernier est consigné dans un livret de suivi électronique délivré au stagiaire en début de formation.

Modalité de validation

• Contrôle des connaissances :

Selon les objectifs de la formation, le contrôle des connaissances et des compétences peut mobiliser différentes modalités d'évaluation tels le contrôle terminal, le contrôle continu, ou une combinaison de contrôle terminal et de contrôle continu. Ces évaluations peuvent prendre des formes variées (écrits et ou oral, travail de groupe, rapport/mémoires, etc.). Ces modalités sont indiquées aux apprenants dans les délais réglementaires.

• Compétences acquises à l'issue de la formation :

- Apprendre le hacking éthique à travers des enseignements orientés vers la sécurité défensive et offensive et des projets basés sur des CTF et des plateformes variés.
- Gérer et piloter la sécurité d'un système d'information sous tous ses aspects (matériel, système, réseau, web, logiciel, information, cloud)
- Connaître les aspects pluridisciplinaires de la cybersécurité, notamment les aspects sociétaux, droit, vie privée et gestion de la sécurité.
- Maîtriser et appliquer les aspects techniques avancés de la sécurité informatique, comme la programmation sécurisée, la biométrie, les blockchains et la forensique.
- Comprendre les aspects théoriques avancés de la cybersécurité, notamment la cryptographie, la cryptanalyse et l'informatique quantique.

Pour plus d'information, vous pouvez consulter notre site internet et la fiche formation :

<https://uniform.unicaen.fr/catalogue/formation/m/7616-master-cybersecurite?e=FA&s=>