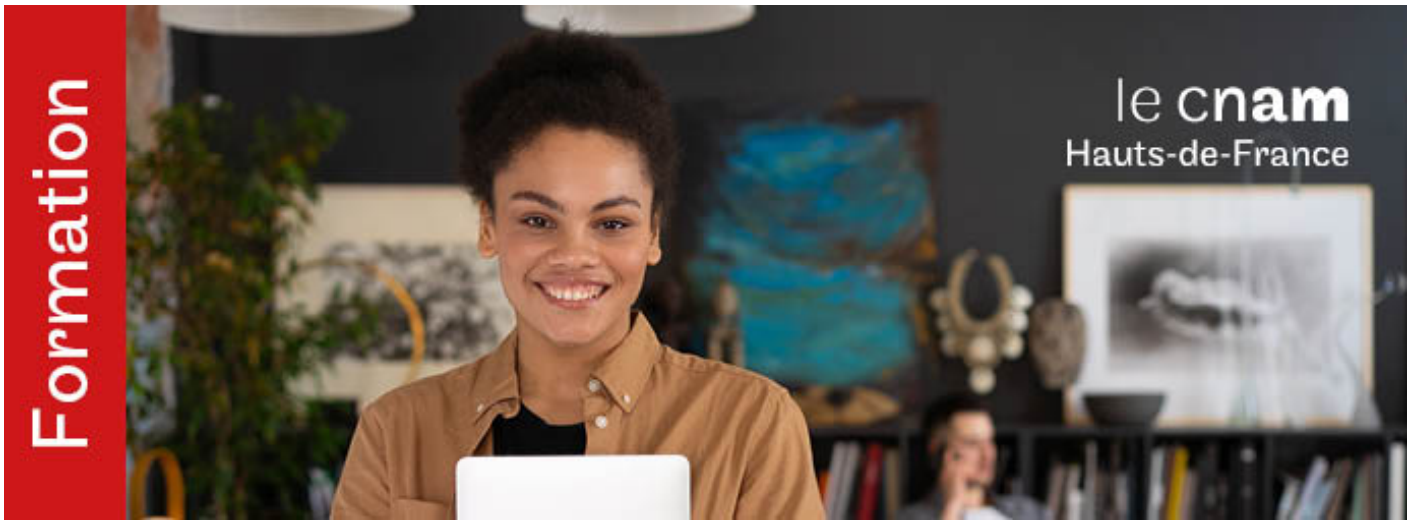

Master Sciences, technologies, santé mention Informatique Parcours Sécurité informatique, cybersécurité et cybermenaces En bretagne

MR11607A - 120 crédits

Niveau(x) d'entrée : BAC+3
Niveau(x) de sortie : BAC+5
Code RNCP (consultez la fiche en cliquant ici) : 34126
Lieu(x) : Non proposé en présentiel au Cnam HdF, nous contacter pour possibilité de formation à distance et hybride

Possibilité d'obtention par la VAE AU CNAM

PRÉSENTATION

Public / conditions d'accès

Accès en M1 :

- Sélection sur dossier de candidature ;
- Et être titulaire d'une licence en informatique, licence sciences et technologies mention informatique, licence génie mathématique et informatique, licence professionnelle métiers de l'informatique, licence professionnelle métiers des réseaux et télécommunication
- Ou autres licences scientifiques et techniques : admission sous réserve d'avoir acquis les UE (ou équivalents) : UTC501, UTC502, UTC503, UTC504, UTC505.

Accès direct en M2 :

- Sélection sur dossier de candidature ;
- Et Accès direct après validation du parcours M1 du Master Sécurité informatique, cybersécurité et cybermenace
- Ou un titre de niveau 6 ou 7 (Bac+4 et plus) avec une dominante soit informatique soit conception et développement d'applications soit administration systèmes et réseaux, soit réseaux/télécom ou spécialités similaires. Selon le cas, la validation d'unités complémentaires pourra être demandée.

Le master est également accessible en première ou seconde année par la VES, la VAE ou la VAPP.

Objectifs

Spécialiser dans la mise en oeuvre des mesures techniques et non techniques permettant la défense de systèmes d'informations essentiels.

COMPÉTENCES ET DÉBOUCHÉS

Compétences

Le programme se déroule sur deux années de 60 ECTS chacune. Chaque année inclut des enseignements techniques et des enseignements plus généraux afin d'asseoir les compétences en cybercriminalité et sécurité informatique sur un solide socle de compétences de base.
Le programme de la 1ère année de Master permet d'aborder les menaces associées à la criminalité informatique, d'en comprendre les motivations et les stratégies à partir de l'étude de la posture de l'attaquant. Ce parcours explique ensuite comment se préparer aux attaques et comment y réagir. Il aborde les thèmes suivants :

- Tronc Commun à l'ensemble des parcours du Master en Informatique du Cnam
- Lutte contre la criminalité
- Compréhension de la menace
- Il comporte également un parcours d'apprentissage de l'anglais.

La 2eme année approfondit les notions abordées en 1ere année et permet de couvrir les domaines liés aux différents métiers Cyber. Elle est architecturée autour des thématiques suivantes :

- Notions avancées de cyber sécurité
- Conception et maintien d'un SI sécurisé
- Homologation d'un SI
- Réaction aux attaques

Et un mémoire de fin d'études (sans stage obligatoire).

INFORMATIONS PRATIQUES

Valider la totalité des UE, US et UA du parcours avec une note supérieure ou égale à 10/20
A noter:

- Les auditeurs qui auraient validé RSX101 dans un parcours antérieur devront valider RSX103 dans le cadre de ce master
- Les auditeurs qui auraient validé SMB101 dans un parcours antérieur devront valider SMB111 dans le cadre de ce master

PROGRAMME

Contenu de la formation

Tronc commun

Parcours £M1

Introduction à la gestion de données à large échelle	NFE115	6 ects
Conception et urbanisation de services réseau	RSX103	6 ects

Parcours Une UE à choisir parmi :

Evaluation de performances et sûreté de fonctionnement	RCP103	6 ects
Optimisation en informatique	RCP104	6 ects

Parcours Une UE à choisir parmi :

Spécification et vérification des systèmes distribués	NFP103	6 ects
Spécification et Modélisation Informatiques	NFP108	6 ects

Parcours Une UE à choisir parmi :

Analyse des données : méthodes descriptives	STA101	6 ects
Intelligence artificielle	NFP106	6 ects
Anglais professionnel	ANG330	6 ects
Systèmes et applications répartis pour le cloud	SMB111	6 ects
Sécurité des réseaux	RSX112	6 ects
Droit, enjeux de sécurité, conformité	SEC103	6 ects
Introduction générale à la Criminologie	CRM201	6 ects

Parcours M2

Etude de la posture de l'attaquant	USCB10	3 ects
Ingénierie sociale et OSINT	USCB11	3 ects
Hacking réseau	USCB12	3 ects
Gérer la sécurité et piloter les projets de sécurité	USCB13	3 ects
Détection des attaques	USCB14	4 ects
Sécurisation avancée des données	USCB15	3 ects
L'homologation de sécurité	USCB16	6 ects
Audit de sécurité technique	USCB17	4 ects
Réagir à une attaque cyber	USCB18	4 ects
Analyse d'un système après incident	USCB19	6 ects
Introduction à la rétro conception et analyse de Malware	USCB1A	3 ects
Mémoire de fin d'étude	UACB06	18 ects

Méthodes pédagogiques:

Pédagogie qui combine des enseignements académiques et des pédagogies actives s'appuyant sur l'expérience en entreprise et le développement des compétences. Equipe pédagogique constituée pour partie de professionnels.

Modalités d'évaluation:

Chaque unité (UE, UA) fait l'objet d'une évaluation organisée en accord avec l'Etablissement public (certificateur) dans le cadre d'un règlement national des examens.

Un référent Cnam est dédié à l'accompagnement de toute personne en situation de handicap. Contactez : hdf_handicap@lecnam.net

Document non contractuel.
Le programme et le volume horaire de cette formation sont susceptibles d'être modifiés en fonction des évolutions du référentiel pédagogique national.

Le Cnam Hauts-de-France vous informe, vous accompagne et vous conseille.

Contactez nos conseillers formation au 0800 719 720 ou hdf_contact@lecnam.net

Tous nos programmes sur www.cnam-hauts-de-france.fr