Master Sciences, technologies, santé mention Informatique parcours Sécurité informatique, cybersécurité et cybermenaces PDL à Angers

Présentation

Publics / 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 œuvre des mesures techniques et non techniques permettant la défense de systèmes d'informations essentiels.

Modalités de validation

Les conditions requises pour valider une année entière sont :
• La moyenne des UE ou US qui composent l'année, calculée en pondérant chaque note par un coefficient égal à leur nombre de crédits (ECTS), doit être supérieure ou égale à 10/20
• ainsi qu'une note minimale de 10/20 à chaque UA
• Aucune note inférieure à 8/20

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

Valide à partir du 01-09-2024

Arrêté du 08 juillet 2021. Accréditation jusque fin 2024-2025. le 08-07-2021

Fin d'accréditation au 31-08-2025

Code : MR11607B

120 crédits

Master

Responsabilité nationale : EPN05 - Informatique / Nicolas PIOCH

Responsabilité opérationnelle : Mariem BENABDALLAH

Niveau CEC d'entrée requis : Niveau 6 (ex Niveau II)

Niveau CEC de sortie : Niveau 7 (ex Niveau I)

Mention officielle : Arrêté du 08 juillet 2021. Accréditation jusque fin 2024-2025.

Mode d'accès à la certification :

- Validation des Acquis de l'Expérience
- Formation continue
- Contrat de professionnalisation
- Apprentissage

NSF : Informatique, traitement de l'information, réseaux de transmission (326)

Métiers (ROME) : Expert / Experte en cybersécurité (M1802)

Code répertoire : RNCP34126

Code CertifInfo : 91725

Contact national :

Cnam Pays de la Loire
25 Bd Guy Mollet
BP 31115
44311 Nantes cedex 3
02 40 16 46 28
Eline Fenelon
ich.ouest@cnam-paysdelaloire.fr

- 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

Enseignements

120 ECTS

M1 60 ECTS

Introduction à la gestion de données à large échelle	USCB1B 5 ECTS
Conception et urbanisation de services réseau	USCB1C 6 ECTS
Optimisation en Informatique	USCB1D 5 ECTS
Spécification et Modélisation Informatiques	USCB1E 5 ECTS
Intelligence Artificielle	USCB1F 6 ECTS
Anglais Professionel	USCB1G 6 ECTS
Sécurité des réseaux	USCB1H 6 ECTS
Systèmes et applications répartis pour le cloud	USCB1J 5 ECTS
Droit, enjeux de sécurité, conformité	USCB1K 6 ECTS
Introduction générale à la Criminologie	USCB1L 5 ECTS
Séquence professionnelle	UACB09 5 ECTS

M2 60 ECTS

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 fin d'études — UACB07

13 ECTS

Séquence professionnelle — UACB08

5 ECTS