Master Sécurité informatique, cybersécurité et cybermenaces

Intitulé officiel : Master Sciences, technologies, santé mention Informatique parcours Sécurité informatique, cybersécurité et cybermenaces

Présentation

Publics / conditions d'accès

Accès en M1 :

- 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 télécommunications
- Autres licences : admission sous réserve d'avoir acquis : UTC501, UTC502, UTC503, UTC504, UTC505

Accès direct en M2 :

- Titre ingénieur en informatique, en télécommunications-réseaux, en réseaux et sécurité, en télécommunications, en informatique et gestion, en génie informatique ou spécialités similaires sous réserve de suivre ou d'avoir suivi, sans obligation de validation, SEC103, NSY115
- Master 2 en informatique, en réseaux ou spécialités similaires sous réserve de suivre ou d'avoir suivi, sans obligation de validation, SEC103, NSY115
- Master 2 Miage, sous réserve de valider RCP104 ou RCP105 et de suivre ou d'avoir suivi, sans obligation de validation, SEC103, NSY115
- Master 1 mention informatique ou mention réseaux et télécommunications, sous réserve de suivre ou d'avoir suivi, sans obligation de validation, SEC103, NSY115
- Titre concepteur-architecte du Cnam, sous réserve de suivre ou d'avoir suivi, sans obligation de validation, SEC103
- Titre de niveau 6 avec une dominante soit informatique soit conception et développement d'applications soit administration systèmes et réseaux, soit réseaux/télécom ou spécialités similaires sous réserve de valider SMB101 ou SMB111, UTC505, RSX101, RSX112, SEC103, NSY115

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

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

Valide le 06-10-2022

Fin d'accréditation au 31-08-2025

Code : MR11607A

120 crédits

Master

Responsabilité nationale : EPN05 - Informatique / Nicolas PIOCH

Responsabilité opérationnelle : Philippe BOINOT

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 Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
cnam@cnam-bretagne.fr

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).

Enseignements

120 ECTS

M1

Introduction à la gestion de données à large échelle	NFE115 6 ECTS

Une UE à choisir parmi : 6 ECTS

Réseaux et protocoles pour l'Internet	RSX101 6 ECTS
Conception et urbanisation de services réseau	RSX103 6 ECTS

Une UE à choisir parmi : 6 ECTS

Optimisation en informatique	RCP104 6 ECTS
Modélisation, optimisation, complexité et algorithmes	RCP105 6 ECTS

Une UE à choisir parmi : 6 ECTS

Spécification et vérification des systèmes distribués	NFP103 6 ECTS
Spécification et Modélisation Informatiques	NFP108 6 ECTS
Technologies pour les applications en réseau	RSX102 6 ECTS

Une UE à choisir parmi : 6 ECTS

Analyse des données : méthodes descriptives	STA101 6 ECTS
Intelligence artificielle	NFP106 6 ECTS

Anglais professionnel	ANG330 6 ECTS

Une UE à choisir parmi : 6 ECTS

Systèmes d'exploitation : principes, programmation et virtualisation	SMB101 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

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 de fin d'étude	UACB06 18 ECTS