DIPLÔME

Master Sciences, technologies, santé mention Informatique parcours Sécurité informatique, cybersécurité et cybermenaces en Bretagne

Code : MR11607A



Niveau d'entrée : Bac + 3, Bac + 4
Niveau de sortie : Bac + 5
ECTS : 120
Diplôme national
Oui

Déployabilité
Apprentissage : Fomation pouvant se suivre en apprentissage
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)
Contrat de professionnalisation : Formation pouvant se suivre en contrat de professionnalisation

Objectifs pédagogiques

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

Compétences et débouchés

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).

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

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

Prérequis et 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.

MENTIONS OFFICIELLES

Code RNCP
39278

Date d'enregistrement au RNCP
30/05/2025

Date de l'échéance de l'enregistrement au RNCP
31/08/2030

Mots-clés

- Réseaux et télécommunications
- Informatique - Réseaux informatiques
- Réseaux informatiques
- Transmission des données
- Réseau de télécommunications
- Politique de sécurité
- sécurisation du poste de travail
- Cryptographie
- Protocoles sécurisés
- Sécurité de l'information
- sécurité des systèmes d'informations
- Gestion des risques des systèmes d'information
- Cybersécurité
- Architecture client-Serveur

Protocole TCP/IP

Internet

Informations complémentaires

Type de diplôme

Master

Code NSF

326 - Informatique, traitement de l'information, réseaux de transmission
326n - Analyse informatique, conception d'architecture de réseaux

Codes ROME

Développeur / Développeuse de sécurité des systèmes d'information[M1805]
Analyste en cybersécurité[M1805]
Post auditeur / Post auditrice en sécurité des systèmes d'information[M1802]
Expert / Experte en tests d'intrusion - sécurité des systèmes d'information[M1802]
Expert / Experte en sécurité des systèmes d'information[M1802]
Auditeur / Auditrice en sécurité des systèmes d'information[M1802]
Architecte de sécurité des systèmes d'information[M1802]
Analyste en vulnérabilité de code logiciel[M1802]
Ingénieur / Ingénieure sécurité web[M1802]
Responsable sécurité informatique[M1802]
Responsable sécurité des systèmes d'information[M1802]
Ingénieur / Ingénieure sécurité informatique[M1802]
Expert / Experte sécurité, méthode et qualité informatique[M1802]
Expert / Experte sécurité informatique[M1802]
Expert / Experte en sécurité des systèmes d'exploitation[M1802]
Administrateur / Administratrice système informatique[M1801]
Administrateur / Administratrice sécurité informatique[M1801]
Expert / Experte en cybersécurité[M1802]

Formacode

Protocole télécommunication [24237]
Informatique - Systèmes d'information et numérique [31054]
Réseau informatique [24231]
Cybersécurité [31045]
Sécurité télécommunication [24293]
Logiciel cybersécurité [73054]
Sécurité informatique [31006]

Code du parcours

MR11607

URL externe

https://informatique.cnam.fr/master/spip.php?rubrique73

Modules d'enseignement

- → Analyse des données : méthodes descriptives
- → Anglais professionnel
- → Conception et Spécification des Systèmes Concurrents
- → Conception et urbanisation de services réseau
- → Intelligence artificielle
- → Introduction à la gestion de données à large échelle

- Introduction générale à la Criminologie
- Optimisation en informatique
- Sécurité des réseaux
- Spécification et Modélisation Informatiques
- Systèmes et applications répartis pour le cloud

M1

- Contrôle d'accès et Gestion des identités numériques
- Évaluation de performances
- Management et organisation des entreprises
- Programmation orientée objet en Python, Java et autres

M2

- Analyse d'un système après incident
- Audit de sécurité technique
- Détection des attaques
- Etude de la posture de l'attaquant
- Gérer la sécurité et piloter les projets de sécurité
- Hacking réseau
- Ingénierie sociale et OSINT
- Introduction à la rétro conception et analyse de Malware
- L'homologation de sécurité
- Mémoire de fin d'étude
- Réagir à une attaque cyber
- Sécurisation avancée des données

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.
Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.

Mettre en oeuvre les usages avancés et spécialisés des outils numériques
MR116B10

Mettre en oeuvre une communication spécialisée pour le transfert de connaissances
MR116B30

Résoudre des problèmes complexes en mobilisant les concepts fondamentaux et avancés de l'informatique
MR116B57

Mobiliser et produire des savoirs hautement spécialisés
MR116B20

Contribuer à la transformation en contexte professionnel
MR116B47

Concevoir des systèmes complexes et conduire des projets collaboratifs avancés
MR116B67

Analyser, valider et vérifier des résultats complexes
MR116B77