Master Sciences, technologies, santé mention Informatique parcours Sécurité informatique, cybersécurité et cybermenaces En formation continue, 100% à distance

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

Former des experts capables de concevoir, sécuriser et auditer les systèmes d'information face aux menaces actuelles.

Compétences développées :

- Architecture et sécurisation des SI
- Gestion des risques et conformité
- Analyse d'incidents (SOC, CERT)
- Posture défense / attaque (Blue & Red Team)

Ce Master débouche sur l'ensemble des métiers de la sécurité informatique tels qu'ils sont définis dans le panorama des métiers de la cybersécurité de l'ANSSI :

- Métiers de la Gestion de la sécurité et pilotage des projets de sécurité : RSSI, SSI, Directeur/coordinateur cybersécurité, …
- Métiers de la conception et du maintien d'un SI Sécurisé : Architecte sécurité, Auditeur/pentesteur, …
- Métiers de la gestion des incidents et des crises de sécurité : SOC, SIEM, Analyste forensic, Gestionnaire de crise, …

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

Mis à jour le 21-04-2026

Arrêté du 30 mai 2025. Accréditation jusque fin 2029-2030. le 30-05-2025

Fin d'accréditation au 31-08-2030

Code : MR11607E

120 crédits

Master

Responsabilité nationale : EPN05 - Informatique / Nicolas PIOCH

Responsabilité opérationnelle : Thierry GAILLARD

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

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

Mention officielle : Arrêté du 30 mai 2025. Accréditation jusque fin 2029-2030.

Mode d'accès à la certification :

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

NSF : Informatique, traitement de l'information, réseaux de transmission (326) , Analyse informatique, conception d'architecture de réseaux (326n)

Métiers (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) ,

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).

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

- Comprendre les concepts criminologiques et en appliquer les outils
- Comprendre la menace cyber pour savoir organiser la défense des systèmes et des réseaux
- Concevoir et maintenir un SI en sécurité
- Mettre en œuvre le process d'homologation d'un SI
- Gérer la sécurité et piloter les projets de sécurité
- Savoir prendre en compte le facteur humain dans les attaques (ingénierie sociale)
- Détecter les attaques cyber et y réagir
- Contrôler la sécurité des applications et des SI en opérant de tests d'intrusion, proposer des solutions techniques de remédiation
- Analyser un système après incident
- Maîtriser les techniques d'analyse statiques de codes (retro conception, analyse de malware)

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)

Code répertoire : RNCP39278

Code CertifInfo : 117222

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.n

Enseignements

120 ECTS

M1 60 ECTS

Introduction à la gestion de données à large échelle	USCB2B 6 ECTS
Conception et urbanisation de services réseau	USCB1C 6 ECTS
Evaluation de performances et sûreté de fonctionnement	USCB2C 6 ECTS
Programmation orientée objet en Python, Java et autres	USCB2D 6 ECTS
Intelligence Artificielle	USCB1F 6 ECTS
Anglais professionnel	USCB1G 6 ECTS
Sécurité des réseaux	USCB1H 6 ECTS
Systèmes et applications répartis pour le cloud	USCB2E 6 ECTS
Droit, enjeux de sécurité, conformité	USCB2F 6 ECTS

Une US à choisir parmi 6 ECTS

Contrôle d'accès et Gestion des Identités Numériques	USCB2G 6 ECTS
Introduction générale à la Criminologie	USCB1L 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