SCIENCES, TECHNOLOGIES, SANTÉ

Cyber-défense et sécurité de l'information

Master Réseaux et Télécommunications

Niveau d'étude visé
BAC +5

ECTS
120 crédits

Durée
4 semestres

Composante
INSA Hauts-de-France, UPHF

Langue(s) d'enseignement
Français

Présentation

Le master Cyber-Défense et Sécurité de l'Information (CDSI) forme des professionnels qualifiés ayant des solides compétences scientifiques, formés aux concepts, méthodes et techniques de traitement de la sécurité et de gestion du risque liés aux systèmes d'information et sachant protéger les ressources d'un système d'information. Il vise à former chaque étudiant aux méthodes et outils permettant de lutter contre la cybercriminalité et les failles des systèmes d'information et de traiter les problèmes liés aux domaines de la sécurité numérique et le codage de l'information afin de pouvoir assurer la disponibilité des services, la confidentialité des informations et l'authentification des contenus informatiques.

Cours dispensés en Français (niveau requis : B2)

Lieu de la formation :
FI : Campus Le Mont Houy Valenciennes
FA et FC : Campus de Maubeuge

Objectifs

Les professionnels ayant suivi ce parcours type Cyber-défense et sécurité de l'information, auront pour mission principale de lutter contre la cybercriminalité et les failles des systèmes d'information. Ils traiteront les problèmes liés aux domaines de la sécurité numérique et du codage de l'information afin de pouvoir assurer la disponibilité des services, la confidentialité des informations et l'authentification des contenus informatiques. Grâce à leurs compétences dans le domaine de la connectivité intelligente entre objets ou machines (Paiement à distance, domotique, montres connectées...) et leurs connaissances des techniques de liaison sans fil (RFID, NFC...) ils pourront répondre aux vulnérabilités de ces systèmes, aux cyber-attaques. Ils pourront aussi améliorer la sécurité de l'utilisation de ces objets connectés dans le domaine de la santé. Ils pourront également traiter des problématiques spécifiques de la sécurité des systèmes de transport intelligents (Communication inter-véhicules, véhicule-infrastructure...)

Compétences visées :

* Assurer la sécurité d'un système informatique en connaissant les techniques de hacking, les menaces et les failles des applications et systèmes actuels.
* Réaliser des audits de l'informatique industrielle et de gestion notamment sur la base des normes européennes de sécurité.
* Assurer la sécurité des procédés industriels.
* Concevoir et analyser des cryptosystèmes et des codes en vue d'application dans la sécurité de l'information.
* Mettre en œuvre ses compétences dans le domaine émergent de la radio intelligente pour la sécurité de l'information.
* Assurer l'ouverture vers des nouvelles technologies sécurisées en étudiant les architectures et les déploiements des réseaux de capteurs.
* Assurer la sécurité des contenus multimédia, des communications mobiles, des bases de données et du Cloud

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023

* Assurer la sécurité des systèmes embarqués en étudiant leurs mécanismes
* Etudier les principes des systèmes de transport intelligents et pour assurer leurs sécurités

Organisation

Stages

* Un stage de 6 mois dans une entreprise est obligatoire à la fin de la formation.
* Les activités de mise en situation s'articulent autour de projets courts, de projets longs et de stages.
* Il est important de noter que si les stages permettent d'acquérir une expérience professionnelle individuelle, la conduite des différents projets du cursus doit permettre aux étudiants de mettre en pratique des compétences complémentaires, telles que la gestion de projet, le travail coopératif, ...

Admission

Conditions d'admission

Master 1 : ouvert aux diplômés d'une licence informatique, mathématiques, GEII, systèmes d'information et réseaux.
Master 2 : Les étudiants ayant validé leur master 1 informatique, mathématiques appliquées, réseaux et télécoms, système d'information et réseaux.

Chaque candidat doit suivre, selon son parcours et ses vœux, une procédure de candidature décrite à l'adresse suivante https://www.uphf.fr/formation/candidatures-inscriptions

Pour toutes personnes n'ayant pas le diplôme requis, possibilité de validation des acquis (VAP) pour accéder à la formation.
Possibilité de validation des acquis de l'expérience (VAE) pour obtenir tout ou partie du diplôme. Contact : formation.continue@insa-hdf.fr

Pour les étudiants internationaux hors UE : https://pastel.diplomatie.gouv.fr/etudesenfrance/dyn/public/authentification/login.html

Modalités d'inscription

S'inscrire administrativement : https://inscription.uphf.fr/

S'inscrire pédagogiquement : Pour tous, auprès de votre secrétariat pédagogique.

Droits de scolarité

Consultez les montants des droits d'inscription ici

Et après

Finalité Master : Professionnel, Recherche

Poursuite d'études

Les diplômés peuvent s'orienter vers la recherche, en préparant une thèse de doctorat en entreprise ou en laboratoire de recherche en cryptologie ou en sécurité informatique et électronique.

Insertion professionnelle

* Les diplômés de cette spécialité auront la possibilité d'exercer leurs activités dans les services des établissements publiques et les collectivités territoriales, au sein des ministères intérieur et de la défense, dans les banques et les établissements financiers et au sein différentes entreprises de service.
* Ils pourront occuper les postes d'administrateur ou responsable de la sécurité du système d'information tant dans le domaine informatique que dans le domaine électronique et télécommunications, être chargés d'études et de conseils techniques liés à la recherche et

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023

développement ou à l'ingénierie pour auditer ou intégrer la sécurité des systèmes et évaluer ou développer les applications et logiciels sécurisées ou encore dans les services de production, d'exploitation, de maintenance, d'essais, de qualité et de sécurité des architectures (informatique et électronique). Ils seront aussi amenés à participer à la conduite de projets.

Intitulés métiers visés

* Responsable de la sécurité du système d'information
* Auditeur en sécurité des systèmes d'information
* Evaluateur d'applications sécurisées
* Ingénieur d'études et développement de logiciels sécurisés
* Consultant en sécurité de l'information
* Auditeur technique ou organisationnel, intégrateur
* Architecte sécurité (informatique et télécom)
* Administrateur de la sécurité (informatique et télécom)
* Enseignant-Chercheur en sécurité informatique et électronique

Infos pratiques

Contacts

Master CDSI

03 27 51 12 34

master-cdsi@uphf.fr

Contact Formation Continue

formation.continue@insa-hdf.fr

Lieu(x)

CAMPUS MONT HOUY - VALENCIENNES

CAMPUS DE MAUBEUGE

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023

Programme

Liste des principaux enseignements

- Maîtriser les concepts, les outils d'attaques, les techniques de contre-mesures
- Maîtriser les audits de l'informatique industrielle et de gestion
- Connaître les normes européennes de sécurité
- Connaître les architectures et les déploiements des réseaux de capteurs
- Maîtriser les outils de la sécurité des contenus multimédia et du Cloud
- Maîtriser les communications mobiles afin de pouvoir assurer leur sécurité
- Compétences transversales
- Compétences humaines : gestion de projet, management et langues

Année 4 (Formation Initiale)

SEMESTRE 7 (FI)

	Nature	CM	TD	TP	Crédits
Remise à niveau	UE				4
Outils mathématiques pour le codage et la cryptographie	UE				4
Exploitation des failles des systèmes distribués	UE				4
Techniques de Hacking des bases de données	UE				4
Sécurité des objets mobiles communicants	UE				4
Anglais	UE				4
Module Polytechnique	UE				4
Module d'ouverture	UE				2

SEMESTRE 8 (FI)

	Nature	CM	TD	TP	Crédits
Cryptographie et algorithmes d'apprentissage	UE				4
Normes de Sécurité et Analyses des Risques	UE				4
Sécurité des réseaux de capteurs	UE				4
Mise en Situation Professionnelle	UE				4
Sécurité des systèmes embarqués	UE				4
Anglais	UE				4
Module Polytechnique	UE				4

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023

Module d'ouverture	UE				2

Année 5 (Formation Initiale)

SEMESTRE 9 (FI)

	Nature	CM	TD	TP	Crédits
Cryptographie avancée	UE				4
Cyber-sécurité	UE				4
Privacité et sécurité des données dans le cloud	UE				4
Systèmes de transport intelligents et radio intelligente	UE				4
Sécurité informatique des procédés industriels	UE				4
Anglais	UE				4
Module Polytechnique	UE				4
Module d'ouverture	UE				2

SEMESTRE 10 (FI)

	Nature	CM	TD	TP	Crédits
Stage	UE				24
Projet	UE				6

Année 4 (Formation par apprentissage)

SEMESTRE 7 (FA)

	Nature	CM	TD	TP	Crédits
Remise à niveau	UE				4
Ethical Hacking	UE				4
Sécurité des bases de données	UE				4
Initiation à la Cybersécurité	UE				4
Anglais	UE				4
Module Polytechnique	UE				4
Activités Entreprise	UE				6

SEMESTRE 8 (FA)

	Nature	CM	TD	TP	Crédits

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023

Outils mathématiques pour la sécurisation de données 1	UE				4
Normes de sécurité et analyse des risques	UE				4
Sécurité des réseaux de capteurs et des systèmes embarqués	UE				4
Sécurité Couche physique	UE				4
Anglais	UE				4
Module d'ouverture	UE				2
Activités Entreprise	UE				8

Année 5 (Formation par apprentissage)

SEMESTRE 9 (FA)

	Nature	CM	TD	TP	Crédits
Outils mathématiques pour la sécurité (1)	UE				4
Sécurité des accès distants	UE				4
Sécurité des systèmes de communication sans fil	UE				4
Sécurité des systèmes industriels 1	UE				4
Anglais	UE				4
Module Polytechnique	UE				4
Activités Entreprise	UE				6

SEMESTRE 10 (FA)

	Nature	CM	TD	TP	Crédits
Transmission sécurisée de données	UE				4
Sécurité des systèmes industriels 2	UE				4
Outils avancés pour la sécurité	UE				4
outils d'audit et de pentest	UE				4
sécurité avancés des systèmes embarqués	UE				4
Activités Entreprise	UE				4
Projet	UE				6

Informations non contractuelles.
Dernière mise à jour le 03 novembre 2023