

INSCRIPTION ET ADMISSION

Le MS CyberSCID s'adresse à :

- des étudiants qui souhaitent se spécialiser et obtenir une double compétence complétant leur cursus initial
- des professionnels qui cherchent à acquérir une expertise spécifique en cybersécurité des systèmes industriels

Ils trouveront dans ce programme l'opportunité d'accéder à un secteur porteur et stratégique en tant qu'expert du domaine.

ADMISSION ET CALENDRIER

Retrait des dossiers de candidature :

- Contactez-nous !
- 3 sessions de recrutement par an (sélection sur dossier et entretien par visioconférence)
- Rentrée : mi-septembre.

CONDITIONS DE CANDIDATURE

- Diplôme de niveau Bac + 5 (ingénieur, M2)
- Sur dérogation, diplôme de niveau Bac + 4, ou M1 avec 3 années d'expérience professionnelle
- Diplôme étranger équivalent aux diplômes français mentionnés ci-dessus

FRAIS D'INSCRIPTION

- Etudiants/inscriptions individuelles : 10 000 €
- Entreprises, organismes : nous contacter
- Alumni et partenaires : nous contacter
- Possibilité de tarifs ajustés en fonction des variabilités des financements accordés par les OPCO et des prises en charge entreprises ou individus avec une remise pouvant aller jusqu'à 50 %.
- Certains déplacements optionnels, proposés dans le cadre des électifs, resteront à la charge des étudiants.

FRAIS DE DOSSIER

- Frais de dépôt et de traitement de dossier : 70 € non remboursables

CONTACTS

CENTRALE MÉDITERRANÉE

Admissions – Services administratifs

Céline Auger
+33 4 91 05 45 91
admission-ms@centrale-med.fr



Responsables pédagogiques

Professeure Caroline Fossati
Centrale Méditerranée et Institut Fresnel
+33 4 13 93 80 63

ÉCOLE DE L'AIR ET DE L'ESPACE

Admissions – Services administratifs

Patrick Franz
+33 4 13 93 80 00 poste 2 85 41
admission-ms@ecole-air.fr



Responsables pédagogiques

Alain Menelet
Chef du Centre d'Excellence Cyberdéfense
aérospatiale
+33 4 13 93 80 86

MASTERE SPECIALISE®

CYBERSÉCURITÉ DES SYSTÈMES COMPLEXES POUR L'INDUSTRIE ET LA DÉFENSE



ENJEUX ET OBJECTIFS PROFESSIONNELS

Avec le passage à un monde hyperconnecté, les entreprises des secteurs de l'industrie ou de la défense doivent désormais pouvoir compter sur des équipes d'experts cybersécurité de haut niveau afin de faire face aux vulnérabilités et aux menaces qui pèsent sur les systèmes d'information, réseaux, systèmes industriels, systèmes embarqués et systèmes de Défense.

Conçu par Centrale Méditerranée et l'École de l'air et de l'espace, en partenariat avec le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) et le Commandement de la Cyberdéfense, le **Mastère Spécialisé® CyberSCID est une formation post-master de niveau bac +6 dédiée aux problématiques de cybersécurité dans les systèmes industriels complexes.**

Elle permettra à chaque apprenant :

- d'appréhender les enjeux spécifiques de la cybersécurité, savoir détecter les vulnérabilités, acquérir une méthodologie et des techniques appropriées au renforcement du niveau de cybersécurité des systèmes existants ;
- de comprendre et d'identifier les points clés à examiner lors de la conception de systèmes complexes pour permettre une détection efficiente des attaques fin de pouvoir y répondre.

ATOUS DE LA FORMATION

- Unique formation Bac +6 en Région Sud, répondant aux besoins de l'industrie, de la défense, de l'énergie, de la santé et des transports.
- Partenariat fort et inédit entre 4 organismes de grande renommée. Accès à un réseau professionnel étendu, diplôme soutenu par le ministère des Armées et de nombreuses entreprises partenaires.
- Programme apportant une compréhension transverse et cohérente de tous les champs de la cybersécurité.
- Travaux pratiques, des plateformes et des outils logiciels de haut niveau. Possibilité de valider le CCNA Académique (*Cisco Certified Network Associate* – optionnel).
- Électifs dans les domaines de la Défense ou de l'énergie et des transports.

PLAN DE FORMATION

SEMESTRE 1

Module 1 : Remise à niveau

6 ECTS / 60 heures

- Remise à niveau EEA & Automatismes
- Remise à niveau informatique & réseau
- CCNA 1

Module 2 : Fondamentaux

6 ECTS / 60 heures

- Catégorisation de la menace
- Droit et réglementation cyber
- Relations internationales et cyber
- Intelligence cyberveille
- Travaux pratiques d'illustration
- CCNA 2 (optionnel)

Module 3 : Cartographie des systèmes, identification de la menace

4 ECTS / 40 heures

- Cartographie des systèmes
- Analyse de risque
- Menace Cyber et mode opératoire

Module 4 : Méthode et mécanismes de protection des systèmes

6 ECTS / 60 heures

- Mise en place d'une architecture sécurisée
- Cryptographie et sécurité de l'information
- Sécurité des logiciels et des systèmes d'exploitation

Module 5 : Méthodes et outils de détection

- IA et Data mining pour la cyber
- Mécanismes et outils de détection

Module 6 : Méthodes de réponse à une attaque, remédiation

3 ECTS / 30 heures

- Déroulement d'une cyberattaque et réactions d'urgence
- Rôle du SOC et du CERT
- Remédiation

Module 7 : Cycle de conférences

1 ECTS / 10 heures

Module 8 : Projet tutoré

9 ECTS / 80 heures

Modules électifs (1/2 au choix)

6 ECTS / 60 heures

- Défense (habilitation requise)
- Énergie et Transports

SEMESTRE 2

Thèse professionnelle

30 ECTS / 4 à 6 mois

- Formation pratique en entreprise validée par la soutenance d'une thèse professionnelle.
- L'étudiant devra réaliser un travail d'analyse, de conception et d'implémentation pour illustrer ses capacités à répondre à un problème de cybersécurité.
- Durant cette période, il bénéficiera à la fois d'un tutorat académique et d'un tutorat industriel.

Les cours se dérouleront en français et principalement dans les locaux de l'École de l'air et de l'espace, à Salon-de-Provence et occasionnellement à Centrale Méditerranée, campus de Marseille.