Mastère Spécialisé ® Cybersecurité & Smart Systems (RNCP 40347)

Présentation

/**/ .actions-fiche__item:first-of-type { margin-top: 0; display: none; } /**/ /**/ . username_field {display:none;} #oscar_school_form_body .form-group { margin-top:0px; } #oscar_school_form_body .btn.btn-primary{ margin:0.5em auto; } /**/

Architecte cybersécurité et internet des objets (RNCP 40347)

Découvrez en vidéo le Mastère Spécialisé ® Cybersecurité & Smart Systems (cybersécurité et systèmes intelligents) :

Dans un monde où les données explosent, où l'intelligence artificielle redéfinit les usages et où des milliards d'objets sont interconnectés, la cybersécurité est devenue un enjeu stratégique majeur.

Les systèmes intelligents, combinant Cloud, IoT, réseaux, données et intelligence artificielle, sont aujourd'hui au cœur des infrastructures critiques. Cette transformation accroît considérablement les surfaces d'attaque et impose de nouvelles approches en cybersécurité.

Le Mastère Spécialisé® Cybersécurité & Smart Systems de CY Tech répond à ces défis en formant des experts capables d'anticiper, analyser et contrer les menaces, tout en maîtrisant les architectures complexes des systèmes modernes. Il prépare des profils hybrides, à la fois techniques et stratégiques, capables d'intervenir sur l'ensemble de la chaîne de valeur de la cybersécurité, de l'IoT et des architectures communicantes.

Une formation à forte valeur ajoutée, alliant expertise technique, vision stratégique et immersion professionnelle au cœur des enjeux cyber actuels.

Objectifs de la formation

Ce programme vise à former des professionnels capables de maîtriser l'ensemble de la chaîne de cybersécurité des systèmes intelligents.

À l'issue de la formation, les diplômés seront capables de :

- concevoir et sécuriser des architectures complexes (Cloud, IoT, systèmes industriels) ;
- identifier, analyser et exploiter les vulnérabilités (pentest, analyse de malwares) ;
- réaliser des investigations numériques (forensic) ;
- mettre en œuvre des solutions de cybersécurité basées sur les données et l'IA ;
- gérer des incidents de sécurité et des crises cyber ;

Durée de la formation

- 1 année

Lieu(x) de la formation

- CY Tech, Campus de Saint-Germain-en-Laye

Stage(s)

Oui, obligatoires

Renseignements

cytech-fc@cyu.fr

+33134251029

https://eisti.osc3.tech/

- déployer des politiques de sécurité conformes aux standards internationaux (ISO 2700x) ;
- intégrer les enjeux de gouvernance, de conformité et de stratégie cyber.

Une formation au croisement de trois expertises clés

Cybersécurité opérationnelle : pentest, forensic, analyse de vulnérabilités, sécurité réseau et web.
Systèmes intelligents & connectés : IoT, systèmes industriels (OT/SCADA), réseaux avancés.
Data & Intelligence artificielle : IA appliquée à la cybersécurité, analyse de données, détection des menaces.

Pour recevoir la brochure, veuillez remplir le formulaire ci-dessous :

Admission

Pré-requis

Formation(s) requise(s)

- Titulaires d'un diplôme Bac+5 (Titre d'Ingénieur, M2, titre RNCP niveau 7)
- Titulaires d'un diplôme Bac+4 (M1) justifiant de 3 ans d'expérience professionnelle au minimum
- A titre dérogatoire : Titulaires d'un diplôme Bac+3 (L3) justifiant de 3 ans d'expérience professionnelle en lien avec le thème de la formation concernée

Candidature

Modalités de candidature

Les candidatures sont ouvertes et s'effectuent en ligne, sur le site web de CY Tech.

L'admission est prononcée sur la base du dossier de candidature et d'un entretien de motivation, réalisé en visio-conférence.
Frais de candidature : 80 € (en cas de refus ou désistement, ces frais restent acquis)

- Rentrée administrative : 9 novembre 2026
- Clôture des candidatures : 17 août 2026 pour les candidats internationaux et 3 semaines avant la date de rentrée pour les candidats résidants en France
- Pour les étudiants déjà résidents en France ou n'ayant pas besoin de passer par une procédure de Campus France ou de demande de visa, veuillez candidater ici :

En savoir plus sur les candidatures

Cette formation est accessible aux personnes en situation de handicap.

Étudier en situation de handicap

Modalités de candidature spécifiques

Si vous résidez à l'étranger, vous devez également effectuer la procédure Campus France afin d'obtenir un Visa.
Pour les personnes salariées, il est possible de financer la formation via votre entreprise dans le cadre de la formation continue.

Conditions d'admission / Modalités de sélection

Candidature : Voie classique ou alternance, choisissez votre parcours

Le Mastère Spécialisé® Cybersécurité & Smart Systems est accessible selon deux voies :

1. Voie classique

- - Statut étudiant
- - 6 mois de cours à temps plein, puis 6 mois de mission en entreprise (stage de fin d'études)

Candidater

2. Voie alternance

- Statut alternant (contrat d'apprentissage ou de professionnalisation)
  - Pour les contrats d'apprentissage : avoir 30 ans ou moins
  - Pour les candidats internationaux en contrat de professionnalisation : il faut être en France minimum un an
- Rythme : 7 jours à l'école / 7jours en entreprise sur toute l'année

Candidater

Modalités communes à toutes les candidatures :

- Dossier de candidature 100 % en ligne
- Étude du dossier par le jury
- Entretien de motivation en visioconférence (si admissible)
- Le jury se prononce sur votre admission et vous êtes informée de sa décision

Et après ?

Activités visées / compétences attestées

À l'issue de la formation, les diplômés auront développé des compétences solides en :

- exploitation des données et de l'IA en cybersécurité ;
- audit et test d'intrusion de systèmes complexes ;
- analyse de vulnérabilités et de malwares ;

- investigation numérique (forensic) ;
- sécurisation d’architectures Cloud, IoT et industrielles ;
- gestion des identités et des accès (IAM) ;
- gestion de crise et réponse à incident ;
- gouvernance et conformité (ISO 27001, EBIOS RM).