RÉCAPITULATIF DE LA FORMATION

Cybersécurité

Mastère Spécialisé de l'école ISEN Yncréa Méditerranée

Ouvrir tous les blocs

PROGRAM IDENTIFICATION

Label	Mastère Spécialisé
Program name	Cybersécurité
School	ISEN Yncréa Méditerranée - Institut supérieur de l'électronique et du numérique Yncréa Méditerranée
Internal number	1385
Acronym	CYBER
English name	
Program web link	https://isen-mediterranee.fr/formation/mastere-specialise-cybersecurite/
First accreditation date	01/09/2024
Number of renewals	
NSF codes	
Program domains	Informatique, traitement de l'information, réseaux
Other (keywords)	Cybersécurité
Co-accreditation establishments	
Academic partners	
Professional partners	Orange Cyberdéfense, 174 boulebard de Paris - 13003 MARSEILLE - France - Partnership convention AMADEUS, 485 route du Pin Montart - 06410 BIOT - France -

	Partnership convention EGERIE, 44 boulevard de strasbourg - 83000 TOULON - France - Partnership convention
Associated partners	WE ARE CYBER, 565 avenue du Prado - 13008 MARSEILLE - France - Partnership convention
Academic heads	LLOYD Benoît
Program directors or supervisors	LLOYD Benoît
Digital department managers	DUQUENOY Willy
Si formation coaccréditée, contact du/des responsable(s) de la formation chez votre/vos coaccréditeur(s)	
Professionnal certification	RNCP registrationConsidered Commentaire (dont historique des enregistrements) :
Program goals adjustments to targeted audience	L'objectif de la formation MS Cybersécurité est de permettre à des professionnels en activité (ou en recherche d'emploi) de se reconvertir ou d'effectuer une transition professionnelle vers le domaine de la sécurité informatique. L'objectif est de répondre aux tensions du marché de l'emploi dans le domaine de la cybersécurité. Les enseignements du MS Cybersécurité fournissent une boite à outils aux candidats dans les divers domaines de la cybersécurité (sécurisation des systèmes, gouvernance, supervision des réseaux, détection d'attaques, gestion de crise...). La thèse professionnelle et la mission en entreprise permettent aux candidat de se spécialiser dans une des branches de la cybersécurité. Le suivi du MS Cybersécurité nécessite certains prérequis chez le candidat (administration Système et Réseau). A l'étude de dossier de candidature, l'école pourra être amenée à proposer aux candidats des formations en ligne pour acquérir les prérequis.
Targeted profession and roles title	Le MS Cybersécurité permet aux candidats d'exercer un métier dans le secteur de la cybersécurité. Le diplômé a vocation a exercé les fonctions ciblées suivantes : - RSSI de TPE/PME - Chef de projet en cybersécurité - Consultant en cybersécurité - Ingénieur Cybersécurité - Responsable de SOC, CSIRT ou CERT - Analyste SOC, CERT ou CSIRT

ROME code(s)	M1801 - Administrateur / Administratrice sécurité informatique M1802 - Architecte de sécurité des systèmes d'information M1806 - Consultant / Consultante en système d'information
Business sectors	Activités spécialisées, scientifiques et techniques
Profession/targeted skills activities description	Activités liées au métier : - Configuration de la protection du SI ou du réseau - Élaboration d'une politique de sécurité de l'information - Préparation d'un audit de sécurité - Réalisation d'un plan de continuité et de reprise d'activité - Analyse des risques cybersécurité - Identification des vulnérabilités d'un système - Supervision des infrastructures et des évènements de sécurité - Détection des incidents et des menaces - Remédiation suite à un incident de sécurité - Veille permanente sur les menaces émergentes - Identification des preuves numériques - Collecte des preuves numériques - Gestion de crise suite à un incident de sécurité Compétences visées : - Intégrer les aspects de sécurité dans l'architecture et dans les éléments du système d'information ou du réseau, en définissant l'architecture adéquate et en proposant des choix de technologies, afin de le sécuriser - Réaliser une analyse de risque en sécurité en utilisant une méthode appropriée afin d'identifier les principaux risques ou failles de sécurité du système et proposer un traitement des risques - Établir un plan de continuité et de reprise d'activités, en définissant les processus et en identifiant les ressources techniques et humaines ainsi que les compétences mobilisables, afin de rétablir le bon fonctionnement du système - Identifier les éléments techniques de sécurité ou les outils à mettre en œuvre, en couvrant la mise en place de solutions de sécurisation des communications (protocoles de sécurité, chiffrement, certificats), segmentation de réseau et cloisonnement, dispositif de filtrage, solution de détection et de protection contre les intrusions sur le réseau et les terminaux (IPS, IDS), l'identification l'authentification forte et le contrôle d'accès, la traçabilité en temps réel ou en temps différé de l'ensemble des activités, la sécurité physique et les outils de contrôle, afin d'améliorer la sécurité des systèmes et des réseaux - Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles en utilisant les outils adéquats selon la méthodologie de tests d'intrusion - Assurer la supervision des infrastructures et des événements de sécurité en exploitant un système de gestion de l'information et des événements de sécurité (SIEM), en utilisant ces informations pour retracer la chronologie d'une cyberattaque afin de mettre en évidence les signaux faibles, qui d'ordinaire,

	passent inaperçus et d'éviter que ces mêmes attaques se reproduisent dans le futur - Collecter l'ensemble des informations relatives aux incidents informatiques à l'aide des outils adéquats afin d'avoir une première idée sur l'ampleur de la crise - Trier les éléments liés à l'incident en les catégorisant afin d'organiser des éléments de preuves analysables - Attribuer l'incident en établissant une grille d'analyse d'intrusion en utilisant les méthodes adéquates : Kill Chain, Diamond Model, la matrice MITRE ATT&CK, afin de modéliser une intrusion ciblée - Anticiper les futures évolutions des menaces à l'aide de la mise en place d'un système de veille recensant le renseignement en source ouverte (OSINT) - Contextualiser l'incident en faisant la corrélation entre signe d'incident et l'analyse de traces informatique (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation afin d'établir des scenarii potentiels d'incident - Gérer une crise avec l'ensemble des parties prenantes an adoptant une communication adaptée
Most frequent practice environments	Le diplômé du MS cybersécurité a vocation a être employé dans les grands groupes, ETI, PME, collectivités et organismes publics
Targeted positions responsibilities and autonomy	Le MS Cybersécurité permet de former des managers de la cybersécurité sachant mener une équipe, travailler en autonomie et prendre des décisions
Links between certification and targeted professional field	L'ouverture du MS Cybersécurité est le fruit des conclusions du conseil de perfectionnement du mois de janvier 2022. L'école a fait appel a certaines entreprises partenaires pour construire le programme et les contenus de formation : Orange CyberDéfense, AMADEUS, EGERIE, Wavestone et Avangarde Consulting. Etude d'opportunité.pdf
Identified needs or attested supports	Pour le MS Cybersécurité, l'école a reçu le soutien de la société Avangarde Consulting mais aussi de la Fondation Méditerranéenne d'Études Stratégiques (FMES). Lettres-soutien.pdf

School fees (euros)	
Initial training - non EU	9750
Initial training - EU	9750
Continuing education	9750
Eventuelles précisions	

COMPARABLE PROGRAMS

General access paths and targeted audience

Course

General evaluation

Knowledge/skills testing means

Methods, rules and procedures	Les modalités d'évaluation des connaissances et des compétences regroupent : - des examens écrits individuels portant sur les connaissances théoriques et les concepts vus dans les enseignements - des mini projets collectifs ou individuels avec rédaction d'un rapport écrit (seul le rapport écrit est évalué) - des mises en situation collective (serious-game) Le candidat doit obtenir au minimum 10/20 pour obtenir les crédits ECTS alloués à l'enseignement. En cas de résultat insuffisant, le candidat (ou le groupe) se verra offrir la possibilité de passer une épreuve de rattrapage. La part des projets collectifs ou mise en situation représente 75% des évaluations du Mastère Spécialisé. Cette part importante accordée aux projets et au travail en équipe est une volonté forte de l'équipe pédagogique. Les examens individuels permettent de s'assurer de l'acquisition des concepts théoriques pour lesquels des travaux pratiques sont difficilement possibles.
Company or laboratory internship evaluation	La mission en entreprise est évaluée par le tuteur industriel à l'aide d'une grille d'évaluation. Pour valider la mission en entreprise, le candidat doit obtenir au minimum 12/20. En cas d'échec, le candidat devra refaire une mission en entreprise de 4 mois minimum. L'équipe pédagogique a pour objectif de faire évoluer la grille d'évaluation entreprise (en pièce jointe au dossier) en prenant en compte les compétences (échéance juin 2024). L'objectif final est d'évaluer les compétences acquise et/ou mises en œuvre dans le cadre de la mission en entreprise.
Professional thesis assessment	La thèse professionnelle est évaluée par le biais de : - un rapport de thèse professionnelle (évalué par le tuteur académique) - une soutenance orale de la thèse professionnelle (évaluée par le jury de soutenance) Pour valider la thèse professionnelle, le candidat doit obtenir une moyenne de 12/20 (moyenne entre le rapport et la soutenance). En cas d'échec, le candidat aura le droit à un rattrapage. Les grilles d'évaluation jointes au dossier proviennent des grilles du Mastère Spécialisé "Maritime Telecommunication Networks"
Complementary documents	Evaluation Thèse professionnelle et mission en entreprise.pdf

Certification issuing

Quality - Continuous improvement