ENGINEERING SCHOOL

GIP CEI - Etablissement Public

GIP CEI - Etablissement Public

Soutenu par l'Etat dans le cadre de l'AMI «Compétences et Métiers d'Avenir» du Programme France 2030, opéré par la Caisse des Dépôts.

Mastère Spécialisé® 3C-IP

Cybersécurité, Cyberdéfense et gestion de Crise cyber pour les OIV Industriels et le secteur public

MS MASTÈRE SPÉCIALISÉ

LIEUX DE FORMATION
EPF Engineering School - 5 Esp. Germaine Tillon, 44600 Saint-Nazaire
Ecole Supérieur de Logistique Industrielle (ESTI) - 6 rue de la Maillardaie, 35600 Redon
Séminaires sur l'usine École de Rennes - https://iut-rennes.univ-rennes.fr/plateau-usine-ecole

Alternance, formation continue

BAC +6

OBJECTIFS

Le MS 3C-IP Atlantique vise à former des managers et chefs de projet en cybersécurité IT et cybersécurité industrielle et/ou portuaire (ICS/CPS-OT) capables de gérer une équipe, concevoir, intégrer et auditer des SI et SMSI en respectant les contraintes de sécurité inhérentes à un environnement donné, notamment au sein des Opérateurs d'Importance Vitale (OIV) et des services publics. Avec la montée en puissance des cybermenaces et la sophistication croissante des attaques, les compétences purement SSI ne suffisent plus à assurer une protection efficace des organisations et des infrastructures critiques. La formation met l'accent sur des savoir-faire essentiels tels que la réaction aux incidents de sécurité, l'investigation numérique, l'analyse de codes malveillants et l'audit de sécurité.

Les compétences développées sont à la fois techniques, organisationnelles, juridiques, géostratégiques et managériales, permettant aux diplômés d'adopter une approche globale et proactive de la cybersécurité. La formation s'attache également à offrir une vision inter-organisationnelle, intégrant les exigences de cybersécurité dans les processus d'achats et dans la gestion des relations avec les fournisseurs et sous-traitants. En effet, la sécurité de la chaîne d'approvisionnement numérique et industrielle et/ou portuaire devient un enjeu central, les attaquants ciblant de plus en plus les maillons faibles pour infiltrer les systèmes critiques.

Les futurs diplômés disposeront d'une compréhension transversale de la cybersécurité dans des environnements complexes, en particulier dans l'Industrie et la Défense. Ils seront en mesure de sécuriser et mettre en œuvre des stratégies adaptées pour garantir la protection et la résilience des systèmes d'information et des infrastructures industrielles, portuaires et maritimes.

Le programme de formation repose sur des entraînements pratiques immersifs, réalisés sur une plateforme de simulation IT/OT et une plateforme industrielle physique dédiée, permettant de confronter les étudiants à des scénarios réalistes de cyberattaques et de défense en environnements IT et OT.

PROGRAMME (PRÉVISIONNEL)

Sécuriser et optimiser la Supply Chain	- Planification et Prévisions appliquées - Stratégie supply chain et processus logistiques - Zero trust et défense en profondeur - Normes, référentiels et réglementations (RGPD, ISO 27001, Directive NIS 2, LPM etc.) - Planification de la gestion des incidents, Plans de Continuité (PCA) et de Reprise d'Activité (PRA) - Test, validation et audit de sécurité des systèmes et des réseaux
Définir et déployer l'organisation des achats	- Gestion des accès - Leadership et Management - Gestion du maintien en condition opérationnelle (MCO) et de sécurité (MCS) - Management des vulnérabilités liées à la transition numérique - Audit de sécurité des systèmes maritimes et portuaires - Traçabilité des opérations et accessibilité des systèmes numériques - Douanes et commerce internationnal
Organiser la qualité	- Schémas directeurs et organisation des transports/mobilités - Réglementations sur les mobilités, logistique urbaine/interurbaine - Traitement et remédiation des incidents - Détection, collecte et analyse des marqueurs de compromission - Cartographie des installations et analyse de risque sur un système industriel automatisé - Investigation numérique et analyse de malware
Conduire la transformation numérique dans la Supply Chain	- Gestion des achats de technologies - Normes, référentiels et réglementations (RGPD, ISO 27001, Directive NIS 2, LPM etc.) - Analyse de marché de la cybersécurité - Simulation d'évaluation des risques fournisseurs - Audits de sécurité des fournisseurs - Blockchain et investigation économique
Déployer la transformation environnementale et sociétale dans la Supply Chain	- Méthodologie de recherche d'information en source ouverte (OSINT) - Digitalisation des processus métiers - Analyse de la menace (CTI) et défenses des systèmes connectés et émergents - Sécurisation des communications et données mobiles, chiffrement - Protection des infrastructures de transports portuaires - Géopolitique et cyberdéfense
Conduire un projet d'amélioration et de la résilience	- Projet technique d'innovation - Challenges, CTF - Thèse professionnelle sur les sujets d'innovation en cybersécurité

SAVOIR-FAIRE CIBLÉS

- Développer, intégrer et évaluer la sécurité des solutions numériques
- Assurer l'adaptation des dispositifs de cybersécurité pour répondre aux évolutions de la menace et aux enjeux écologiques et sociétaux
- Intégrer la cybersécurité dans les processus achats et dans les relations avec les fournisseurs
- Assurer l'évaluation et la gestion des risques et des crises
- Garantir la continuité d'activités et des opérations de production et le maintien en condition opérationnelle de sécurité

DÉBOUCHÉS

Management et gouvernance de la cybersécurité
- Chef.fe de projet (cyber)sécurité
- Chef.fe de projet systèmes d'information
- Responsable de la sécurité des systèmes d'information (RSSI)
- Gestionnaire de crise en cybersécurité

Architecture et intégration de solutions
- Architecte en cybersécurité
- Intégrateur.rice de solutions de sécurité

Opérations de cybersécurité et SOC
- Ingénieur.e cybersécurité
- Analyste SOC (Niveau 1, 2, 3)
- Analyste réponse aux incidents de sécurité
- Spécialiste en lutte informatique défensive
- Analyste de menace cybersécurité

Audit et évaluation de la sécurité
- Auditeur.rice en conformité et sécurité organisationnelle et physique
- Auditeur.rice de sécurité technique
- Évaluateur.rice de la sécurité des technologies de l'information

Expertise technique avancée
- Expert.e en reverse engineering
- Consultant.e en cybersécurité

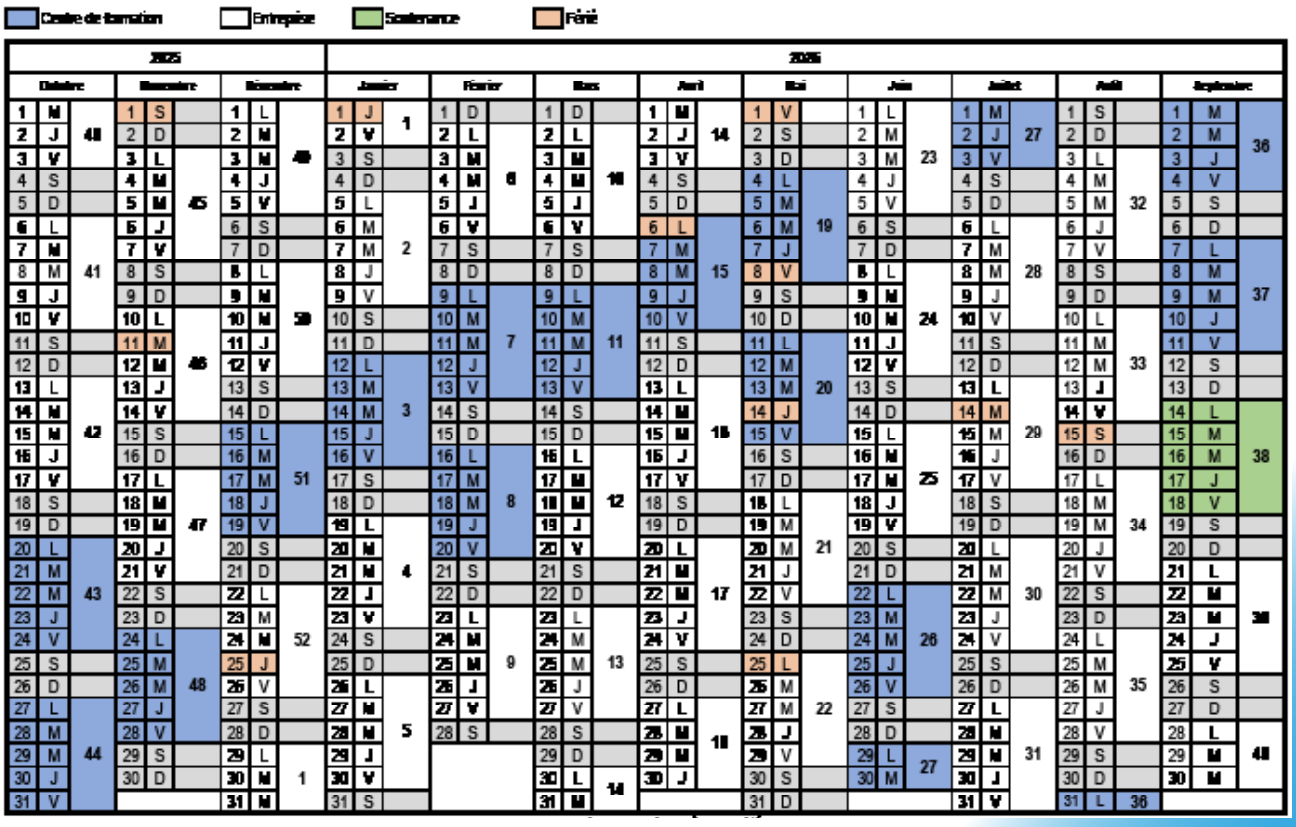
Formation et sensibilisation
- Formateur.rice en cybersécurité

RESPONSABLES DE FORMATION

Dr Zehira HADDAD
Responsable de la majeure ingénieurie et numérique à l'EPF
zehira.haddad@epf.fr

Dr Thierry SAUVAGE
Directeur de la recherche en Supply Chain
tsauvage@gip-cei.com

CALENDRIER (ANNÉE TYPE)



CONDITIONS D'ADMISSION ET PRÉREQUIS

Pour un parcours de formation en alternance ou en initial, être titulaire :
• d'un diplôme ou d'une certification reconnue de niveau bac +5
• d'un titre d'ingénieur diplômé conférant le grade de master
• d'un titre inscrit au répertoire national des certifications professionnelles (RNCP) niveau 7
• d'un diplôme étranger équivalent aux diplômes français exigés ci-dessus (avec attestation d'équivalence)

Pour un parcours en formation continue, être titulaire :
• d'un diplôme ou d'une certification reconnue de niveau Bac+4 et attester d'une expérience professionnelle de 2 ans minimum en lien avec la formation visée

A titre dérogatoire, VAAP :
• BAC+3 avec 3 ans d'expérience professionnelle minimum en lien avec la formation visée
• BAC/BAC+2 peuvent être admis avec 5 ans d'expérience professionnelle minimum en lien avec la formation visée via une procédure VAE/VAPP

CANDIDATURES

ADMISSION SUR DOSSIER, TESTS À DISTANCE ET ENTRETIENS
Dossier à compléter en ligne sur : **www.gip-cei.com**

Formation accessible aux personnes en situation de handicap, contacter le Pôle handicap du GIP CEI : handicap@gip-cei.com

COÛT

EN ALTERNANCE : GRATUITE ET RÉMUNÉRÉE
L'alternant signe un contrat de travail, lequel doit prévoir une rémunération.
Les frais de formation sont pris en charge par l'OPCO de l'entreprise d'accueil.

RÉFÉRENT ADMISSIONS

Thomas Kocinski
Responsable Développement et Admissions
tkocinski@gip-cei.com
Ligne directe : 06 40 79 79 23 | Standard : 02 99 71 60 20

MÉTHODES ET MOYENS MOBILISÉS

Exposés des notions essentielles, travaux pratiques systématiques, défis blue/red team, similations, CTF, visites d'entreprises, témoignages, la formation favorise une pédagogie active et le travail en groupe.
Le programme de formation prévoit des entraînements sur une plateforme de simulation IT/OT et une plateforme industrielle physique dédiées.
Suivi individualisé des étudiants en double tutorat : tuteur pédagogique (au centre de formation) et un
tuteur industriel (en entreprise), avec une visite de suivi par an par le tuteur pédagogique dans l'entreprise d'accueil. Salle mise à disposition, diaporamas, supports de cours, livret de l'étudiant, salle informatique en libre accès. Salle de détente de jeux et de musique en libre accès (pour les étudiants inscrits au BDE).

MODALITÉS D'ÉVALUATION

Contrôle continu de l'acquisition des connaissances avec une large part données aux travaux pratiques d'application, DST/ quizz, études de cas. Thèse professionnelle et soutenance portant sur une problématique d'actualité en cybersécurité. L'objet de la thèse professionnelle porte sur un thème choisi en lien avec la mission réalisée en entreprise/administration. Une mission au sein d'une entreprise/administration permettant d'évaluer la capacité de mise en œuvre et de conduite de projets de l'apprenant dans les domaines pré-cités. Une soutenance devant un jury composé de professionnels et d'universitaires pour mesurer la capacité de l'étudiant à faire valider un projet.

DURÉE

Les périodes de cours représentent une durée totale de 560h (16 semaines) par an.

DATES IMPORTANTES

Candidatures : acceptées jusque fin juin
Date des jurys et entretiens : à partir de décembre 2025
Rentrée : octobre 2026

Le GIP CEI / ESTI a obtenu, le 12 juillet 2021,
la certification du référentiel national de qualité Qualiopi.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre des catégories d'actions suivantes :
ACTIONS DE FORMATION
ACTIONS PERMETTANT DE VALIDER LES ACQUIS DE L'EXPÉRIENCE
ACTIONS DE FORMATION PAR APPRENTISSAGE

CONTACT IFALP/GIP CEI
Thomas Kocinski
Responsable Développement
et Admissions
06 40 79 79 23 | 02 99 71 60 20
tkocinski@gip-cei.com

www.gip-cei.com