ENGINEERING SCHOOL

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 - 55, avenue du Président Wilson, 94230 CACHAN
Ecole militaire de Paris - 1 Place Joffre, 75007 PARIS
Plate-forme industrielle de recherche LIFE
de l'ICAM Grand Paris Sud - Carré Sénart, 34 Points de Vue, 77127 LIEUSAINT

Alternance, formation continue

Bac +6

OBJECTIFS

Le MS 3C-IP vise à former des managers et chefs de projet en cybersécurité IT et cybersécurité industrielle (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 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.
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)

GARANTIR LA CYBERSÉCURITÉ DES INFRASTRUCTURES DE PRODUCTION	• Dispositifs de sécurité et configuration de la sécurité du SI et réseaux durcis • Dispositifs de sécurité des systèmes industriels • Configuration sécurité des SCADA et CPS • Administration IioT • Gestion avancée des identités et des accès (IAM)
DÉVELOPPER, INTÉGRER ET ÉVALUER LA SÉCURITÉ DES SOLUTIONS NUMÉRIQUES	• Développement logiciel et programmation d'automates et de systèmes embarqués • Cryptographie avancée et cryptanalyse • Intelligence artificielle et machine learning appliquée à la cybersécurité • Audit de sécurité technique et tests d'intrusion • Recherche de vulnérabilité et Tests d'intrusion systèmes IT, systèmes embarqués et IOT
ASSURER L'ADAPTATION DES DISPOSITIFS DE CYBERSÉCURITÉ POUR RÉPONDRE AUX ENJEUX ÉCOLOGIQUES ET SOCIÉTAUX	• Cyber Threat Intelligence et modélisation de la menace • Méthodologie d'OSINT avancée • Reverse-engineering, analyse de malware avancée • Investigations numériques (forensique) et analyse post-mortem avancée • Gestion avancée des risques cyber et d'un système de management de la sécurité de l'information
INTÉGRER LA CYBERSÉCURITÉ DANS LES PROCESSUS ACHATS ET DANS LES RELATIONS AVEC LES FOURNISSEURS	• Sécurité et Intelligence économique et grands enjeux de la sécurité de l'information • Droit de la SSI : LPM, SIIV/OIV, RGPD, NIS2, SecNumCloud, IGE13000 • Fondamentaux sur la fonction achats et le management de la chaine d'approvisionnement numérique et industrielle • Achats IT et analyse de marché de la cybersécurité • Stratégie d'externalisation IT/OT sécurisée et sécurité des approvisionnements • Ingénierie sociale et sensibilisation à la corruption • Audit de sécurité organisationnel, des normes et conformité
GARANTIR LE MAINTIEN EN CONDITION OPÉRATIONNELLE ET DE SÉCURITÉ	• Conception d'un SOC • Systèmes de détection d'intrusion (IDS) • Gestion de la continuité de l'activité et de la sécurité de l'information • Gestion de la réponse à incidents • Gestion de crise de cybersécurité, PCA/PRA
CONVAINCRE ET LÉGITIMER PAR UNE DÉMARCHE DE RECHERCHE ET L'ACTION	• Challenges CTF, hakathon • Projet collectif de recherche de cybersécurité • Thèse professionnelle sur un sujet innovant 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

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

Thibault FERRAND
Responsable de la filière Cybersécurité et Cyberdéfense
tferrand@gip-cei.com

CALENDRIER (ANNÉE TYPE)

Centre de formation | Entreprise | Soutenance | Férié

2025									2026																										
Octobre			Novembre			Décembre			Janvier			Février			Mars			Avril			Mai			Juin			Juillet			Août			Septembre		
1	M		1	S		1	L		1	J	1	1	D		1	D		1	M		1	V		1	L		1	M		1	S		1	M	
2	J	40	2	D		2	M		2	V		2	L		2	L		2	J	14	2	S		2	M		2	J	27	2	D		2	M	36
3	V		3	L		3	M	49	3	S		3	M		3	M		3	V		3	D		3	M	23	3	V		3	L		3	J	
4	S		4	M		4	J		4	D		4	M	6	4	M	10	4	S		4	L		4	J		4	S		4	M		4	V	
5	D		5	M	45	5	V		5	L		5	J		5	J		5	D		5	M		5	V		5	D		5	M	32	5	S	
6	L		6	J		6	S		6	M		6	V		6	V		6	L		6	M	19	6	S		6	L		6	J		6	D	
7	M		7	V		7	D		7	M	2	7	S		7	S		7	M		7	J		7	D		7	M		7	V		7	L	
8	M	41	8	S		8	L		8	J		8	D		8	D		8	M	15	8	V		8	L		8	M	28	8	S		8	M	
9	J		9	D		9	M		9	V		9	L		9	L		9	J		9	S		9	M		9	J		9	D		9	M	37
10	V		10	L		10	M	50	10	S		10	M		10	M		10	V		10	D		10	M	24	10	V		10	L		10	J	
11	S		11	M		11	J		11	D		11	M	7	11	M	11	11	S		11	L		11	J		11	S		11	M		11	V	
12	D		12	M	46	12	V		12	L		12	J		12	J		12	D		12	M		12	V		12	D		12	M	33	12	S	
13	L		13	J		13	S		13	M		13	V		13	V		13	L		13	M	20	13	S		13	L		13	J		13	D	
14	M		14	V		14	D		14	M	3	14	S		14	S		14	M		14	J		14	D		14	M		14	V		14	L	
15	M	42	15	S		15	L		15	J		15	D		15	D		15	M	16	15	V		15	L		15	M	29	15	S		15	M	
16	J		16	D		16	M		16	V		16	L		16	L		16	J		16	S		16	M		16	J		16	D		16	M	38
17	V		17	L		17	M	51	17	S		17	M		17	M		17	V		17	D		17	M	25	17	V		17	L		17	J	
18	S		18	M		18	J		18	D		18	M	8	18	M	12	18	S		18	L		18	J		18	S		18	M		18	V	
19	D		19	M	47	19	V		19	L		19	J		19	J		19	D		19	M		19	V		19	D		19	M	34	19	S	
20	L		20	J		20	S		20	M		20	V		20	V		20	L		20	M	21	20	S		20	L		20	J		20	D	
21	M		21	V		21	D		21	M	4	21	S		21	S		21	M		21	J		21	D		21	M		21	V		21	L	
22	M	43	22	S		22	L		22	J		22	D		22	D		22	M	17	22	V		22	L		22	M	30	22	S		22	M	
23	J		23	D		23	M		23	V		23	L		23	L		23	J		23	S		23	M		23	J		23	D		23	M	39
24	V		24	L		24	M	52	24	S		24	M		24	M		24	V		24	D		24	M	26	24	V		24	L		24	J	
25	S		25	M		25	J		25	D		25	M	9	25	M	13	25	S		25	L		25	J		25	S		25	M		25	V	
26	D		26	M	48	26	V		26	L		26	J		26	J		26	D		26	M		26	V		26	D		26	M	35	26	S	
27	L		27	J		27	S		27	M		27	V		27	V		27	L		27	M	22	27	S		27	L		27	J		27	D	
28	M		28	V		28	D		28	M	5	28	S		28	S		28	M	18	28	J		28	D		28	M		28	V		28	L	
29	M	44	29	S		29	L		29	J					29	D		29	M		29	V		29	L	27	29	M	31	29	S		29	M	40
30	J		30	D		30	M	1	30	V					30	L	14	30	J		30	S		30	M		30	J		30	D		30	M	
31	V					31	M		31	S					31	M					31	D					31	V		31	L	36			

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

Antony CARDOSO
Responsable Développement et Admissions IFALP
acardoso@gip-cei.com
Ligne directe : 06 03 79 53 48 | Standard : 01 87 66 58 37

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 2024
Rentrée : octobre 2025

Le GIP CEI / ESLI – 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
Antony CARDOSO
Responsable Développement et Admissions
01 87 66 58 37 | 06 03 79 53 48
acardoso@gip-cei.com

www.gip-cei.com