

MASTÈRE 2 : MANAGER MLAI

Titre de niveau 7, reconnu par l'Etat et inscrit au RNCP (JO du 31/05/2023)

Option : C2SI Cybersécurité des Supply Chain et des Systèmes Industriels

2025



**Prix de Lancement de
Programme**
EDUNIVERSAL



 **GOUVERNEMENT**
Liberté
Égalité
Fraternité

 **BANQUE des
TERRITOIRES**

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.



LIEUX DE FORMATION

GIP CEI / ESTI
6, rue de la Maillardais
35600 REDON

IUT DE RENNES – DÉPARTEMENT GEI
3, rue du clos Courtel
35704 Rennes cedex

ALTERNANCE, FORMATION CONTINUE ET VAE

TITRE RECONNU PAR L'ETAT

BAC +5 | MASTÈRE 2

**Option : C2SI - Cybersécurité des
Supply Chain et des Systèmes Industriels**



Cette formation conduit à l'obtention du titre de niveau 7 MLAI, certification enregistrée au RNCP (37618) sur décision de France Compétences en date du 31 mai 2023, délivrée par le Groupement d'Intérêt Public (GIP CEI).

VOS RESPONSABLES DE FORMATION

Hind ABOUSSIKINE

Responsable du M2 MLAI C2SI
Professeure affiliée
haboussikine@gip-cei.com

Rémi SAISSET

Professeur agrégé de SII, responsable
pédagogique de la ligne Usine école
«Outil de Production intelligent»
- Smart Production
remi.saisset@univ-rennes.fr
rsaisset@gip-cei.com

Patrick ERARD

Directeur des Opérations du Pôle
d'excellence cyber, coordinateur des
axes formation & recherche
patrick.erard@pole-excellence-cyber.org



PROGRAMME (PRÉVISIONNEL)

	Fondamentaux	Spécialité C2SI
CONDUIRE LA TRANSFORMATION NUMÉRIQUE DANS LA SUPPLY CHAIN	- Digitalisation des processus métiers supply chain - Cybersécurité des systèmes industriels - Normes, référentiels et réglementations (RGPD, ISO 27001, Directive NIS 2, ISO 62443 etc.)	- Analyse des risques numériques dans la supply chain - Audit de sécurité sur les systèmes industriels - Découverte des vulnérabilités et Test d'intrusion en milieu industriel
CONCEVOIR ET DÉPLOYER UN PROJET DE CYBERSÉCURITÉ POUR LA SUPPLY CHAIN	- Méthodologie de gestion de projet en cybersécurité - Mise en œuvre des solutions de sécurité adaptées	- Développement d'un projet de cybersécurité sur un système industriel - Revue des solutions de sécurisation et mise en pratique - Gestion du Maintien en Condition Opérationnelle (MCO) et de Sécurité (MCS) d'un système d'information industriel
SÉCURISER ET OPTIMISER LE FONCTIONNEMENT DES SYSTÈMES DE PRODUCTION	- Prévention et défense en profondeur des systèmes industriels - Surveillance des installations - Gestion des incidents, Plans de Continuité (PCA) et de Reprise d'Activité (PRA)	- Cartographie des installations et analyse de risques sur un système industriel automatisé - Menaces cyber associées à la digitalisation des processus industriels - Tests d'intrusion - Traitement et remédiation des incidents
DÉPLOYER DES PRATIQUES NUMÉRIQUES DURABLES	- Intégration des enjeux de cybersécurité industrielles dans les stratégies de développement durable - Responsabilité Sociétale des Entreprises	Audit et conformité des infrastructures numériques face aux défis sociétaux et environnementaux
DÉFINIR ET SÉCURISER L'ORGANISATION DES ACHATS	- Gestion des risques liés à la cybersécurité sur la filière achat - Sécurisation des contrats et relations fournisseurs - Gestion des audits de sécurité des fournisseurs	- Simulation d'évaluation des risques fournisseurs - Création d'un contrat sécurisé conforme aux bonnes pratiques - Mise en place d'un processus d'audit des fournisseurs - Mise en place d'une chaîne d'alerte
ORGANISER ET SÉCURISER LES INFRASTRUCTURES DE TRANSPORT	- Protection des infrastructures de transports - Sécurisation des communications et données mobiles	- Analyse des menaces et défenses des transports - Protection des données mobiles et échanges sécurisés

OBJECTIFS

Les systèmes industriels et logistiques sont au cœur de la souveraineté et de l'indépendance des tissus économiques et des nations. Les niveaux croissants d'informatisation, d'automatisation, de robotisation et d'internet industriel des objets s'appuient sur de l'intelligence artificielle aux formes et outils multiples nécessitant des compétences nouvelles. Ces nouveaux outils, qui couplent des données massives (vidéo/image/texte/QR codes etc.), et les risques nouveaux associés (sociaux, juridiques, stratégiques, cybersécurité etc.) s'imposent aux organisations et sont au centre du cursus C2SI. Leur maîtrise constitue un formidable levier de compétitivité et de création de valeur à tous les échelons de la supply chain (achat/approvisionnement, production, distribution/transports).

Le programme vise à former des futurs responsables, capables de :

- comprendre les enjeux et les spécificités de la cybersécurité dans les systèmes industriels ;
- réaliser des audits de systèmes industriels, proposer et piloter le déploiement de plans d'action ;
- maîtriser la réalisation d'analyses de risques et l'identification des vulnérabilités ;
- déployer des méthodes et outils permettant d'anticiper, de détecter et de se prémunir contre les attaques ;
- définir un plan de continuité d'activité / plan de reprise activité ;
- assurer le pilotage de la sécurité au sein d'un environnement industriel.

DÉBOUCHÉS

Perspectives d'emploi :

- Administrateurs réseaux et systèmes ICS / Scada / IT / OT en industries et logistique/production
- Fonctions d'expertise en cabinet de conseils : audit, consultant, intégrateur, formateur en cybersécurité

Plan de carrière possible :

- Responsable sécurité des systèmes de production et systèmes d'information
- Ingénieur et Chef de projet en cybersécurité industrielle

CALENDRIER (ANNÉE TYPE)

2024												2025																
Septembre			Octobre		Novembre		Décembre		Janvier		Février		Mars		Avril		Mai		Juin		Juillet		Août					
1	D		1	M	1	V	44	1	D	1	M	1	S	1	S	1	M	1	J	18	1	D	1	M	1	V		
2	L		2	M	2	S		2	L	2	J	1	2	D	2	D	2	M	2	V	2	L	2	M	2	S		
3	M		3	J	3	D		3	M	3	V		3	L	3	L	3	J	3	S	3	M	3	J	3	D		
4	M	36	4	V	4	L		4	M	4	S		4	M	4	M	4	V	4	D		4	M	4	V	4	L	
5	J		5	S	5	M		5	J	5	D		5	M	5	M	5	S	5	L		5	J	5	S	5	M	
6	V		6	D	6	M	45	6	V	6	L	6	6	J	6	J	6	D	6	M		6	V	6	D	6	M	
7	S		7	L	7	J		7	S	7	M		7	V	7	V	7	L	7	M	19	7	S	7	L	7	J	
8	D		8	M	8	V		8	D	8	M	2	8	S	8	S	8	M	8	J		8	D	8	M	8	V	
9	L		9	M	9	S		9	L	9	J		9	D	9	D	9	M	9	V		9	L	9	M	9	S	
10	M		10	J	10	D		10	M	10	V		10	L	10	L	10	J	10	S		10	M	10	J	10	D	
11	M	37	11	V	11	L		11	M	11	S		11	M	11	M	11	V	11	D		11	M	11	V	11	L	
12	J		12	S	12	M		12	J	12	D		12	M	12	M	12	S	12	L		12	J	12	S	12	M	
13	V		13	D	13	M	46	13	V	13	L		13	J	13	J	13	D	13	M		13	V	13	D	13	M	
14	S		14	L	14	J		14	S	14	M	3	14	V	14	V	14	L	14	M	20	14	S	14	L	14	J	
15	D		15	M	15	V		15	D	15	M		15	S	15	S	15	M	15	J		15	D	15	M	15	V	
16	L		16	M	16	S		16	L	16	J		16	D	16	D	16	M	16	V		16	L	16	M	16	S	
17	M		17	J	17	D		17	M	17	V		17	L	17	L	17	J	17	S		17	M	17	J	17	D	
18	M	38	18	V	18	L		18	M	18	S		18	M	18	M	18	V	18	D		18	M	18	V	18	L	
19	J		19	S	19	M	47	19	J	19	D		19	M	19	M	19	S	19	L		19	J	19	S	19	M	
20	V		20	D	20	M		20	V	20	L		20	J	20	J	20	D	20	M		20	V	20	D	20	M	
21	S		21	L	21	J		21	S	21	M	4	21	V	21	V	21	L	21	M	21	21	S	21	L	21	J	
22	D		22	M	22	V		22	D	22	M		22	S	22	S	22	M	22	J		22	D	22	M	22	V	
23	L		23	M	23	S		23	L	23	J		23	D	23	D	23	M	23	V	17	23	V	23	L	23	M	
24	M		24	J	24	D		24	M	24	V		24	L	24	L	24	J	24	S		24	M	24	J	24	D	
25	M	39	25	V	25	L		25	M	25	S		25	M	25	M	25	V	25	D		25	M	25	V	25	L	
26	J		26	S	26	M		26	J	26	D		26	M	26	M	26	S	26	L		26	J	26	S	26	M	
27	V		27	D	27	M	48	27	V	27	L		27	J	27	J	27	D	27	M		27	V	27	D	27	M	
28	S		28	L	28	J		28	S	28	M	9	28	V	28	V	28	L	28	M	22	28	S	28	L	28	J	
29	D		29	M	29	V		29	D	29	M	5	29	S	29	S	29	M	29	J		29	D	29	M	29	V	
30	L	40	30	M	30	S		30	L	30	J		30	D	30	D	30	M	30	V		30	L	30	M	30	S	
			31	J				31	M	31	V				31	L		31	S					31	J		31	D

Calendrier susceptible d'être modifié

(Calendrier susceptible d'être modifié)



CONDITIONS D'ADMISSION ET PRÉREQUIS

Sont admissibles les candidats ayant un diplôme de niveau Bac +3 dans le domaine du génie industriel, des réseaux industriels, et de la sécurité des systèmes d'information. Parcours uniquement proposé sur 2 ans.

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

EN FORMATION CONTINUE ET VAE :

Nous vous remercions de prendre contact avec Sylvia DÉSIGNÉ : 0 2 99 71 60 23

MÉTHODES ET MOYENS MOBILISÉS

Salle mise à disposition, diaporamas, supports de cours, livret de l'étudiant, salle informatique en libre accès.

Face à face, exposés des notions essentielles, cas pratiques, jeux pédagogiques, visites d'entreprises, témoignages, la formation favorise le travail en groupe. Suivi individualisé des étudiants en double tutorat : tuteur pédagogique (au centre de formation) et un tuteur industriel (en entreprise). 1 visite de suivi par an par le tuteur pédagogique dans l'entreprise d'accueil.

DURÉE

Formation en 24 mois.

14 semaines de formation par an.

MODALITÉS D'ÉVALUATION

Contrôle continu, études de cas.

Projet de fin d'études portant sur un thème choisi en lien avec la mission réalisée en entreprise.

Une mission en entreprise permettant d'évaluer la capacité de mise en œuvre et de conduite de projets de l'apprenant dans les domaines précités. Une soutenance devant un jury composé de professionnels et mesurant la capacité de l'étudiant à faire valider un projet ou un travail réalisé.

DATES IMPORTANTES

Ouverture des candidatures : janvier 2025

Date des jurys et entretiens : avril 2025

Portes Ouvertes :

14 décembre 2024, 1er février et 15 mars 2025

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



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 GIP CEI / ESTI

02 99 71 60 20

02 99 71 60 24

admissions@gip-cei.com



www.gip-cei.com