IFALP
Institut Français des Achats et de la Logistique Publics

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 2 : MANAGER MLAI

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

Option Cybersécurité et Cyberdéfense

En partenariat avec le Pôle d'Excellence Cyber

LIEUX DE FORMATION
EPF Engineering School - 55, avenue du Président Wilson, 94230 CACHAN
Plate-forme industrielle de recherche LIFE
de l'ICAM Grand Paris Sud - Carré Sénart - 34 Points de Vue, 77127 LIEUSAINT

Alternance, formation continue

TITRE RECONNU PAR L'ÉTAT

BAC +5 | MASTÈRE 2 | TITRE RNCP DE NIVEAU 7

MANAGER LOGISTIQUE ET ACHATS INDUSTRIE

Option : Cybersécurité et Cyberdéfence

FRANCE compétences CERTIFICATION enregistrée au RNCP

Cette formation conduit à l'obtention du titre de niveau 7 « Manager Logistique et Achats Industrie», 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).

2025 Prix de Lancement de Programme EDUNIVERSAL

PRIX DE LANCEMENT DE PROGRAMME

au classement des meilleurs Masters, MS et MBA 2025

RESPONSABLE DE FORMATION

Thibault FERRAND

Responsable de la filière cybersécurité et cyberdéfense

tferrand@gip-cei.com

PROGRAMME (PRÉVISIONNEL)

	Fondamentaux	Spécialité Cybersécurité et Cyberdéfense
GÉRER LA CONTINUITÉ DES OPÉRATIONS DE PRODUCTION ET DE LOGISTIQUE	• Cybersécurité des systèmes industriels • Protection et administration sécurisée des systèmes numériques et des bases de données • Traçabilité des opérations et accessibilité des systèmes numériques • Gestion des accès	• Management des vulnérabilités liées à la transition numérique • Audit de sécurité des systèmes industriels • Gestion du maintien en condition opérationnelle (MCO) et de sécurité (MCS)
SÉCURISER ET OPTIMISER LES PROCESSUS LOGISTIQUES	• Méthodologie de gestion de projet en cybersécurité • Mise en oeuvre des solutions de sécurité adaptées à la chaîne d'approvisionnement • Normes, référentiels et réglementations (RGPD, ISO 27001, Directive NIS 2, LPM etc.)	• Zero trust et défense en profondeur • 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
DÉPLOYER DES PRATIQUES NUMÉRIQUES DURABLES	• Sensibiliser aux enjeux de la cybersécurité dans le contexte de la maîtrise de la chaîne d'approvisionnement • Détection, collecte et analyse des marqueurs de compromission • Analyse de la robustesse des systèmes d'intelligence artificielle RSE	• Traitement et remédiation des incidents • Menaces cyber associées à la digitalisation des processus industriels • Cartographie des installations et analyse de risque sur un système industriel automatisé • Investigation numérique et analyse de malware
PILOTER L'ORGANISATION DES ACHATS ET DE LA CHAÎNE DE FOURNISSEURS	• Gestion des achats de technologies • Audits de sécurité des fournisseurs • Gestion des risques liés à la cybersécurité sur la filière achat • Analyse de marché de la cybersécurité	• Simulation d'évaluation des risques fournisseurs • Mise en place d'une chaîne d'alerte • Méthodologie de recherche d'information en source ouverte (OSINT) • Blockchain et investigation économique
PROTÉGER LES INFRASTRUCTURES ET SYSTÈMES DE TRANSPORT FACE AUX CYBERMENACES	• Sécurisation des communications et données mobiles, chiffrement • Protection des infrastructures de transports	• Analyse de la menace (CTI) et défenses des systèmes connectés et émergents
ACCOMPAGNER LA TRANSFORMATION NUMÉRIQUE DE L'INDUSTRIE	• Projet technique d'innovation	• Challenges, CTF • Thèse professionnelle sur les sujets d'innovation en cybersécurité

OBJECTIFS

Dans un monde où les chaînes d'approvisionnement deviennent des cibles stratégiques, la sécurité des systèmes industriels et logistiques constitue un enjeu majeur pour garantir la souveraineté économique, la résilience des organisations et la compétitivité des nations. L'interconnexion croissante des environnements IT, OT et IoT, alimentée par l'automatisation, l'intelligence artificielle et plus généralement, les technologies numériques, s'accompagne de risques multidimensionnels (cyberattaques, disruptions logistiques, conflits réglementaires). Face à ces défis, l'IFALP propose une formation multidisciplinaire pour outiller les futurs experts capables de répondre aux enjeux de sécurité des chaînes d'approvisionnement critiques. Ces compétences s'étendent à toutes les étapes de la supply chain – achats, production, transport, distribution – pour en faire des leviers de compétitivité et de résilience face aux menaces contemporaines.

Ce programme vise à former des cadres et experts en cybersécurité, capables de :
- Assurer la sécurisation des systèmes industriels et logistiques ;
- Conduire des audits de sécurité sur des environnements IT, OT, IoT et industriels ;
- Maîtriser l'analyse de risques en identifiant les vulnérabilités spécifiques aux chaînes d'approvisionnement ;
- Déployer des méthodologies et des outils avancés pour protéger les flux logistiques et les infrastructures ;
- Maîtriser l'aspect normatif (ISO 2700x, NIS2, LPM…) ;
- Concevoir une campagne d'achat dans un environnement sécurisé ;
- Piloter la résilience des organisations en concevant et testant des plans de continuité et de reprise d'activité ;
- Intégrer les enjeux de durabilité et de conformité pour sécuriser les transitions numérique et écologique des chaînes logistiques.

DÉBOUCHÉS

PERSPECTIVES D'EMPLOI

• Administrateurs réseaux et systèmes ICS / Scada / IT / OT
• Fonctions d'expertise : auditeur, intégrateur, formateur en cybersécurité
• Spécialiste de l'investigation numérique et de la réponse à incident
• Gestion des risques et analyse de la menace
• Ingénieur et chef de projet en cybersécurité industrielle

CALENDRIER (ANNÉE TYPE)

Centre de formation | Entreprise | Soutenance | Férié

2024

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

2025

Janvier			Février			Mars			Avril			Mai			Juin			Juillet			Août		
1 M		1	1 S			1 S			1 M			1 J		18	1 D			1 M			1 V		
2 J			2 D			2 D			2 M		14	2 V			2 L			2 M		27	2 S		
3 V			3 L			3 L			3 J			3 S			3 M			3 J			3 D		
4 S			4 M			4 M			4 V			4 D			4 M		23	4 V			4 L		
5 D			5 M		6	5 M		10	5 S			5 L			5 J			5 S			5 M		
6 L			6 J			6 J			6 D			6 M			6 V			6 D			6 M		32
7 M			7 V			7 V			7 L			7 M		19	7 S			7 L			7 J		
8 M		2	8 S			8 S			8 M			8 J			8 D			8 M			8 V		
9 J			9 D			9 D			9 M		15	9 V			9 L			9 M		28	9 S		
10 V			10 L			10 L			10 J			10 S			10 M			10 J			10 D		
11 S			11 M		7	11 M		11	11 V			11 D			11 M		24	11 V			11 L		
12 D			12 M			12 M			12 S			12 L			12 J			12 S			12 M		
13 L			13 J			13 J			13 D			13 M		20	13 V			13 D			13 M		33
14 M		3	14 V			14 V			14 L			14 M			14 S			14 L			14 J		
15 M			15 S			15 S			15 M		16	15 J			15 D			15 M			15 V		
16 J			16 D			16 D			16 M			16 V			16 L			16 M		29	16 S		
17 V			17 L			17 L			17 J			17 S			17 M			17 J			17 D		
18 S			18 M		8	18 M		12	18 V			18 D			18 M		25	18 V			18 L		
19 D			19 M			19 M			19 S			19 L			19 J			19 S			19 M		
20 L		4	20 J			20 J			20 D			20 M		21	20 V			20 D			20 M		34
21 M			21 V			21 V			21 L			21 M			21 S			21 L			21 J		
22 M			22 S			22 S			22 M			22 J			22 D			22 M			22 V		
23 J			23 D			23 D			23 M		17	23 V			23 L			23 M		30	23 S		
24 V			24 L			24 L			24 J			24 S			24 M			24 J			24 D		
25 S			25 M		9	25 M		13	25 V			25 D			25 M		26	25 V			25 L		
26 D			26 M			26 M			26 S			26 L			26 J			26 S			26 M		
27 L			27 J			27 J			27 D			27 M			27 V			27 D			27 M		35
28 M		5	28 V			28 V			28 L			28 M		22	28 S			28 L			28 J		
29 M						29 S			29 M		18	29 J			29 D			29 M		31	29 V		
30 J						30 D			30 M			30 V			30 L			30 M			30 S		
31 V						31 L						31 S						31 J			31 D		

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 proposé sur 2 ans.

Formation disponible en VAE

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

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 systématique, 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).

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.

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

DURÉE

Les périodes de cours représentent une durée totale de 490h (14 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