

Share



Email destinataire :

Vous devez renseigner un email valide

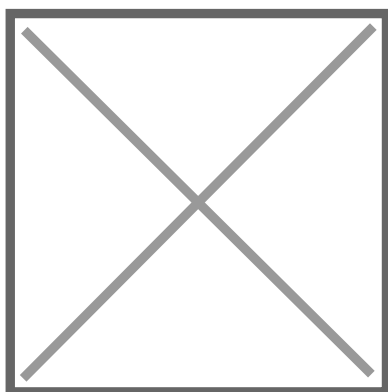
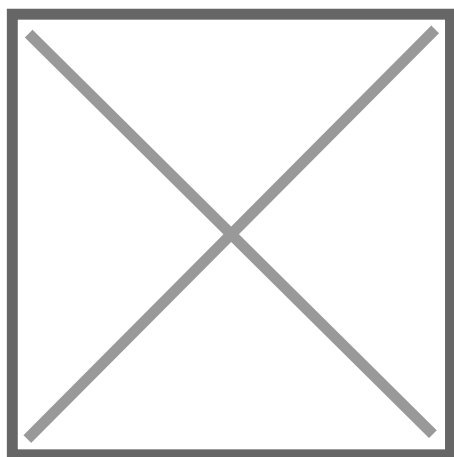
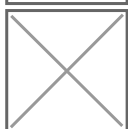
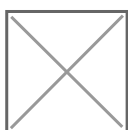
Envoyer

Une erreur est survenue. Merci de réessayer ultérieurement

Le mail de partage a bien été envoyé.

Add to Compare

M2 Ingénierie de Réseaux et des Systèmes - voie Cybersécurité - Apprentissage



Master's degree

Specialisation Computer Science

Enrolment type

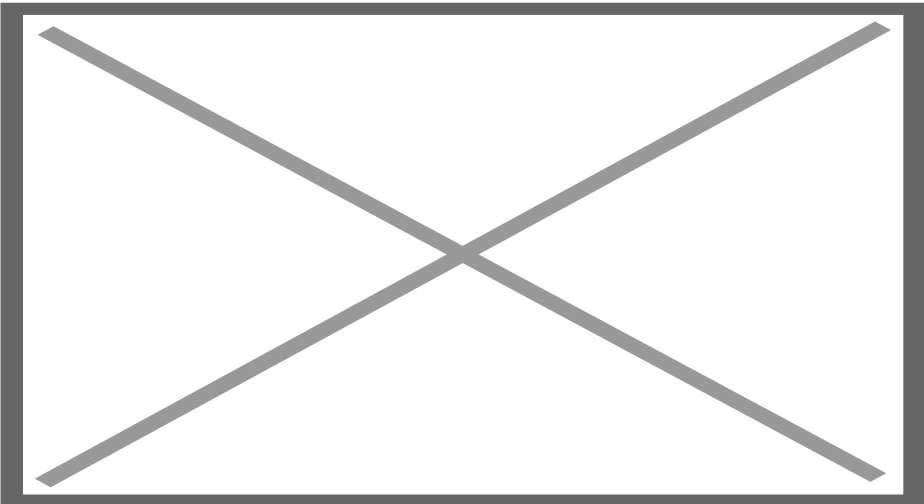
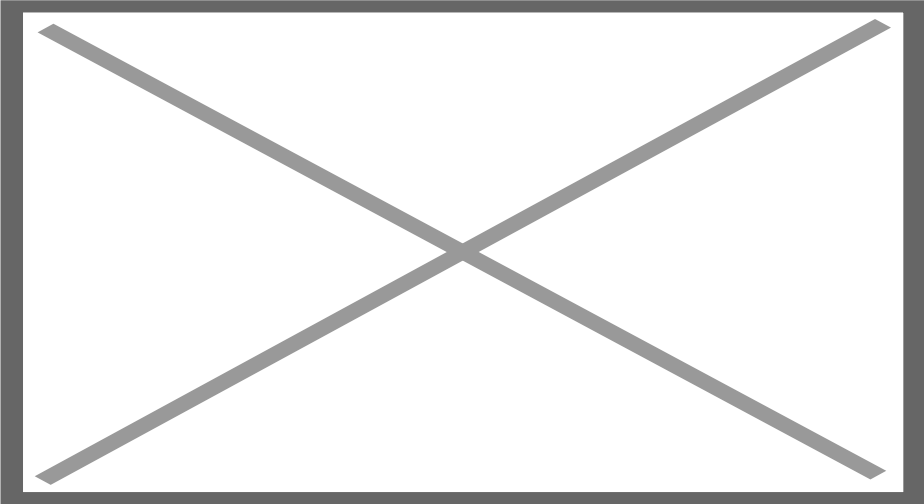
Professional training contract Work-study programme

Language(s) of instruction

French

[Télécharger la fiche détaillée](#)

[Apply Now](#)





■ ■

Information

- [Overview](#)
- [Application requirements](#)
- [Schedule](#)

Présentation

Calendar

Start of programme (indicative date)

14/09/2026

End of programme (indicative date)

31/08/2027

Admission

Capacity

Available Places

Période(s) de candidature

Inception Platform

From 30/01/2026 to 30/06/2026

Supporting documents

Compulsory supporting documents

Motivation letter.

All transcripts of the years / semesters validated since the high school diploma at the date of application.

Curriculum Vitae.

Additional supporting documents

VAP file (obligatory for all persons requesting a valuation of the assets to enter the diploma).

Supporting documents :

- Residence permit stating the country of residence of the first country
- Or receipt of request stating the country of first asylum
- Or document from the UNHCR granting refugee status
- Or receipt of refugee status request delivered in France
- Or residence permit stating the refugee status delivered in France
- Or document stating subsidiary protection in France or abroad
- Or document stating temporary protection in France or abroad.

Programme

Bloc 1 : Vie de l'entreprise et gouvernance

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
Anglais	3	Semestre 1	28	0	0				c

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	----

■

Anglais

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 28

Practical study : 0

Directed study: 0

Tutored project 0

Project : 0

Independant learning: 0

Language(s) of instruction

Anglais

Remote teaching

non

Learning objectives

L'objectif du module est d'être capable de présenter oralement et de rédiger, en anglais, un projet technique. Les trois axes principaux du module sont : la consolidation et l'approfondissement des outils grammaticaux, l'apprentissage du lexique tant technique que général et l'étude de la langue fonctionnelle. De nombreux supports documentaires écrits, oraux et visuels extraits des actualités techniques ou non sont utilisés.

Overall organisation

Cours

Type of assessment

Evaluation Continue non Intégrale

[Management de la cybersécurité](#)

3	Semestre 1	14	14	0
---	------------	----	----	---

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	----

Management de la cybersécurité

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 14

Practical study : 0

Directed study: 14

Tutored project 0

Project : 0

Independant learning: 0

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Ce module vise à définir les règles de sécurité tactiques et opérationnelles, telles que la mise en place des contrôles appropriés, et les rôles et responsabilités de chacun. Elle assure de ce fait une mise en conformité aux normes applicables et une cohérence dans la mise en œuvre du cadre normatif.

Type of assessment

Evaluation Continue non Intégrale

Cybersécurité et le Marché	3	Semestre 1	18	18
--	---	------------	----	----

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	----

■

Cybersécurité et le Marché

ECTS : 3
Semester: Semestre 1
Detail
Lecture: 18
Directed study: 18
Language(s) of instruction
Français
Remote teaching
non
Learning objectives

Une étude des solutions de la cybersécurité et leurs impacts sur le marché.

Type of assessment
Evaluation Continue non Intégrale

Bloc 2 : La sécurité opérationnelle

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
Remise à niveau	3	Semestre 1		48					

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	---

■

Remise à niveau

ECTS : 3

Semester: Semestre 1

Detail

Directed study: 48

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Remise à niveau : obtenir les prérequis dans l'informatique, les réseaux, les systèmes et la sécurité

Overall organisation

TD

Type of assessment

Evaluation Continue non Intégrale

Sécurité by design	3	Semestre 1	12	12
------------------------------------	---	------------	----	----



Sécurité by design

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 12

Directed study: 12

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

La « sécurité par la conception » désigne un produit tel qu'un logiciel dont la sécurité et la notion de risque sont au cœur de sa conception. Cette approche permet d'augmenter la sécurité du produit/projet pour le protéger de potentielles menaces en réduisant les risques de failles. L'idée n'est donc plus de renforcer un système seulement en cas de défaillance comme cela pouvait se faire auparavant, mais bien de prévenir ces risques. Cette approche de secure by design se généralise donc : bon nombre de logiciels et de systèmes créés aujourd'hui intègrent la sécurité et le risque dans leur conception. Lors de la création d'un tel produit, un travail doit être mené pour identifier ses vulnérabilités, ses risques et les contrôles nécessaires afin d'anticiper de potentielles défaillances. Une fois la conception terminée, l'architecture logicielle doit être préservée tout au long de l'exploitation du système.

Dans ce module : Une étude de cas sera menée dans le cadre d'un TP : sécurité by design (menaces, risques, => homologation)

Overall organisation

Cours + TD

Type of assessment

Evaluation Continue non Intégrale

Sécurité des Infrastructures	3	Semestre 1	12	12
--	---	------------	----	----

Sécurité des Infrastructures

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 12

Directed study: 12

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

sécurité des Infrastructures (des réseaux, systèmes et le cloud) : Dans ce module la sécurité de l'infrastructure des réseaux, des systèmes d'Info SI sera abordée avec une optique cloud. Cela se fera comme suit :

1. Identifier les vulnérabilités
2. Mise en place de solutions

Partie 1 : la sécurité de l'infrastructure des réseaux

: Les réseaux informatiques sont constamment soumis à un nombre grandissant de menaces. Chaque entreprise peut être la cible de ces attaques c'est pourquoi il est primordial de s'équiper de plusieurs systèmes permettant de renforcer la sécurité des installations informatiques. Contre ces attaques, des mesures de sécurité spécifiques sont nécessaires : réduction de la surface d'attaque, segmentation du réseau, chiffrement des communications, sensibilisation des utilisateurs aux attaques d'ingénierie sociale, principe du moindre privilège, monitoring des logs, etc. Des audits de sécurité ou des tests d'intrusion sont également un bon moyen de détecter les failles existantes sur votre réseau informatique afin de les corriger.

Partie 2 : La sécurité des SI : c'est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information.

Partie 3 : Vers la cloudification des réseaux et systèmes : sécurité dans le cloud

la sécurité dans le Cloud est la cybersécurité dédiée à la sécurisation des systèmes informatiques et réseaux dans le Cloud. Elle vise

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	directed study/practical class
Sécurité des systèmes ICS	3	Semestre 1	28						

Sécurité des systèmes ICS

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 28

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

- Découvrir ce que sont les systèmes de contrôle industriel (ICS)
- Comprendre les dépendances systèmes et réseaux des ICS
- Appréhender les principes de la cybersécurité (DICT) et le cycle de vie des ICS
- Appréhender les vecteurs d'attaques des ICS
- Découvrir comment assurer la sécurité des ICS

Type of assessment

Evaluation Continue non Intégrale

Bloc 3 : Audit, résilience et gestion de crise

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	directed study/practical class
Détection et réaction	3	Semestre 1	12	12					



Détection et réaction

ECTS : 3
Semester: Semestre 1
Detail
Lecture: 12
Directed study: 12
Language(s) of instruction
Français
Remote teaching
non
Learning objectives

Savoir détecter et traiter les cyberattaques.
La Cyber-défense permet de désigner tous les systèmes mis en place au niveau d'un réseau informatique pour le protéger d'attaques de cybercriminels. (iso 22301)
Ce module permet de qualifier une approche synthétique de la cyber-défense :

- Surveiller toutes les couches du système d'information (données et applications).
- Détecter tous les incidents de sécurité, qu'ils soient liés à un problème technique, humain ou environnemental.
- Réagir face à un incident en prenant en compte toutes les informations liées à l'événement et en y remédiant en s'appuyant sur une procédure liant le traitement technique et organisationnel de l'incident.

Partie 1 : Surveillance et Cyber-défense
Partie 2 : Gestion de crise & résilience

Overall organisation

Cours + TD

Type of assessment
Evaluation Continue non Intégrale

[Investigations numériques](#) 3 Semestre 28
1

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
■									

Investigations numériques

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 28

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Analyse médico-légale après un crime informatique

Overall organisation

Cours

Type of assessment

Evaluation Continue non Intégrale

Audits de sécurité	3	Semestre 1	14	14
------------------------------------	---	------------	----	----

■

Audits de sécurité

ECTS : 3

Semester: Semestre 1

Detail

Lecture: 14

Directed study: 14

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Audit de maturité des mesures de sécurité déployées
par l'organisation Conception d'une roadmap d'amélioration de la sécurité du système d'information

Type of assessment

Evaluation Continue non Intégrale

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	di
Exploitation des canaux auxillières	3	Semestre 2	28						
■									

Exploitation des canaux auxillières

ECTS : 3

Semester: Semestre 2

Detail

Lecture: 28

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Appréhender les différentes techniques liées aux attaques side channel: Fondamentaux en Sécurité Embarquée ; Exemples de composants pour la sécurité; Fuite d'informations sensibles; Machine Learning et SCA; Attaques par fautes et rétroconception hardware.

Overall organisation

Cours

Type of assessment

Evaluation Continue non Intégrale

[Cryptologie post quantique](#)

3 Semestre 2 28

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	discovery
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	-----------

Cryptologie post quantique

ECTS : 3

Semester: Semestre 2

Detail

Lecture: 28

Language(s) of instruction

Français

Remote teaching

non

Prerequisites

Avoir de bonnes connaissances en Mathématiques.

Avoir de bonnes connaissances générales en informatique et en sécurité des systèmes d'information.

Learning objectives

- Connaitre les nouvelles règles en matière de cryptologie quantique
- Appréhender la cryptologie quantique et ses algorithmes principaux
- Savoir expliquer / vulgariser la cryptologie quantique

Overall organisation

Cours

Type of assessment

Evaluation Continue non Intégrale

Bloc 4 : Pratique de métiers

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	discovery
Projet école	3	Semestre 2	0	50	0				

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	dis
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	-----

Projet école

ECTS : 3

Semester: Semestre 2

Detail

Lecture: 0

Practical study : 0

Directed study: 50

Tutored project 0

Project : 0

Independant learning: 0

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

L'objectif du cours est la connaissance des fondamentaux du processus de conduite de réalisation d'un lot au sein d'un projet dans le domaine des services réseaux. Le module est constitué de trois cas pratiques couvrant les phases d'architecture, de sécurité et d'intégration. A la fin de ces trois cas pratiques, les participants ont appris par la pratique les différentes techniques de conduite : l'analyse et la décomposition d'un système (WBS), la planification, l'estimation, la gestion des risques, le suivi de projet et les indicateurs.

Type of assessment

Evaluation Continue non Intégrale

[Stage en](#)

[entreprise et](#)

[mémoire](#)

[professionnel](#)

21

Semestre

2

1

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	discovery/practical class
■									

Stage en entreprise et mémoire professionnel

ECTS : 21

Semester: Semestre 2

Detail

Directed study: 1

Project : 0

Language(s) of instruction

Français

Remote teaching

non

Learning objectives

Le stage en entreprise est constitué de deux périodes :

une première période d'une durée de deux mois qui permet le démarrage d'une première mission (participation à une étude ou à un travail de spécification, administration et exploitation de réseaux, ...). une seconde période de cinq mois demandant une plus grande autonomie soit dans la continuité de la première mission (déploiement et intégration) soit dans un cadre de réalisation différent.

La restitution du travail effectué en entreprise se fait à travers une soutenance orale et un rapport écrit.

Overall organisation

Stage

Type of assessment

Evaluation Continue Intégrale

Teaching Location(s)

CACHAN

GUYANCOURT

Contact

- **Mourad GUEROUI**

<http://www.universite-paris-saclay.fr/formation/master/informatique/m2-ingenierie-de-reseaux-et-des-systemes-voie-cybersecurite-apprentissage>