CFA EVE CENTRE DE FORMATION UNIVERSITAIRE EN APPRENTISSAGE

**BAC +6**
**MASTERE SPECIALISÉ**
**Code RNCP : 36855**

version : janvier 2025

# Mastère spécialisé Cybersécurité des Infrastructures et des Données

**Type de contrat**
Contrat d'apprentissage

**Durée de la formation**
12 mois
440 heures
**ECTS* :** 75
*Système européen de transfert et d'accumulation de crédits

**Formation délivrée par**
TELECOM SudParis — INSTITUT POLYTECHNIQUE DE PARIS

## Objectifs

L'objectif de cette formation est de répondre aux exigences de la gouvernance de la sécurité dans les entreprises avec une approche globale couvrant tous les aspects de la cybersécurité : techniques, méthodologiques, organisationnels et réglementaires.

Ce Mastère Spécialisé permet d'acquérir les compétences nécessaires à l'élaboration et la mise en place d'un plan de sécurité destiné à la protection des ressources vitales de l'entreprise, contre les attaques internes et externes. En particulier :

- Conduire un projet de cybersécurité
- Analyser et traiter les problématiques de cybersécurité spécifiques aux Opérateurs de Services Essentiels
- Analyser les menaces réseau et les mécanismes de sécurisation
- Analyser les vulnérabilités et sécuriser des applications informatiques
- Auditer un système d'information
- Déployer des services d'authentification, de chiffrement et de protection de la vie privée dans un système d'information

Les participants sont préparés à prendre en charge un poste d'expert en cybersécurité dès la sortie de formation.

## Accès au diplôme

**Pour postuler à la formation**, les candidats doivent satisfaire aux conditions d'admission suivantes :

- Être titulaire d'un diplôme bac+5 français ou d'un diplôme étranger équivalent ou d'un diplôme bac+4 avec au moins 3 ans d'expérience professionnelle dans le domaine.
- Avoir de bonnes connaissances de base en systèmes, réseaux et programmation Maîtriser le français (niveau C1) et l'anglais technique (B2)

**La procédure d'admission est la suivante :**

- Dossier de candidature
- Test en ligne sur les prérequis techniques + Entretien par visio ou téléphone
- Jury d'admission

Les conditions de candidature et de recrutement sont définies précisément dans le Règlement d'admission et disponibles sur le site de Télécom SudParis : https://www.telecom-sudparis.eu/formation/mastere-specialise-cybersecurite/

**Candidatures** : de novembre 2024 à mi- juin 2025 à *admissions-ms@telecom-sudparis.eu*

## Rythme d’alternance

• 1 semaine de formation sur le campus / 2 semaines en entreprise, de septembre 2025 à avril 2026

• Temps plein en entreprise de mai à fin août 2026

• Soutenance début septembre 2026

**Modalités pédagogiques :** Méthodes mobilisées : L'acquisition des compétences et des connaissances se fait au travers de cours magistraux, de travaux dirigés, de travaux pratiques, de travaux de groupe et de mises en situation professionnelle.

## Contacts

**Responsable pédagogique :** Christophe KIENNERT - Christophe.kiennert@telecom-sudparis.eu

**Contact administratif :** Séverine TROTOU - severine.trotou@telecom-sudparis.eu - Tél : 01 60 76 42 14

**Contact CFA EVE :** Chargé(e) des relations entreprises : PUJOL Adeline - a.pujol@cfa-eve.fr - Tél : 01 60 79 54 07 / Référent(e) handicap : DARRAC Elodie - e.darrac@cfa-eve.fr - Tél : 01 60 79 54 00 / En savoir +

## Lieu(x) de formation

**TELECOM SudParis - PALAISEAU**
19 place Marguerite Perey
91120 PALAISEAU

# Programme de la formation

### Fondamentaux Réseaux IP

**30h**

- Rappels TCP/IP
- Vulnérabilités TCP/IP
- Lecture de trames - Wireshark
- Introduction à la cryptographie
- TP IP
- SMTP
- TP sécurité réseau
- Filtrage

### Fondamentaux systèmes

**30h**

- Cours Intro Processus Synchro
- TD OS synchro
- Cours OS mem/secu/int/syscall + TD Gestion mémoire
- Cours shell + TP Shell
- TP Shell
- Cours Langage C
- TP C (fichier texte)
- TP C (listes dynamiques)
- Programmation système Unix
- TP Backdoor
- TP Buffer Overflow

### Évaluation des risques et détection des attaques

**45h**

- Introduction to Security Operations

- Blueteam CTF Challenge (Qradar 101)
- Forensics
- Vulnerability Discovery and Exploitation
- Pentesting (Web Application)
- Risk Management (EBIOS RM)
- Intrusion Detection Systems
- Blueteam CTF Feedback
- PIA and GDPR
- Pentesting Feedback

## Authentification, VPN et chiffrement

**45h**

- Security protocols and VPN
- Fundamental cryptography
- IPsec lab
- Electronic certificate lab
- Database anonymization
- Security architectures
- Protocol flaws
- PKI & IAM

## NET6533 – Filtrage

**45h**

- Introduction to filtering architectures
- Lab: Filtering in an AWS environment
- Filtering at layer 2/layer 2.5
- Lab:Layer 2, Layer 2.5 filtering
- Mechanisms and algorithms for filtering systems
- Lab: DPI
- Network Address Translation
- Lab: NAT and applications
- Lab: Checkpoint NGFW

## NET6534 - Sécurité des applications et des services

**45h**

- System calls
- Unix security
- Frama-C
- Windows internal security
- Graded hands-on exercise
- Document security
- CTF

## NET6535 – Projet de cybersécurité

**60h**

- Présentation des projets
- Travaux en groupes projet
- Suivi de projet

## NET6536 - Cybersécurité des systèmes industriels

**40h**

- Introduction aux systèmes industriels
- Sécurité des systèmes industriels
- Etude de cas - Tunnel virtuel
- Norme IEC 62443 - Gouvernance
- Norme IEC 62443 - Aspects techniques
- Internet des drones
- IA for CPS security
- Etude de cas - Santé
- Sécurité des conteneurs maritimes
- ITS - Vehicule autonome

### NET6537 - Aspects juridiques et réglementaires de la cybersécurité

**40h**

- Droit de la Sécurité des Systèmes d'Information
- Certification
- GPDR and NIS directive
- Gestion du cycle de vie de la donnée
- Suivi de projet
- Soutenances

### NET6538 - Cycle de conférences / visites d'entreprise

**30h**

- Conférences industrielles et visites
- Suivi de projet

### Mission et Thèse professionnelle

**5 mois**

• Mission en entreprise

• Tutorat de mission

• Rédaction de la thèse professionnelle

• Tutorat de thèse

• Soutenance devant jury

## Blocs de compétences

**Analyser et traiter les problématiques de cybersécurité spécifiques aux Opérateurs de Services Essentiels**

- Analyser les besoins en cybersécurité des systèmes industriels et des Opérateurs de Services Essentiels dans le cadre de la loi du 26 février 2018 transposant la directive NIS (3) au droit français et dans le respect des obligations requises par l'ANSSI ;

- Proposer et déployer une solution technique répondant aux besoins et aux contraintes d'un Opérateur de Service Essentiel, c'est-à-dire conforme aux 23 règles de sécurité à appliquer dans les 4 domaines que sont : la gouvernance de la sécurité des réseaux et systèmes d'information, la protection des réseaux et systèmes d'information, la défense des réseaux et systèmes d'information et la résilience des activités ;

- Identifier les réglementations des cadres juridiques français et européen qui s'appliquent dans des situations concrètes liées à la cybersécurité, notamment au sein des Opérateurs de Services Essentiels ;

- Déterminer le rôle et les missions des acteurs cybersécurité de l'entreprise pour organiser efficacement la gestion et la mise en œuvre de solutions, en tenant compte de personnel avec un handicap.

- Étude de cas portant sur une problématique technique spécifique aux Opérateurs de Services Essentiels

- Étude de cas + soutenance visant à traiter des problématiques techniques et juridiques rencontrées par des entreprises

- Rapport écrit visant à cartographier les métiers et les pratiques de la cybersécurité au sein des opérateurs de services essentiels

**Conduire un projet de cybersécurité**

- Établir et analyser l'état de l'art associé à une problématique de cybersécurité afin d'en déterminer les enjeux et de concevoir une contribution scientifique permettant d'y répondre

- Concevoir un prototype répondant à un cahier des charges et permettant de traiter la problématique identifiée en argumentant les choix réalisés

- Réaliser et déployer un prototype de la solution permettant d'évaluer sa faisabilité technique afin de s'assurer que la solution réponde fonctionnellement au cahier des charges

- Un projet est à mener sur un sujet de cybersécurité avec livrable de dossiers et soutenance orale devant jury

**Analyser les menaces réseau et les mécanismes de sécurisation**

-Identifier les différents types d'attaques portant sur le réseau ainsi que les mécanismes de sécurité permettant de faire face à chacun de ces types d'attaques afin de mettre en œuvre les mécanismes de sécurité les plus efficaces face aux menaces identifiées

- Mettre en œuvre les règles de filtrage appropriées afin de bloquer des attaques réseau sans entraver le fonctionnement des applications

- Configurer et tester un pare-feu nouvelle génération (NGFW) afin de mettre en place une politique de sécurité qui vise à protéger un réseau interne tout en filtrant l'accès à certains services pour les utilisateurs de ce réseau interne

- Cas pratiques

**Analyser les vulnérabilités et sécuriser des applications informatiques**

- Analyser les vulnérabilités classiques des systèmes d'exploitation et des applications informatiques, identifier les solutions permettant d'y remédier

- Mettre en œuvre des mécanismes de contrôle d'accès et d'isolation de fichiers sur un système Unix afin d'empêcher des attaques en confidentialité et en intégrité sur ces fichiers

- Analyser une vulnérabilité du noyau Linux pouvant conduire à une élévation de privilèges afin de déterminer les correctifs à apporter

- Cas pratiques et étude de cas

**Auditer un système d'information**

- Identifier les risques, découvrir les vulnérabilités afin d'évaluer la sécurité du système d'information

- Appliquer la démarche d'analyse de risque EBIOS et employer les outils d'audit d'un réseau afin de professionnaliser la démarche d'audit d'un SI

- Concevoir des règles pour la détection d'intrusion dans le contexte d'un centre de sécurité opérationnelle (SOC) afin de réduire le niveau d'exposition des SI aux risques externes comme internes

- Élaborer une méthodologie de réponse à incident pour faire face à des intrusions réelles afin de plus rapidement et efficacement réagir en cas d'attaques

- Auditer une application Web et rédiger un rapport d'audit afin d'identifier les vulnérabilités web

- Cas pratique, étude de cas, mise en situation pratique

**Déployer des services d'authentification, de chiffrement et de protection de la vie privée dans un système d'information**

- Établir les besoins en chiffrement et en authentification dans l'architecture d'un système d'information afin de garantir la confidentialité des données sensibles et de certifier l'identité des utilisateurs de manière robuste

- Générer des certificats numériques X.509 et déployer une infrastructure à clés publiques (PKI) afin de mettre en œuvre des connexions sécurisées en HTTPS

- Configurer et déployer un réseau privé virtuel (VPN) IPsec entre deux sites distants afin de déterminer les options adéquates à utiliser pour répondre aux différents besoins, notamment en confidentialité et en authentification

- Mettre en œuvre des mécanismes d'anonymisation des bases de données afin d'assurer la conformité avec le RGPD

# Public concerné

## Contrat d’apprentissage

- Avoir moins de 30 ans à la date de début du contrat,
- **et** être de nationalité française, ressortissant de l’UE, ou étranger en situation régulière de séjour et de travail.

La formation est gratuite pour l'alternant.

### Qui peut accueillir un jeune en contrat d’apprentissage ?

- **Toute personne physique ou morale de droit privé, assujettie ou non à la taxe d’apprentissage :** les entreprises, les sociétés civiles, les groupements d’intérêt économique, les associations…
- **Toute personne morale de droit public dont le personnel ne relève pas du droit privé :** l’État, les collectivités territoriales, les établissements publics…

# Marche à suivre

**1.** Candidater via le site du CFA, www.cfa-eve.fr ou directement auprès des écoles / universités partenaires concernées.
**2.** Rechercher activement une structure d’accueil et répondre aux offres de nos partenaires.
**3.** L’inscription n’est définitive qu’à la signature du contrat d’apprentissage.



**AGESUP A EVRY – CFA EVE**
48, cours Blaise Pascal
91025 EVRY-COURCOURONNES Cedex
Tél. : 01 60 79 54 00 - cfa@cfa-eve.fr - www.cfa-eve.fr
UAI : 0912119J – SIRET : 402 924 849 00027