



Ecole du leader
européen de la
Cybersécurité

Recruter les
spécialistes de
demain en
cybersécurité du
Groupe



Parcours Orange
Security School

Accompagner
les expertises et
les compétences
essentiels en
cybersécurité
du Groupe

Orange Security School

Une école du groupe au service des compétences stratégiques

Cybersécurité, Cyberdéfense & Confiance Numérique



Les parcours diplômants & certifiants internes



#1

**Analyste en
Cybersécurité**

#2

**Master Sécurité
informatique,
cybersécurité
et cybermenaces**

#3

**Master of
Science in
Cybersecurity**

#4

**Executive
Master
in Cybersecurity**

#5

**Accompagnement
Certifications**



Nos partenaires académiques



Avec une histoire qui remonte à plus de cent trente ans, **TU Dublin est un pionnier de l'enseignement supérieur technologique**, nos anciens élèves jouant un rôle important dans l'innovation, le développement économique et social, la culture et l'éducation en Irlande et à l'échelle internationale.

With a history stretching back over one hundred and thirty years, **TU Dublin is a pioneer of technological higher education** with our alumni playing important roles in innovation, economic and social development and culture and education both in Ireland and internationally.

Master of science in Cybersecurity

17 Apprenants déjà diplômés

le cnam

Promouvoir la recherche et l'innovation

Le Cnam met en œuvre une politique scientifique ambitieuse dans de nombreux domaines d'excellence, en collaboration avec des partenaires nationaux, européens et internationaux. L'établissement investit dans les spécialités des sciences humaines et sociales, des sciences de gestion et des sciences pour l'ingénieur. Les enseignants-chercheurs sont engagés dans la recherche fondamentale, indispensable aux innovations futures et à la recherche appliquée.

Master Sécurité informatique,
cybersécurité et cybermenaces

Ingénieur Spécialité informatique
Parcours Cybersécurité

Analyste en Cybersécurité

250 Apprenants déjà diplômés



Une expertise reconnue dans la formation professionnelle pour les cadres et les dirigeants.

L'École polytechnique associe recherche, enseignement et innovation au meilleur niveau scientifique et technologique. Sa formation promeut une culture d'excellence à forte dominante scientifique, ouverte sur une grande tradition humaniste. L'École forme des femmes et des hommes responsables, capables de mener des activités complexes et innovantes pour répondre aux défis actuels et à venir de la société.

Executive Master in Cybersecurity

27 Apprenants en cours

Les parcours diplômants & certifiants



Upskilling & Reskilling

Analyste en Cybersécurité

le cnam



1 an

1,5 jour / semaine



Certificat de compétence



Niveau Bac +2



Inscriptions
fév. - juin



Démarrage
octobre



Sur poste
100% distanciel



3 000€

Upskilling & Reskilling

Master Sécurité informatique, cybersécurité et cybermenaces

le cnam



1 ou 2 ans

2 jours / semaine



Titre RNCP
niveau 7



Niveau Bac +3



Inscriptions
fév. - juin



Démarrage
octobre



Sur poste
100% distanciel



8 000€

Upskilling

Master of Science in Cybersecurity



2 years

2 days / week



Master
of Science



Bachelor's
degree



Applications
february to june



Start in
october



Workplace
100% online



8 500€

Upskilling

Executive Master in Cybersecurity



1 an

2 jours / semaine



Executive
Master



Niveau
Bac +4/5



Inscriptions
fév. - juillet



Démarrage
novembre



Sur poste
100% distanciel



14 500€

Upskilling & Reskilling

Accompagnement Certifications



CISM



CISSP



CEH



ISO 27001

...offre complète...



Ouvert toute
l'année

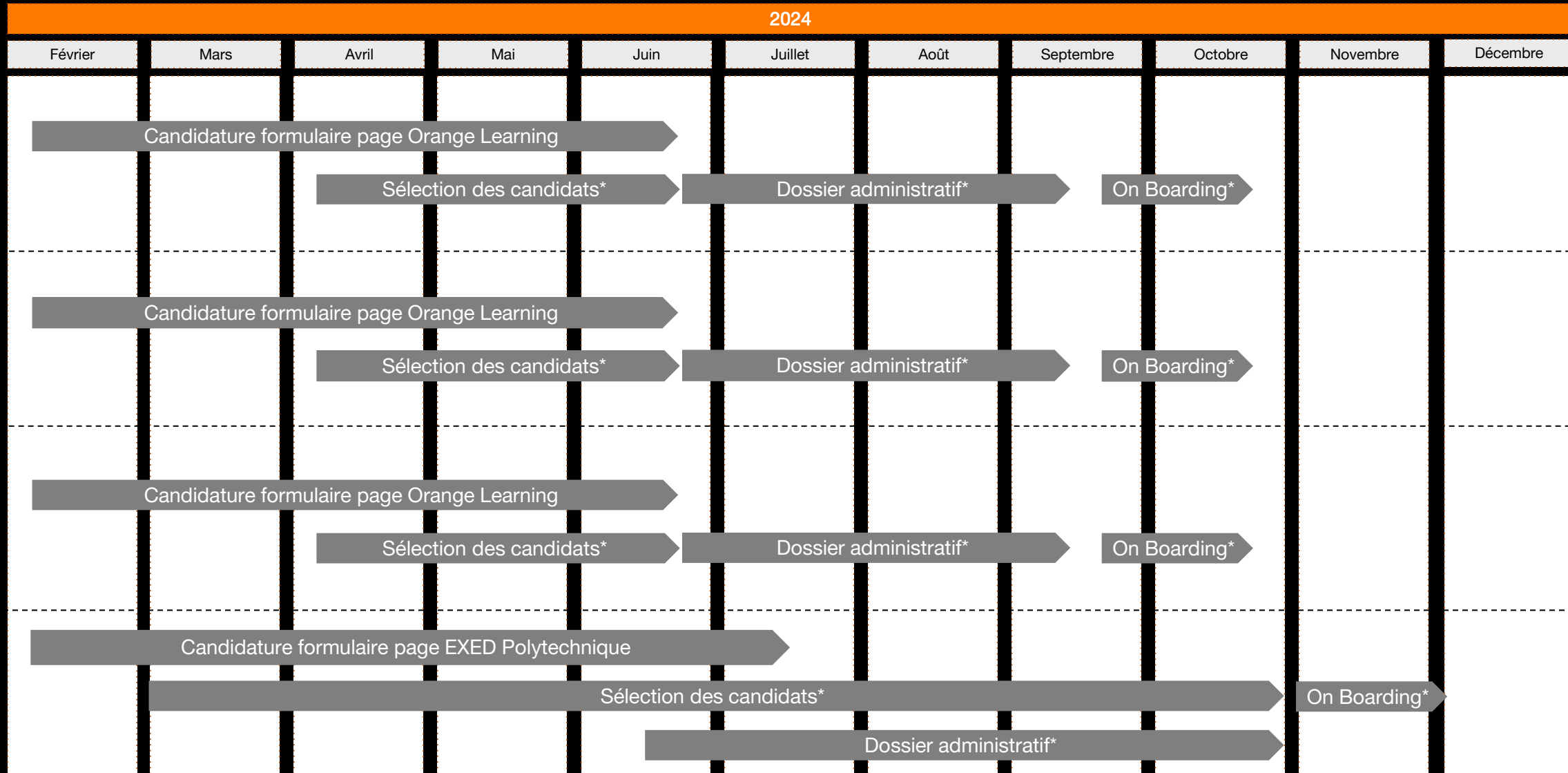


E-learning



Selon offre

La roadmap des parcours diplômants & certifiants



* Sélection : vérification prérequis, test de sélection, entretien de sélection, validation REDC/Manager/RRH

* Dossier administratif : mobilisation CPF, inscription partenaire académique

* On Boarding : séminaire de rentrée, rentrée académique

Analyste en Cybersécurité

le cnam



1 an

1,5 jour / semaine



Certificat de compétence



Niveau Bac +2



Inscriptions
fév. - juin



Démarrage
octobre



Sur poste
100% distanciel



3 000€

Parcours ouvert en Upskilling & Reskilling

Au cœur des équipes en charge de produits et de services Orange ou dans la filière Cyber, ce parcours apporte l'expertise nécessaire à la protection et la défense des services et/ou des clients.

Permet à des techniciens ou ingénieurs de prendre en charge des opérations de sécurité des SI en connaissant les référentiels et les techniques élémentaires.

Objectifs pédagogiques

Acquérir les bases théoriques et pratiques qui l'aideront à être plus opérationnel dans le domaine de la sécurité.

Pour qui

- Salariés déjà en poste et ayant besoin de monter en compétences sur le sujet, ou le salarié ayant un souhait de mobilité vers les métiers de la sécurité.
- Profil technique (DBis, E) ayant une appétence pour la sécurité.

Contenu

- 1 séminaire de rentrée en octobre en distanciel
- 4 Unités d'Enseignement (UE) de 50h :
 - Architectures des systèmes informatiques [NSY104](#)
 - Architectures et bonnes pratiques de la sécurité... [SEC105](#)
 - Menaces IT et codes malveillants : analyse et lutte [SEC102](#)
 - Cybersécurité : référentiel, obj. et déploiement [SEC101](#)
- 1 séminaire de clôture en juillet en distanciel



Candidature

Formulaire d'inscription accessible sur la page [Orange Learning](#)

Validation pré-candidature par le REDC (Responsable Emplois et Compétences), RH et Manager
Mobilisation du CPF

Master Sécurité informatique, cybersécurité et cybermenaces

le cnam



1 ou 2 ans

2 jours / semaine



Titre RNCP
niveau 7



Niveau Bac +3



Inscriptions
fév. - juin



Démarrage
octobre



Sur poste
100% distanciel



8 000€

Parcours ouvert en Upskilling & Reskilling

Le programme de la 1ère année de Master permet d'aborder les menaces associées à la criminalité informatique, d'en comprendre les motivations et les stratégies à partir de l'étude de la posture de l'attaquant, comment se préparer aux attaques et comment y réagir.

La 2ème année approfondit les notions abordées en 1ère année et permet de couvrir les domaines liés aux différents métiers Cyber.

Objectifs pédagogiques

L'objectif est de se spécialiser dans la mise en œuvre des mesures techniques et non techniques permettant la défense de systèmes d'informations essentiels.

Pour qui

- Salariés déjà en poste et ayant besoin de monter en compétences sur le sujet, ou le salarié ayant un souhait de mobilité vers les métiers de la sécurité.
- Profil technique (DBis, E, F) ayant une appétence pour la sécurité

Contenu

- 1 séminaire de rentrée en octobre en présentiel
- **Accès en M1**
 - Tronc Commun
 - Lutte contre la criminalité
 - Compréhension de la menace
 - Anglais
- **Accès en M2**
 - Notions avancées de cyber sécurité
 - Conception et maintien d'un SI sécurisé
 - Homologation d'un SI
 - Réaction aux attaques
- Cyber exercice Gestion de crise en juin



Candidature

Formulaire d'inscription accessible sur la page [Orange Learning](#)

Validation pré-candidature par le REDC (Responsable Emplois et Compétences), RH et Manager
Mobilisation du CPF

Master Sécurité informatique, cybersécurité et cybermenaces

Les contenus détaillés

le cnam

M1

Anglais professionnel [ANG330](#)
Introduction générale à la Criminologie [CRM201](#)
Introduction à la gestion de données à large échelle [NFE115](#)
Spécification et vérification des systèmes distribués [NFP103](#)
Intelligence artificielle [NFP106](#)
Evaluation de performances et sûreté de fonctionnement [RCP103](#)
Conception et urbanisation de services réseau [RSX103](#)
Sécurité des réseaux [RSX112](#)
Droit, enjeux de sécurité, conformité [SEC103](#)
Systèmes et applications répartis pour le Cloud [SMB111](#)

le cnam

M2

Etude de la posture de l'attaquant [USCB10](#)
Ingénierie sociale et OSINT [USCB11](#)
Hacking réseau [USCB12](#)
Gérer la sécurité et piloter les projets de sécurité [USCB13](#)
Détection des attaques [USCB14](#)
Sécurisation avancée des données [USCB15](#)
Homologation de sécurité [USCB16](#)
Audit de sécurité technique [USCB17](#)
Réagir à une attaque Cyber [USCB18](#)
Analyse d'un système après incident [USCB19](#)
Introduction à la rétro conception et l'analyse de Malware [UACB1A](#)
Mémoire de fin d'étude [UACB06](#)

Master of Science in Cybersecurity



2 years

2 days / week



Master
of Science



Bachelor's
degree



Applications
february to june



Start in
october



Workplace
100% online



8 500€

Training Path open on Upskilling

At the heart of the teams in charge of Orange products and services or in the Cyber sector, provides the expertise necessary to protect and defend services and/or customers.

Enables engineers or technicians to take on IS security positions anywhere in the world with an internationally recognized degree

Learning objectives

At the heart of the teams in charge of Orange products and services or in the Cyber sector, provides the expertise needed to protect and defend services and/or customers.

Enables engineers or technicians to take up IS security positions anywhere in the world, with an internationally recognized diploma.

For who

- Employees already in post who need to upgrade their skills in this area, or employees wishing to move into the security sector.
- Being bilingual
- Technical profile (E, F) with an appetite for Cybersecurity

Content

- 1 distance learning Training Path Launch on september
- 10 Academic courses de 10 à 30h [link Program](#) :
 - Digital Forensics
 - Secure Communications & Cryptography
 - Network Security
 - Research Skills and Ethics
 - Cyber Crime Malware
 - Business Continuity Management
 - Research project
- 1 distance learning closing seminar in July on the second year
- 1 face-to-face graduation ceremony in Dublin in November on the second year



Admission process

Registration form available on the [Orange Learning page](#)
Managerial and HR agreement

Executive Master in Cybersecurity



1 an

2 jours / semaine



Executive Master



Niveau
Bac +4/5



Inscriptions
fév. - juillet



Démarrage
novembre



Sur poste
100% distanciel



14 500€

Parcours ouvert en Upskilling

Il s'agit d'un programme complet pour les futurs cadres de haut niveau en lien avec la sécurité informatique et les activités où la protection des données et de la vie privée est essentielle. S'adapter aux nouvelles menaces et trouver de nouveaux moyens de défense sera votre défi quotidien. Vous développerez votre capacité à gérer les équipes dans un environnement complexe en situation de crise.

Ce parcours vous permettra l'obtention d'un diplôme d'établissement polytechnique.

Objectifs pédagogiques

Appréhender les technologies pour la convergence numérique et l'interopérabilité. Définir la stratégie de la gouvernance et de la conformité de la sécurité d'une organisation. Assurer la sécurité opérationnelle et la cyberdéfense des services, produits et systèmes.

Pour qui

- Professionnels du secteur de l'informatique ayant un minimum de 5 années d'expérience professionnelle, qui sont en prise de poste ou qui ont la responsabilité de la cybersécurité.
- Profil technique (E, F, G) ayant une appétence pour la sécurité

Contenu

- 1 séminaire de rentrée en distanciel en novembre
- Bloc commun 4 enseignements de 60h Programme :
 - Fondamentaux techniques
 - Convergence technologique et interopérabilité / Enjeux et veille
 - Management de projet
 - Communication et Leadership
 - Self-leadership et Communication en situation de crise
- Option 1 Gouverneur de 2 enseignements de 75h
 - Elaborer la stratégie de la gouvernance
 - Piloter la gouvernance et la conformité
- Option 2 Architecte de 2 enseignements de 75h
 - Concevoir les architectures de sécurité
 - Piloter la sécurité opérationnelle
- Cyber exercice Gestion de crise en présentiel en novembre N+1



Candidature

Formulaire d'inscription accessible sur la page [Orange Learning](#)

Validation pré-candidature par le REDC (Responsable Emplois et Compétences), RH et Manager
Mobilisation du CPF

Accompagnement des certifications

Pour la réussite de votre projet de formation



CISM



CISSP



CEH



ISO 27001

...offre complète...



Ouvert toute l'année



E-learning



Selon offre

Renforcer vos compétences avec des certifications à la clé

Vous êtes motivé pour développer vos compétences ou bien assoir votre expertise technique par une certification reconnue.

Nous vous proposons une offre accompagnée avec un accès aux contenus en e-learning, un forum dédié et une communauté d'experts.

Etape 1

Candidature via le **formulaire d'accompagnement**

Etape 2

Contact par Orange Security School

Etape 3

Accès aux outils (Plateforme Percipio / Communauté...)

Des démarrages au fil de l'eau, des contenus diversifiés (vidéos, livres, LAB, test de niveau...).

Orange Security School

Merci

orange.securityschool@orange.com

