


# MASTÈRE 1 et 2 - Tech et data spécialité Cybersécurité

Titre RNCP "Ingénieur systèmes, réseaux et cybersécurité", Titre certifié de niveau 7, code NSF 326, enregistré au RNCP par décision de France compétences le 18/10/2023, délivré par AFORP FORMATION

En  
alternance  
ou initial

  
Formats  
**HYBRIDE 60% / 40% OU  
ONLINE TUTORÉ 100%**

  
Rythme  
**4 JOURS en entreprise  
/ 1 JOUR à l'école**

  
Rentrée  
**SEPTEMBRE  
OCTOBRE 2024**

  
**TITRE  
RECONNU  
PAR L'ÉTAT**

## Tech et data pour quoi faire ?

Les derniers constats écologiques et la crise du Covid imposent aux entreprises du monde entier de nouvelles priorités en intégrant de nouvelles obligations : utilisation responsable de l'informatique, sobriété énergétique, intégration des dynamiques locales et globales...

Nos objectifs de restauration et de préservation des ressources imposent désormais de mettre la Tech au service du bien commun.

Les besoins sont aujourd'hui innombrables. Grâce à nos 5 spécialités (Data et IA, Web3, cybersécurité, développement et cloud computing) notre école se distingue par son engagement à former des experts dans les domaines de la Tech, devant anticiper les besoins cruciaux de notre ère numérique, tout en considérant les enjeux écologiques.

## LES + DE NOTRE PROGRAMME

- Des certifications éditeurs **intégrées** au programme (Microsoft, Opquast, Oracle)
- Un programme conçu **avec les recruteurs et les entreprises**
- Une pédagogie immersive par projets avec **des cas pratiques proposés par les entreprises**
- Une mise en situation **professionnelle** unique
- Un enseignement qui intègre **les nouveaux enjeux éthiques**
- et responsables de l'informatique
- Un programme qui **forme aux outils d'intelligence artificielle** pour être plus efficace et productif
- Un accompagnement **personnalisé** tout au long du parcours pour suivre ta progression
- Une formation à **l'entrepreneuriat en partenariat** avec le plus grand incubateur d'Europe, EuraTechnologies

## LES DÉBOUCHÉS

- Pentester
- Consultant cybersécurité
- Architecte cybersécurité
- Directeur de projet informatique
- Directeur du système informatique
- Chief information security
- Ingénieur en cybersécurité
- SOC manager (security operation center)
- Auditeurs en sécurité

**65 Mds**  
d'euros : chiffre d'affaires 2023 de l'industrie numérique en France\*

**12,55 Mds**  
USD : prévision marché français de la cybersécurité d'ici 2028\*\*

**4,26 Mds**  
d'euros : montant des levées de fonds 2023 dans la Tech en France\*\*\*



## OBJECTIFS PÉDAGOGIQUES

- Maîtriser la cryptanalyse avancée, les architectures de sécurité sophistiquées, et les protocoles de sécurité de nouvelle génération
- Étudier les menaces émergentes, notamment les attaques par ransomware, l'espionnage cybernétique, et les campagnes de désinformation
- Maîtriser la protection des infrastructures critiques, y compris les réseaux de télécommunication, les systèmes de contrôle industriel, et les services cloud
- Concevoir des systèmes de défense capables de contrer des attaques avancées et persistantes
- Explorer la gestion des risques dans des environnements complexes et data-centric
- Comprendre et naviguer dans le paysage mondial de la conformité, en se concentrant sur des réglementations telles que le GDPR, le CCPA, et d'autres normes internationales
- Développer des compétences en gestion de crise et en réponse aux incidents à grande échelle
- Élaborer des plans de continuité des activités et de récupération après sinistre
- Explorer les implications de l'intelligence artificielle et du machine learning en matière de cybersécurité
- Aborder les défis spécifiques liés à la sécurité dans les environnements cloud hybrides et multi-cloud



## COMPÉTENCES VISÉES

- **Gérer un projet** international
- **Recueillir et analyser** les exigences du client

■ **Concevoir l'architecture, réaliser et déployer** la solution technique

■ **Maintenir le système** en condition opérationnelle et de sécurité



## NOTRE PÉDAGOGIE

■ Apprendre en étant **connecté au monde des entreprises**

■ Des secteurs d'activité choisis pour leur **excellent taux d'employabilité**

■ Tous **nos diplômes reconnus par l'État**

■ **Modèles agiles** : 100% online tutoré ou hybride : 60% en distanciel (cours synchrones), 40% en présentiel

**100%**

Online

ou

**60%**

En distanciel

**40%**

En présentiel

- Des **classes virtuelles tutorées** (200 intervenants professionnels reconnus dans chacun de leur domaine)
- Tous les jours, **des étudiants à disposition de l'ensemble des apprenants**
- **L'accompagnement des étudiants** au cœur de notre performance pédagogique
- Des **semaines intensives autour de projets** en groupe
- L'étudiant valide des compétences par des **projets réels apportés par de grandes marques** (+ de 300)
- Des cours au sein de **nos campus dans des espaces de coworking** modernes
- Du **reverse mentoring** pour apprendre auprès des adultes plus seniors

## NOS CAMPUS : PARIS • LILLE • DIJON • LYON • SAINT-ÉTIENNE • MONTPELLIER



## FINANCEMENT

- Formation en initial
- Formation en alternance
- Formation en contrat de professionnalisation



## PRÉREQUIS

Être titulaire d'un Bac+3 ou niveau équivalent (Titre RNCP niveau 6)



Headn Éducation te propose **2 années pour construire ton projet professionnel en Tech et data spécialité Cybersécurité.**

**Le programme de sécurité informatique est conçu pour les étudiants visant une maîtrise approfondie des techniques de cybersécurité**, incluant l'audit, les tests d'intrusion, et l'analyse de malwares. Ce parcours offre une compréhension avancée des méthodes pour sécuriser les systèmes d'information et protéger les données critiques.

Avec un focus sur l'identification proactive des menaces et la gestion des vulnérabilités, tu développeras des compétences essentielles pour maintenir l'intégrité, la sécurité des systèmes et des réseaux dans un environnement numérique en constante évolution.

Tu seras formé pour devenir un spécialiste capable de détecter, analyser et contrer les attaques informatiques, tout en assurant la conformité et la protection des infrastructures.

**À travers des projets pratiques, tu exploreras des domaines tels que la détection avancée de vulnérabilités, la sécurité proactive des systèmes, l'analyse Forensic et la sécurité offensive.** Tu te prépareras également à des certifications professionnelles reconnues, telles que CEH et OSCP, élargissant ainsi tes compétences et ton employabilité.



## PROGRAMME

### Mastère 1 - Cybersécurité

#### ■ Sécurité technique pour un numérique éthique

- Python pour la sécurité éthique : utilisation avancée de Python pour développer des solutions de sécurité éthiques et efficaces
- Stratégies proactives de détection des intrusions : techniques avancées pour détecter et prévenir les intrusions de manière proactive
- Computer Forensic pour la justice numérique : exploration des techniques de Forensic pour enquêter et analyser les incidents de sécurité
- Linux administration sécurisée : gestion avancée des systèmes Linux avec un accent sur la sécurité et la responsabilité
- Rust pour la sécurité système et réseau : utilisation de Rust pour développer des systèmes et réseaux sécurisés
- Reverse engineering pour la défense : techniques de reverse engineering pour comprendre et contrer les menaces
- Sécurité des IoT pour un avenir connecté : stratégies pour sécuriser les dispositifs IoT dans notre monde connecté
- Cisco CCNA security pour l'expertise réseau : formation avancée pour obtenir la certification CCNA Security
- Hardening et sécurité défensive : techniques avancées pour renforcer et sécuriser les infrastructures informatiques
- OSINT pour une collecte d'informations responsable : utilisation éthique de l'OSINT pour collecter des informations de manière responsable

- Cryptographie avancée pour la protection des données : exploration des techniques avancées de cryptographie pour sécuriser les données

#### ■ Technique pour une sécurité innovante

- Sécurité des cartes bancaires pour la confiance : techniques pour sécuriser les transactions par cartes bancaires
- Assembleur x64 pour une compréhension profonde : exploration avancée de l'assembleur x64 pour une compréhension approfondie de la sécurité
- Sécurité RFID et radio pour un monde connecté : stratégies pour sécuriser les communications RFID et radio
- Sécurité Shellcode pour une défense avancée : techniques pour comprendre et contrer les Shellcodes malveillants

#### ■ Fonction pour une gouvernance éclairée

- EBIOS Risk-Manager pour une gestion des risques : formation pour devenir un gestionnaire de risques éclairé avec EBIOS
- ISO 27001 : Lead implementer pour la conformité : stratégies pour mettre en œuvre et gérer la conformité ISO 27001
- Gouvernance et sécurité des SI pour un leadership éclairé : approches pour une gouvernance éclairée et sécurisée des systèmes d'information

#### ■ Soft skills

- Communication professionnelle pour innovateurs : développement de compétences en communication adaptées au monde professionnel moderne et conscient



## PROGRAMME

## Mastère 2 - Cybersécurité

### ■ Sécurité technique pour un numérique éthique

- Sécurité système Windows avancée : stratégies avancées pour sécuriser les systèmes Windows contre les menaces modernes
- Analyse Forensic de malwares : techniques pour analyser et comprendre les malwares pour une meilleure prévention
- Audit et test d'intrusion éthique : formation avancée pour réaliser des audits et tests d'intrusion responsables
- Sécurité réseau avancée : stratégies pour renforcer la sécurité des réseaux contre les intrusions
- Linux sécurité avancée : techniques avancées pour sécuriser les systèmes Linux
- Gestion avancée de l'identité et des accès : stratégies pour gérer efficacement l'identité et les accès dans un environnement numérique
- Sécurité cloud responsable : approches pour sécuriser les environnements cloud tout en restant responsable

### ■ Technique pour une cybersécurité innovante

- Blue team : gestion des SIEM, formation sur les systèmes de gestion des informations et des événements de sécurité pour une défense proactive
- Sécurité offensive responsable : techniques avancées pour une approche offensive éthique de la sécurité
- Préparation à la certification OSCP : formation pour la certification offensive security certified professional
- Red team : intrusion éthique, stratégies pour les équipes red team dans une approche éthique et responsable
- Sécurité des systèmes industriels SCADA : approches pour sécuriser les systèmes industriels contre les cybermenaces
- Sécurité des drones : stratégies pour sécuriser les drones et les systèmes associés
- Exploitation avancée de binaires : techniques pour comprendre et sécuriser les binaires contre les exploitations

### ■ Fonction pour une gouvernance éclairée

- Préparation à la certification CISA : formation pour la certification certified information systems auditor
- Préparation à la certification CISSP : formation pour la certification certified information systems security professional
- Lead auditor ISO 27001 : stratégies pour mener des audits conformes à la norme ISO 27001
- Gestion de risques ISO 27005 : approches pour gérer les risques informatiques conformément à la norme ISO 27005
- Réponse à incidents et gestion de crise : stratégies pour répondre efficacement aux incidents de sécurité et gérer les crises

### ■ Soft skills

- Leadership en management d'équipe : développement de compétences en leadership pour gérer des équipes de sécurité efficacement
- Droit, éthique et cybercriminalité : compréhension des aspects légaux et éthiques de la cybersécurité pour une pratique responsable

