# Mastère Spécialisé® Expert en Cybersécurité

https://competencesplus.utt.fr/
/

**Université de technologie de Troyes - Compétences +**

## Durée de la formation

5 blocs de compétences de 70h + Stage de 4 à 6 mois

## Stage(s)

Oui, obligatoires

## Langues d'enseignement

- Français

## Modalités

- Présentiel

## Renseignements

**Christine Champeau**
christine.champeau@utt.fr
03 25 71 56 31
https://ecandidat.utt.fr/

Devenez un expert de l'analyse des systèmes compromis et de la sécurité des dispositifs informatiques.

## Présentation

La formation cybersécurité




Avec des compétences techniques pointues sur les systèmes d’information, l’expert cybersécurité **collecte, identifie, analyse et interprète les différentes cybermenaces possibles**, quels que soient les dispositifs touchés (ordinateurs, téléphones mobiles, objets connectés, systèmes industriels). Il définit et met en œuvre une stratégie de sécurité des systèmes d’information pour éradiquer les menaces, en prévention ou en réaction à celles rencontrées.

Cette **formation cybersécurité** permet dans un premier temps de développer une compréhension

des environnements techniques et technologiques dans lesquels opèrent aujourd'hui les entreprises ; dans un deuxième temps, elle permet de pouvoir sécuriser le SI grâce à l'acquisition de compétences techniques et méthodologiques de pointe. La formation aborde les **aspects techniques, fonctionnels et juridiques de la SSI**, apportant des connaissances approfondies des techniques d'audit de sécurité et de sécurisation. Elle permet en outre de pouvoir mener des **analyses forensiques**.

Avec l'utilisation
d'Internet au quotidien, les entreprises deviennent les proies potentielles de menaces et autres codes malveillants. Le **Mastère Spécialisé® "Expert en Cybersécurité"** répond à un besoin fort des entreprises pour lesquelles les compétences purement SSI ne réussissent plus à assurer une sécurité optimale des diverses infrastructures informatiques.

Le Mastère Spécialisé® "Expert en Cybersécurité" est **accrédité par la Conférence des Grandes Ecoles** et s'adresse à la fois à des étudiants motivés par la Sécurité des Systèmes d'Information, et à des professionnels du domaine qui souhaitent acquérir des **compétences de haut-niveau**, afin de relever efficacement les challenges actuels et futurs de la cybersécurité.

Ce programme bénéficie du **label SecNumEdu** depuis 2017 : il apporte l'assurance aux étudiants et aux employeurs qu'une formation dans le domaine de la sécurité du numérique répond à **une charte et des critères définis par l'ANSSI** en collaboration avec les acteurs et professionnels du domaine (établissements d'enseignement supérieur, industriels, etc.).

Points forts

- Formation unique en France labellisée SecNumedu par l'ANSSI depuis 2017
- Intervenants spécialistes de la cybersécurité
- Des profils rares et recherchés
- Un HackLab pour les expérimentations

Zoom sur le HackLab de l'UTT

**Optez pour l'apprentissage !**

- pour accéder à un Bac+6 d'excellence, gratuit et rémunéré ;
- pour bénéficier d'une année d'expérience de terrain en adéquation avec la formation académique

**Les + apprentissage de l'UTT**

- un accompagnement personnalisé pour la recherche d'entreprise
- un fichier de 3 000 entreprises partenaires, de tous secteurs d'activité, partout en France
- une réputation établie et des expertises reconnues

Partenariats

- Nous sommes membre fondateur de l'association « CECyF » : Centre Expert contre la Cybercriminalité Français
- Nous sommes membre fondateur de l'association Européenne « ECTEG » : European Cybercrime for Training and Education Group
- Nous formons, en association avec la Gendarmerie Nationale, ses Enquêteurs en Technologies Numériques et leurs délivrons la Licence Professionelle Enquêteurs en Technologies Numériques.

Témoignages

**Alexandre**
**Neyret, Direction des Enquêtes de l'Autorité des Marchés Financiers (AMF), Promo 2017**

*"La cybercriminalité est un des sujets majeurs du XXIème siècle et la sphère boursière n'y échappe (ra) pas.*
*Afin d'analyser au mieux cette menace et de mener efficacement les éventuelles investigations forensiques associées aux enquêtes de l'AMF, il apparaissait nécessaire d'approfondir mes connaissances avec une formation adaptée.*
*La variété et la richesse des thématiques abordées dans ce Mastère Spécialisé®, m'a permis d' acquérir une compréhension généraliste de haut niveau, tandis que les nombreux exercices pratiques m'ont fourni les clés pour développer l'indispensable expertise technique. Bref, une formation sur des sujets complexes et à enjeux qui a tenu toutes ses promesses."*

**Marie-Hua, Acheteuse Projet, Promo 2016**
*"Diplômée d'une grande école de commerce et forte de six années d'expérience dans les achats industriels, il m'est apparu évident que la cybersécurité sera l'enjeu essentiel des entreprises. Le Mastère Spécialisé® Expert forensic & cybersécurité et l'équipe pédagogique m' ont donné l'opportunité d'acquérir les compétences nécessaires pour aborder les problématiques et enjeux de la cybersécurité. Cette formation a donné une nouvelle dimension à mon profil."*

**Eric EGEA, Responsable de la Sécurité des Systèmes d'Information (RSSI), Promo 2016**
*"Le Mastère Spécialisé® Expert forensic & cybersécurité propose un programme très dense, riche et pertinent représentant l'état de l'art de ce sujet. L'intervention de professionnels, experts en leur domaine et au contact de la réalité de terrain, est d'une valeur inestimable et fait de ce Mastère Spécialisé®, un outil de formation unique qui se présente comme une véritable référence pour les entreprises. Fier de faire partie de la première promotion."*

# Admission

## Pré-requis

**Formation(s) requise(s)**

- Fondamentaux en informatique
- Fondamentaux en SSI
- Réseau (TCP/IP, topologies, modèle OSI, Cisco ACL)
- SGBD (Requêtes SQL)
- Programmation (algorithmique, Python, Bash)
- Linux, Windows
- Notions de Droit, RGPD.

*Des ressources pédagogiques seront proposées après l'admission.*

## Conditions d'admission

Les candidats devront être titulaires d'un des diplômes suivants dans le domaine de la formation Expert en Cybersécurité :

- Diplôme d'ingénieur habilité par la Commission des Titres d'Ingénieur (liste CTI)
- Diplôme d'une école de management habilitée à délivrer le grade de Master (liste CEFDG)
- Diplôme de 3e cycle habilité par les autorités universitaires (Master, DEA, DESS) ou diplôme professionnel cohérent et équivalent avec le niveau bac+5
- Diplôme de M1 ou équivalent, pour des auditeurs justifiant d'au moins trois années d'expérience professionnelle en informatique décisionnelle

- Titre inscrit au RNCP niveau 7
- Diplôme étranger équivalent aux diplômes Bac+5 français exigés ci-dessus

Pour maximiser les chances d'être accepté(e), les candidat(e)s doivent avoir un niveau cohérent avec les enseignements prodigués durant la formation. Certaines connaissances sont donc pré-requises afin d'être admis(e).

Conditions d’accès dérogatoires

1. Dans la limite de 40 % maximum de l’effectif de la promotion suivant la formation Mastère Spécialisé concernée, sont recevables, après une procédure de Validation des acquis personnels et professionnels (VAPP), les candidatures de personnes justifiant à minima de 10 années d’expérience professionnelle (hors stage, césure, cursus initial en alternance).
2. Par dérogation pour 30 % maximum du nombre d’étudiants suivant la formation Mastère Spécialisé concernée, sont recevables les candidatures d’étudiants titulaires d’un des diplômes suivants :
    - Niveau M1 validé ou équivalent sans expérience professionnelle
    - Diplôme de L3 justifiant d’une expérience adaptée de 3 ans minimum

Le pourcentage total des dérogations prévues au 1) et au 2) ci-dessus ne doit pas excéder 40 %.

## Candidater

Candidatures en ligne, du 1er décembre au 15 juin

Candidater

L’admission est prononcée sur dossier, tests et entretien individuel.

Dans le cas d’une candidature pour l’alternance, l’admission n’est définitive qu’après signature du contrat avec l’entreprise d’accueil.

L’admission prononcée pourra être assortie d’une préconisation d’approfondissements académiques le cas échéant.

**Montant de frais de dossier (hors apprentissage) : 105 €**

Les résultats seront envoyés par e-mail à l'issue de chaque période d'entretien.

# Programme

Organisation des enseignements

Le Mastère Spécialisé® Expert Cybersécurité s’articule autour de **4 blocs de compétences** :

- Traiter les incidents de cybersécurité
- Analyser la menace cyber pesant sur une organisation
- Auditer la sécurité technique d’une organisation
- Réaliser une analyse technico-légale (forensique)

Les enseignements sont répartis sur 10 Unités d'Enseignement (UE), de 35 h chacune, dispensées par des enseignants-chercheurs et des professionnels.

Tableau des enseignements

| | | |
|---|---|---|
| **UE 01** | **Remise à niveau** | Bases de données ; systèm |
| **UE 02** | **Cybersécurité et SHS** | Intelligence économique ; psychologie du cybercrimi |
| **UE 03** | **Analyse de malwares** | Concept de rétro-ingénieri logiciels malveillants |
| **UE 04** | **Audit de sécurité et réponse à incidents** | Aspects légaux ; pen-testir |
| **UE 05** | **Big Data** | Généralités sur le Big Data |
| **UE 06** | **Recherche en sources ouvertes & droit** | Anonymisation ; bases de automatique du web |
| **UE 07** | **Analyse forensique** | Analyse technico-légale de |
| **UE 08** | | Analyse technico-légale de |
| **UE 09** | **Etude des architectures critiques** | Environnements virtualisé |
| **UE 10** | **Etude de cas** | Conférences et travaux en |

Programme détaillé

**Les ++ de la formation**

- chaque année en octobre, les apprenants participent à la Cyberweek UTT (35 h) pendant laquelle des entreprises proposent des challenges cyber aux étudiants
- 17 h d'activités e.learning sont proposées : remise à niveau, anglais, ressources en ligne

**Un seul rythme de formation**

- les enseignements sont dispensés au rythme d'une semaine par mois, de septembre à juillet ; ils alternent avec des semaines en entreprise.
- pour les apprenants en Formation Continue ou Formation Initiale, **exceptionnellement** les enseignements seront dispensés au rythme d'une semaine par mois, d'octobre à juillet

## Période en entreprise et thèse professionnelle

S'il n'est pas apprenti, l'apprenant devra effectuer un stage alterné de 4 mois minimum en entreprise ou dans une administration publique sur une thématique liée à la cybersécurité, réponse à une problématique identifiée. Une durée de 6 mois est recommandée.

Dans tous les cas, l'apprenant produira un rapport et soutiendra une Thèse professionnelle devant un jury à l'issue de son apprentissage ou de sa période en entreprise (septembre).

Compétences visées

- Traiter les incidents de cybersécurité
- Analyser la menace cyber pesant sur une organisation
- Auditer la sécurité technique d'une organisation
- Réaliser une analyse technico-légale (forensique)

https://www.francecompetences.fr/recherche/rncp/40640/#anchor3

Validation possible par bloc de compétence : oui

Modalités de contrôle des connaissances

1. Contrôle continu sous forme de travaux pratiques, tests, devoirs, exposés, etc.
2. Examen intermédiaire (épreuves individuelles écrites ou orales)
3. Exposé oral, rapport (ou thèse) écrit
4. Réalisation, projet
5. Examen final

Méthodes mobilisées

- Cours
- TP : Travaux Pratiques
- TD : Travaux Dirigés
- Projets