Mise à jour Novembre 2022

Public :
Salarié ou demandeur d'emploi

Prérequis :
Conditions d'admission
Les candidats devront être titulaires d'un des diplômes suivants :

- 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

Conditions d'accès dérogatoires :

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).

1. 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

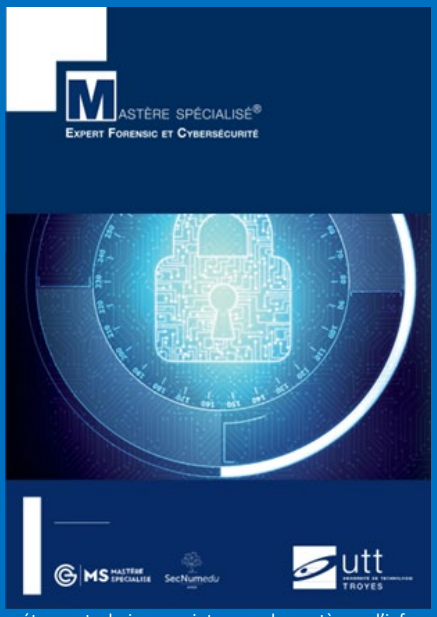
Le pourcentage total des dérogations prévues au 1) et au 2) ci-dessus ne doit pas excéder 40 %.

Modalités et délai d'accès :

Pour Candidater

L'admissibilité 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'admissibilité prononcée pourra être assortie d'une préconisation d'approfondissements académiques le cas échéant.
Montant de frais de dossier : 90 €
Les résultats seront envoyés par courrier et e-mail à l'issue de chaque période d'entretien.

Mastère Spécialisé® Expert Forensic et Cybersécurité
Niveau 7 (Bac+6)
En Formation Continue, en apprentissage, contrat de professionnalisation ou
Par la VAE plus d'infos ici



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 Forensic et 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 Forensic et 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.).

Contact :

formation.continue@utt.fr

Candidater en Mastère Spécialisé

Calendrier :

- Ouverture des admissions : **novembre**
- Rentrée : septembre
- Jurys d'admission : chaque mois de janvier à juin
- Période d'application en entreprise **: 4 mois minimum**
- **Soutenance de la Thèse Professionnelle** en septembre

Durée : 1 an

Rythme de formation

- les enseignements sont dispensés au rythme d'une semaine par mois, de septembre à juin pour les alternants sous Contrat d'Apprentissage ou de Professionnalisation ;
- pour les apprenants en Formation Continue ou Formation Initiale, les enseignements se déroulent en continu de septembre à décembre.

L'apprenant doit effectuer un stage de 4 mois minimum en entreprise ou dans une administration publique sur une thématique liée à la cybersécurité, produire un rapport et soutenir une thèse professionnelle à l'issue de ce stage.

Tarifs :

Coût de la formation

Apprentissage / Contrat de professionnalisation
Formation rémunérée et gratuite pour l'apprenant. Les frais de scolarité sont pris en charge par l'entreprise d'accueil.
Etudiant / Demandeur d'Emploi / Individuel
9 500€
Entreprise
15 500€
Plus d'informations sur l'aide au financement

**Ce tarif est net, l'UTT étant exonérée de la TVA pour ses activités de formation. La participation aux entretiens d'admission nécessite la fourniture du dossier de candidature complet et le règlement des frais de dossiers à minima 1 semaine avant la session d'entretien.*

Méthodes mobilisées :

Les formations de mastère spécialisé® peuvent être organisées suivant un parcours classique : formation en école puis mission en entreprise ou suivant un parcours en alternance école /entreprise.

La durée normale d'études pour une formation de mastère spécialisé® est d'un an.

Objectifs opérationnels – Blocs de Compétences

A l'issue de la formation, l'étudiant sera capable de :

BC 1 - Traiter les incidents de cybersécurité

- Collecter l'ensemble des informations relatives aux incidents informatiques (journaux d'évènements systèmes et réseau, diagrammes de topologie réseau, images systèmes) à l'aide d'outils open-source (autopsy, foremost, scalpel, volatility, plaso, log2timeline, etc.) souvent présents sur la distribution Kali Linux afin d'avoir une première idée sur l'ampleur de la crise.
- Trier les éléments liés à l'incident en les catégorisant afin d'organiser des éléments de preuves analysables
- Analyser les preuves numériques collectées selon la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées permettant d'identifier la nature de l'incident et de reconstituer le déroulement de l'attaque, afin lancer une action interne ou une procédure judiciaire
- Contextualiser l'incident en faisant la corrélation entre signe d'incident et l'analyse de traces informatiques (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation afin d'établir des scenarii potentiels d'incidents
- Élaborer un plan de remédiation afin d'appliquer les actions nécessaires à la résolution de l'incident telles que décrites dans la politique de sécurité des systèmes d'information (PSSI) en émettant notamment des recommandations aux collaborateurs afin de répondre à la crise cyber
- Enrichir la politique de sécurité (PSSI)et des documents associés avec le RSSI et/ou DSI en utilisant les méthodologies d'analyse de risques telles que Méhari ou EBIOS, ainsi que la norme ISO 27001, spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc., afin d'améliorer la sécurité et la résilience du SI
- Améliorer de façon continue ses pratiques en coopérant avec des experts à l'aide des outils de réponse à incident spécifiques (CERT, plateforme de partage, virus total) dans le but de partager les failles, les vulnérabilités, les indices de compromission, et éviter que d'autres structures ne soient affectées par les mêmes menaces

BC 2 - Analyser la menace cyber pesant sur une organisation

- Assurer la supervision des infrastructures et des événements de sécurité en exploitant un système de gestion de l'information et des événements de sécurité (SIEM) et en utilisant ces informations pour retracer la chronologie d'une cyberattaque, pour mettre en évidence les signaux faibles, qui d'ordinaire, passent inaperçus. Cela permettra de mettre à jour de nouveaux risques identifiés, et d'apporter des modifications sur les équipements pour éviter que ces mêmes attaques ne se reproduisent dans le futur
- Détecter en temps réel les incidents et les menaces en identifiant leurs sources afin de bloquer leur accès au système informatique
- Analyser le code malveillant par les techniques d'analyse statique et/ou dynamique pour le qualifier et le catégoriser
- Produire un correctif à l'aide de la distribution Kali Linux (langage python, script bash sous linux, exécutable écrit en C++.) qui sera appliqué par les équipes afin de produire une réponse à incident
- Attribuer l'incident en établissant une grille d'analyse d'intrusion en utilisant les méthodes adéquates : Kill Chain, Diamond Model, la matrice MITRE ATT&CK, afin de modéliser une intrusion ciblée
- Anticiper les futures évolutions des menaces à l'aide de la mise en place d'un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les médias sociaux (SOCMINT), le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web, afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un hacker

Chaque formation comprend au minimum 350 heures d'enseignements théoriques, travaux pratiques et travaux de groupe correspondant à 45 crédits ECTS, suivies d'une période de thèse professionnelle de 4 mois minimum qui donne lieu à la production d'un rapport et à une soutenance et correspondant à 30 crédits ECTS.

Pour les formations en alternance, un calendrier universitaire présente les périodes en entreprise et les périodes en école. Si un étudiant n'a pas validé le parcours de formation après 12 mois de formation (hors semestre annulé ou cursus aménagé), son exclusion peut être prononcée par le Directeur de l'UTT. Il lui est alors délivré une attestation d'études précisant les crédits ECTS obtenus.

L'enseignement est organisé en unités d'enseignement. Une unité d'enseignement correspond à la quantité de travail nécessaire pour l'acquisition de compétences, comprises comme un ensemble intégré et fonctionnel de savoirs, savoir-faire, savoir-être et savoir devenir qui permettront, face à une catégorie de situations, de s'adapter, de résoudre des problèmes et de réaliser des projets.

En particulier, la formation peut comprendre : les sciences et techniques ; découverte de la vie professionnelle et du monde de l'entreprise ; gestion et réalisation de projets à l'université, à l'extérieur, ou à l'étranger ; l'interculturalité et les enjeux sociétaux. Conformément aux recommandations de la Commission européenne sur le système ECTS, à chaque unité d'enseignement est associé des crédits ECTS correspondant à un nombre d'heures de face à face et un nombre d'heures de travail hors encadrement.

Les étudiants ont l'obligation de suivre et de valider un travail personnel préparé dans le cadre d'une mission en milieu professionnel et débouchant sur la soutenance d'une thèse professionnelle, d'une durée comprise entre 4 mois et 6 mois.

Modalités d'évaluation :

Les règles relatives au contrôle des connaissances sont adoptées par le Conseil d'Administration sur proposition du directeur de l'UTT après consultation du CE. Les modalités d'application pratique, propres à chaque Unité d'Enseignement, sont arrêtées par le directeur de l'UTT au plus tard un mois après le début du semestre, sur proposition du responsable de l'UE. Les modalités de contrôle des connaissances doivent comprendre au minimum deux moyens de contrôle. En général, le contrôle des connaissances peut tenir compte de certains des moyens suivants :
contrôle continu sous forme de travaux pratiques, tests, devoirs, exposés, etc. ;
examen(s) intermédiaire(s), épreuves individuelles écrites ou orales ;
examen final ; exposé oral, rapport écrit ; réalisation, projet ; évaluation du niveau d'acquisition de compétences identifiées. Les étudiants doivent impérativement se présenter aux dates d'examen qui leur auront été préalablement communiquées.

Equivalences, passerelles, suites de parcours, débouchés pour Mastère Spécialisé® Expert Forensic et Cybersécurité

Fonctions occupées :

Les diplômés de cette formation cybersécurité peuvent exercer différentes fonctions :

- Auditeur, contrôleur, évaluateur en cybersécurité
- Post-auditeur en cybersécurité

➢ BC 3 - Auditer la sécurité technique d'une organisation

- Analyser le périmètre d'intervention des tests d'intrusion (après avoir défini le périmètre d'intervention, et la modalité des tests à utiliser, les outils de la distribution Kali Linux seront utilisés, tels que nmap, metasploit et armitage) afin de lancer des tests cadrés
- Réaliser des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles en utilisant les outils adéquats selon la méthodologie de tests d'intrusion (définition du plan d'audit, des scenarii, etc.), tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion en respectant le Code pénal spécifique à la cybercriminalité, les articles 323-1 et suivants notamment, afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions
- Élaborer un rapport détaillé des résultats des tests comprenant des captures d'écran des tests et, systématiquement, une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre-mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation

➢ BC 4 - Réaliser une analyse technico-légale (forensique)

- Identifier le périmètre et l'environnement technique, en accédant si nécessaire au système d'exploitation ou au matériel pour avoir une vision précise de la volumétrie des données afin d'évaluer la quantité de données à acquérir
- Définir la stratégie de préservation des données (en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes) afin de rédiger le document de traçabilité des actions effectuées
- Réaliser la collecte de façon technico-légale à l'aide d'outils de collecte dédiés soit en extrayant les données sur un support de type clé USB, ou bien, soit en réalisant une copie technico-légale avec des outils open source, tels que dd, dcfldd, présents sur la distribution Kali Linux, ou bien des outils commerciaux comme ftk imager, afin de préserver les preuves numériques
- Analyser des artefacts identifiés (disque dur, mémoire, traces réseaux, journaux d'évènements, e-mail, navigateurs, smartphones…) afin de tracer les preuves numériques
- Rédiger un rapport d'analyse en adaptant son discours afin de le présenter à divers publics, techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents)

Programme

Le Mastère Spécialisé® Expert Forensic & 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.

- Opérateur en cybersécurité
- Intégrateur en cybersécurité
- Formateur, instructeur en cybersécurité
- Expert en sécurité des systèmes d'information
- Expert des tests d'intrusion
- Analyste cybersécurité
- Consultant cybersécurité
- Spécialiste en gestion de crise
- Responsable de la sécurité des systèmes

Types d'entreprises concernées :

- Grands groupes industriels
- Secteur bancaire
- Entreprises publiques
- Administrations

Possibilité de valider un/ou des blocs de compétences : Oui
Equivalences, passerelles :
Lien Fiche RNCP France Compétences Mastère Spécialisé EFC
Suite de parcours : doctorat en informatique accessible selon parcours antérieur

Accessibilité aux personnes en situation de handicap :
Les étudiants en situation de handicap doivent s'identifier auprès du pôle santé, et de la référente handicap étudiant : emeline.lambert@utt.fr
Seul le personnel médical est autorisé à voir ou conserver vos documents médicaux.

Indicateurs de résultats de la formation issus de la promotion 2021
Taux d'obtention certification : 90%
Insertion professionnelle
Taux net d'emploi : **100 %**

CDI : **100 %**

Statut cadre : **100 %**

Salaire moyen : **56,2 k€ brut annuel**
Classement : 4ème sur meilleurmaster.com
https://www.meilleurs-masters.com/master-cybersecurite-securite-des-systemes-et-protection-des-donnees/utt-universite-de-technologie-de-troyes-mastere-specialise-expert-forensic-et-cybersecurite.html
Mention Très Bien avec 8.41/10 de satisfaction

Tableau des enseignements :

UE 01	**Remise à niveau**	Bases de données ; systèmes d'exploitation ; cryptographie ; langage de programmation
UE 02	**Cybersécurité et SHS**	Intelligence économique ; aspects légaux de la cybersécurité en entreprise ; psychologie du cybercriminel ; anglais intensif
UE 03	**Analyse de malwares**	Concept de rétro-ingénierie et aspects légaux ; analyse statique et dynamique de logiciels malveillants
UE 04	**Audit de sécurité et réponse à incidents**	Aspects légaux ; pen-testing ; réponse à incidents et gestion de crise
UE 05	**Big Data**	Généralités sur le Big Data ; outils d'analyse ; corrélations d'évènements ; SIEM
UE 06	**Recherche en sources ouvertes**	Anonymisation ; bases de vulnérabilités ; analyse des réseaux sociaux ; surveillance automatique du web
UE 07	**Analyse forensique**	Analyse technico-légale de matériel informatique
UE 08		Analyse technico-légale de matériel téléphonique et réseau
UE 09	**Etude des architectures critiques**	Environnements virtualisés et stockages ; sécurité des systèmes SCADA
UE 10	**Etude de cas**	Conférences et travaux en groupes

Moyens mis à disposition par l'UTT

Moyens humains :
Des formations qui s'appuient sur l'expertise d'enseignants-chercheurs, investis dans les laboratoires et les chaires de l'UTT, et qui répondent aux besoins de compétences des entreprises.
Moyens techniques :
Un campus XXL :
2 halles industrielles de 2 200 m2
2 000 m2 de bibliothèque
5 000 m2 de laboratoires et plateformes de recherche
4 000 m2 dédiés aux activités sportives
1 antenne à Nogent (52)
L'UTT se situe au centre d'un campus et écosystème favorables à l'innovation, avec, à moins d'1 kilomètre, l'IUT, la Technopole de l'Aube en Champagne et son Young entrepreneur center et 3 autres écoles : l'EPF, l'ESTP et Y Schools.
Avec 11 000 étudiants, Troyes est une ville attractive pour les jeunes qui poursuivent des études supérieures.