Université de Paris

Master Informatique – Parcours : Cybersécurité et esanté

SCIENCES, TECHNOLOGIES, SANTÉ

Présentation

La numérisation accélérée des entreprises et organismes de santé se traduit par : la dématérialisation massive des systèmes d'Information vers le cloud, l'explosion de l'internet des objets (IoT) dans un monde tout connecté accessible en mobilité avec smartphone, tablettes…, l'accumulation des données provenant des utilisateurs dans le Big Data. Dans ce contexte, les exemples de cyberattaques en lien avec la transformation digitale sont de plus en plus nombreux. Ce qui oblige les organisations à repenser leur approche de la Cybersécurité, dans un cadre règlementaire de plus en plus contraignant, pour être en mesure de continuer à protéger leurs utilisateurs, leurs activités et leurs actifs (Systèmes d'Information, données, …) de la « Cyber-menace » en constante évolution.

Par ailleurs, les risques et les menaces de sécurité informatique avec la professionnalisation de la cybercriminalité face à un niveau de protection des entreprises et des institutions qui est nettement insuffisant, à la multiplication des cyberattaques massives et non-ciblées type ransomware, à la fraude sur internet via différentes techniques d'ingénierie sociale, à la perte de données sensibles suite à des malversations, aux risques inhérents au fait de transférer leurs applications et données vers un tiers (Cloud computing), et l'accroissement de la télémédecine utilisant des réseaux de communication vulnérables (Internet, mobiles, wifi, …).

Face à ces enjeux, le Master Cybersécurité et e-Santé a pour mission de former en deux ans des experts en Cybersécurité des systèmes, réseaux et données associés aux secteurs de la santé connectée (e-Santé) et de l'Internet des Objets (IoT). Les experts seront capables de mener des missions de conseil, d'analyse et d'audit de sécurité, ainsi que de développement, d'implémentation et de validation de solutions techniques de sécurité.

OBJECTIFS

Le Master **Cybersécurité et e-Santé** a pour objectif de former des experts en Sécurité des Systèmes d'Information et des nouvelles technologies de la **santé connectée** (e-Santé) et de l'I**nternet des Objets** (IoT). La formation vise dans un premier temps à acquérir une compréhension des environnements technologiques et réglementaires dans lesquels opèrent aujourd'hui les entreprises et en particulier l'industrie et les établissements du secteur de la santé; puis dans un deuxième temps, identifier, analyser et interpréter les différentes cybermenaces possibles ; pour enfin sécuriser les systèmes d'Information, les données et les composants informatiques (réseaux et systèmes informatiques, dispositifs médicaux, capteurs, IoT …) grâce à l'acquisition de compétences scientifiques, techniques et méthodologiques de pointe. Outre un enseignement scientifique et technique de haut niveau en Cybersécurité et e-Santé en M2, le socle généraliste du M1 permet de fournir une culture informatique et sécurité suffisamment large (Programmation, Systèmes, Réseaux, IA, Cryptographie), bien adaptée aux métiers visés et à leurs évolutions futures.

COMPÉTENCES VISÉES

La formation de **Master Cybersécurité et e-Santé** aborde les aspects techniques, fonctionnels et juridiques de la Sécurité des Systèmes d'Information et de la e-Santé, apportant ainsi des connaissances approfondies

Pour en savoir plus, rendez-vous sur > u-paris.fr/choisir-sa-formation

Université de Paris

des techniques d'audit de sécurité et de sécurisation des infrastructures, des données et des applications d'entreprises, IOT ou médicales. Elle permet en outre de développer des compétences en tests de pénétration et d'analyse forensique.

L'expert en Cybersécurité et e-Santé ainsi formé pourra définir, mettre en œuvre et gérer une politique de sécurité pour son organisation ; protéger le Système d'Information, les données, et les équipements médicaux et IoT en exploitation ; et maîtriser les différentes phases d'analyse de risques, de spécifications et d'implémentation des solutions techniques de sécurité pour éradiquer les menaces, en prévention ou en réaction.

Programme

ORGANISATION

Le **Master Cybersécurité et e-Santé** se déroule sur deux années en présentiel à l'université. Former par un corps professoral et de professionnels experts de la Cybersécurité, des réseaux IOT et de la santé numérique, les étudiants suivent les enseignements fondamentaux et pratiques suivants :

1ère année :

* Programmation et Algorithmique
* Réseaux TCP/IP et Systèmes d'exploitation
* Intelligence Artificielle, Science des Données et Big Data
* Cryptographie et sécurité informatique
* Cybersécurité
* Sécurité des réseaux et des systèmes
* Droit, Anglais et Management de projet
* Projet tutoré

2ème année :

* Réseaux de capteurs corporels pour la santé
* Télémédecine et protection des données : Réglementation et Conformité
* Cryptographie avancée et Blockchain
* Sécurité des réseaux IOT et capteurs médicaux
* Sécurité des réseaux mobiles, et du Cloud Computing
* Audit de Sécurité, Hacking Ethique, et Tests de pénétration
* Cybersécurité avancée: Analyse Forensique et Malware
* Veille technologique et Innovation
* Projet tutoré

STAGE

Stage : Obligatoire

Durée du stage : Alternance en entreprise toute l'année (de septembre à août)

Stages et projets tutorés :
La formation requière de réaliser un projet tutoré en première année par équipe et sous la supervision d'un enseignant de l'équipe pédagogique. Ce projet donne lieu à la rédaction d'un mémoire et d'une soutenance orale devant un jury. Les sujets de projets tutorés sont proposés par les enseignants du Master en partenariat avec les responsables des plateformes d'étude du Master, et sont souvent inspirés par les nouveaux enjeux et l'actualité de la Cybersécurité et de la santé connectée. Le projet se déroule sur 6 mois (semestres 2).
Le semestre 4 (2eme année) est consacrée à la réalisation d'un stage professionnel ou de recherche d'une durée minimale de 4 mois. Il est ponctué par la remise d'un mémoire et d'une soutenance orale devant un jury composé de représentants de l'équipe pédagogique et des entreprises d'accueil.

Admission

Le Master **Cybersécurité et e-Santé** s'adresse à la fois à des étudiants motivés par la Sécurité des Systèmes d'Information et les nouvelles technologies des IOT et de la santé connectée, ainsi qu'à des professionnels du domaine

Pour en savoir plus, rendez-vous sur > u-paris.fr/choisir-sa-formation

qui souhaitent acquérir des compétences de haut-niveau, afin de relever efficacement les challenges actuels et futurs de la cybersécurité, de l'Internet des Objets et de la e-Santé.

PRÉ-REQUIS

Prérequis pour entrer en M1 :
Licence d'informatique ou validation d'acquis personnels et professionnels (VAPP D. 23/08/1985)

Prérequis pour entrer en M2 : Master 1 en informatique, diplôme d'ingénieurs ou validation d'acquis personnels et professionnels (VAPP D. 23/08/1985)

Et après ?

POURSUITE D'ÉTUDES

Après l'obtention du Master, les diplômés peuvent soit entrer directement dans le monde professionnel dans différents secteurs (Industrie, Santé, Télécoms, Banques, Conseils, …) ou bien choisir de poursuivre les études pour préparer une thèse de doctorat en Cybersécurité et/ou e-Santé au moyen d'un contrat de financement doctoral ou CIFRE en partenariat avec une entreprise.

PASSERELLE

A l'issue de la première année, une réorientation en seconde année vers le parcours « Machine Learning For Data Science en alternance/apprentissage du Master Informatique de l'Université Paris Descartes est envisageable.

TAUX DE RÉUSSITE

90 % en M1 et 100 % en M2

INSERTION PROFESSIONNELLE

De nombreuses entreprises (Sanofi, Orange, Airbus, Medtronic, BNP PARIBAS, Huawei, Thales, Alcatel, Dassault, …), ainsi que des cabinets de conseils (PWC, Cap Gemini, Deloitte, …), SSII (Altran, Atos, …) , startups et administrations publiques (ASIP-Santé, Hôpitaux, Préfectures, ...) accueillent nos diplômés. A l'issue de leur formation, quelques diplômés choisissent l'international (USA, Canada, UK, …).

Les métiers qui leurs sont proposés sont de : Ingénieur Cybersécurité, Ingénieur systèmes IOT, Ingénieur de recherche en e-santé, Consultant Cybersécurité, Pentesters, Auditeur sécurité, Développeur applications e-santé, Développeur sécurité, Analyste SOC, …

Le taux d'insertion professionnel de nos diplômés est de 100%, 6 mois après la fin de la formation.

Contacts

Responsable du Master 1
Osman Salem
osman.salem@parisdescarertes.fr

Responsable du diplôme
Ahmed Mehaoua
ahmed.mehaoua@parisdescartes.fr

En bref

Composante(s)
UFR des Sciences fondamentales et biomédicales

Niveau d'études visé
BAC +5

Durée
2 ans

ECTS
120

Pour en savoir plus, rendez-vous sur > u-paris.fr/choisir-sa-formation

Université de Paris

Modalité(s) de formation

- Formation initiale
- Formation continue

Validation des Acquis de l'Expérience

Oui

Langue(s) des enseignements

- Français

Lieu de formation

Campus Saint Germain des Prés

Pour en savoir plus, rendez-vous sur > u-paris.fr/choisir-sa-formation