DIPLOME D'UNIVERSITÉ
CYBERSÉCURITÉ

La Cybersécurité est devenue un élément stratégique pour les entreprises et les administrations publiques. De plus en plus conscientes des enjeux, ces dernières investissent davantage dans la sécurité de leurs infrastructures et systèmes d'information.
Plus qu'une simple fonction support, l'intégration des problématiques de sécurité devient un atout différenciant sur le marché, notamment pour les grandes entreprises. Tous les acteurs économiques, privés ou publiques, sont aujourd'hui concernés par la Cybersécurité.

DIPLOME VISE

Type de diplôme : Diplôme d'Université

PUBLIC VISE - PREREQUIS – ADMISSIBILITE - ADMISSION

Public : salariés en CDI/CDD, intérimaires, demandeurs d'emploi, adultes en reprise d'études, souhaitant valider et compléter des acquis professionnels.
Prérequis :
- Master 2 en Informatique et/ou Réseaux,
- M2 MIAGE,
- Licence générale ou professionnelle en Informatique et/ou Réseaux avec 3 années d'expérience professionnelle dans le domaine,
- DUT et BTS en Informatique et/ou Réseaux avec 3 à 5 années d'expérience professionnelle dans le domaine.

Admissibilité : examen approfondi du dossier de candidature
Admission : éventuel entretien individuel (en présentiel ou par visioconférence)

OBJECTIFS

En raison du fort développement des plateformes technologiques, ayant des flux de données sensibles (cloud, mobiles, internet des objets, etc.), et de l'impact croissant du numérique dans tous les secteurs d'activité, les compétences dans le domaine de la Cybersécurité sont constamment recherchées et demeurent en très forte croissance.
Face à un nombre toujours croissant d'attaques dirigées envers les administrations et les entreprises de tous les secteurs d'activités, il est nécessaire d'étudier et d'analyser l'ensemble des composantes associées aux réseaux et systèmes informatiques. Cela va des moyens de transport des données jusqu'aux services applicatifs, en passant par les équipements physiques, les systèmes d'exploitation, et les logiciels de communication.
Dans cette formation, l'ensemble de ces composantes seront étudiées et analysées afin de comprendre et d'identifier les menaces ainsi que les contre-mesures associées. Aussi, une très bonne compréhension des attaques est nécessaire pour une mise en œuvre efficace de ces contre-mesures. La sécurité des réseaux informatique est devenue ainsi un élément critique qu'il faudrait traiter sous les angles conceptuels et pratiques. C'est l'objectif de cette formation.

COMPETENCES VISEES

Cette formation couvre l'ensemble des composantes fondamentales et nécessaires à la maîtrise, l'analyse, la conception et la mise en œuvre de solutions de sécurité des systèmes et réseaux informatiques. Les compétences acquises à l'issue de cette formation permettront aux participants de :
- Contribuer à l'ensemble du processus d'une étude de sécurité, depuis le recensement des besoins et des risques jusqu'à la mise en œuvre des solutions de sécurité,
- Appréhender les techniques, outils et protocoles de sécurité,
- Disposer de compétences nécessaires pour concevoir et mettre en œuvre une architecture de sécurité.

CONTENU DE LA FORMATION

Plaquette et calendrier de la formation :
https://www.iut.parisdescartes.fr/diplome-duniversite-cybersecurite/

Programme :
Le DU est constitué de 5 certificats (modules) qui alternent enseignements théoriques, travaux pratiques et dirigés.
Un tutorat individualisé en ligne sera également mis en place. Les stagiaires devront fournir un travail individuel sur une étude de cas avec remise d'un rapport.

Module 1 : Systèmes cryptographiques
- La cryptographie symétrique et asymétrique
- Les fonctions de hachage,
- La signature numérique
- Le partage des clés secrètes

Applications: Cartes à Puces, Blockchain

Module 2 : Sécurité des réseaux et des systèmes
- Concepts, définitions et standards relatifs aux attaques et à leurs conséquences
- Systèmes de détection d'intrusions
- Architectures de cloisonnement
- Protocoles de tunneling
- Protocoles d'authentification

Module 3 : Audit et analyse des réseaux et des systèmes
- Audit de vulnérabilités
- Audit de configuration
- Audit d'organisation

Module 4 : Infrastructures de confiance et sécurité des échanges
- Architectures PKI, Protocoles
- Mécanismes et protocoles cryptographiques
- Politiques de sécurité

Module 5 : Sécurité des réseaux sans fil
- Architectures et Protocoles des reseaux sans fil
- Attaques et analyses
- Mecanismes de défense contre les attaques

ÉQUIPE, METHODES ET MOYENS PEDAGOGIQUES

Responsable du cycle : Farid NAÏT-ABDESSELAM, Professeur des Universités
Équipe pédagogique : enseignants-chercheurs et professionnels qualifiés ayant des activités en lien avec le contenu de la formation.
Méthodes : cours magistraux, ainsi que des travaux pratiques et dirigés sur des outils/logiciels du marché et/ou opensource.
La pédagogie laisse une large place à l'initiative du stagiaire et à son travail personnel pour mettre en œuvre les connaissances et les compétences acquises.
L'assiduité en cours est obligatoire ; elle fait l'objet de listes d'émargements par demi-journées.

Moyens pédagogiques adaptés : logiciels professionnels, salles informatiques (1 poste par stagiaire), bibliothèque universitaire avec salle multimédia, centre d'étude des langues, supports de cours.
Un ensemble d'ordinateurs connectés en réseaux à Internet (un ordinateur par stagiaire).
Un ensemble de clés USB, d'une bonne capacité (32 Go), pour contenir les logiciels et machines virtuelles à utiliser lors des ateliers (une clé par stagiaire).
Les stagiaires bénéficient d'un environnement numérique de travail leur permettant de recevoir et consulter des cours, consignes, informations pédagogiques et administratives ainsi que de déposer des documents et partager leur expérience.

ÉVALUATION DE LA FORMATION

Organisation du contrôle des connaissances (*) : le DU Cybersécurité est sanctionné par un contrôle continu dans chacun des certificats**.** Chaque certificat (module) fera l'objet d'un contrôle continu indépendant sous la forme suivante : QCM, projet et/ou compte rendu de TP. Les candidats ayant satisfait aux conditions d'assiduité et ayant obtenu une moyenne générale supérieure ou égale à 10 seront déclarés admis au DU Cybersécurité. Une note minimale de 7/20 dans chaque module est requise en cas de compensation entre les notes des différents modules. Par ailleurs, tout certificat pour lequel la note est supérieure ou égale à 10/20 est acquis définitivement. La formation est sanctionnée par un contrôle continu comportant une évaluation par module, notée chacune sur 20.
L'assiduité est obligatoire.
Validation des études (*) : le diplôme est décerné à tout candidat ayant satisfait aux conditions d'assiduité et obtenu une note moyenne supérieure ou égale à 10 sur 20 sur l'ensemble des modules. Tous les autres cas relèvent d'une délibération spéciale du jury. Les délibérations du jury sont secrètes.

(*) extrait des Modalités de Contrôle des Connaissances. Les MCC sont votées annuellement par le Conseil d'Administration de l'IUT de Paris et par les instances de l'Université. Elles sont remises au stagiaire dès l'entrée en formation.
Seules les MCC votées au titre de l'année universitaire pour laquelle le stagiaire FC est inscrit en formation feront foi.

PERSPECTIVES PROFESSIONNELLES

- Responsable de la sécurité des systèmes d'information
- Chef de projet sécurité
- Administrateur système, réseau et sécurité
- Consultant Cybersécurité

MODALITES DE CANDIDATURE

Session de candidature : 01/07/2021 au 15/12/2021
Candidature en ligne : https://ecandidat.app.u-paris.fr/sh1/

ORGANISATION DE LA FORMATION

Déroulement de la formation : à temps partiel et en discontinu
Dates de la formation : 10/01/2022 au 21/06/2022
Enseignement théorique : 21,5 jours répartis sur 11 semaines soit 150 heures
Horaires : 9 h 00 à 12 h 30 - 13 h 30 à 17 h 00 (sous réserve de modification)
Nombre de stagiaires par groupe : en moyenne 25 personnes (groupe dédié formation continue).

Les formations sont délivrées en présentiel. Toutefois l'IUT de Paris – Rives de Seine pourra être amené à assurer ses activités pédagogiques en mode distanciel si la situation sanitaire l'exige et conformément aux directives ministérielles.

COUT ET DROITS D'INSCRIPTION UNIVERSITAIRE

Coût du cycle d'enseignement théorique : 3 000,00 € nets.
(tarif sous réserve d'approbation par les instances d'Université de Paris - l'Université de Paris est un établissement public non assujetti à la TVA).
Droits d'inscription universitaire : obligatoires ; ils sont fixés chaque année par arrêté du MESRI.

CVEC : https://cvec.etudiant.gouv.fr/

Salariés : la prise en charge du coût de la formation peut être assurée dans le cadre des dispositifs de Formation Professionnelle en vigueur. Il appartient aux candidats d'effectuer les démarches nécessaires auprès des organismes dont ils dépendent : DRH, OPCO…
Demandeurs d'emploi : sous certaines conditions, vous pouvez bénéficier de l'Aide Individuelle à la Formation (AIF) ou obtenir une Autorisation d'Inscription à un Stage de Formation (AISF). Les démarches doivent être faites auprès du conseiller Pôle Emploi.

INFORMATIONS PEDAGOGIQUES

DEPARTEMENT INFORMATIQUE
✆ **01 76 53 47 25**
✉ **secretariat-info@iut.parisdescartes.fr**

MONTAGE DU DOSSIER DE FINANCEMENT, DEVIS, CALENDRIER

SERVICE FORMATION CONTINUE ET ALTERNANCE (SFCA)
✆ **01 76 53 49 75**
✉ **bernadette amiaud@u-paris.fr**

LIEU DE LA FORMATION

IUT de Paris – Rives de Seine
143, avenue de Versailles - 75016 PARIS
✆ 01 76 53 47 00
https://www.iut.parisdescartes.fr/

ACCES A L'IUT

Exelmans, Mirabeau, Église d'Auteuil, Chardon Lagache
22, 62, 72, PC1
Pont du Garigliano
Pont du Garigliano