Diplôme d'Université

Cybersécurité

La cybersécurité constitue aujourd'hui un enjeu stratégique majeur pour les entreprises et les administrations publiques. De plus en plus conscientes des risques liés au numérique, ces organisations investissent désormais de manière significative dans la protection de leurs infrastructures et de leurs systèmes d'information.
Au-delà d'une simple fonction support, la prise en compte des problématiques de sécurité devient un véritable facteur différenciant et un avantage compétitif, notamment pour les grandes organisations. Aujourd'hui, l'ensemble des acteurs économiques, qu'ils soient publics ou privés, sont directement concernés par les enjeux de cybersécurité.

Quel type de formation ?

Formation continue

Comment s'organisent les études ?

La formation se répartit sur 6 mois. Le DU, d'une durée de 150 h, suivra un rythme d'environ 2 jours de cours par semaine, sur 11 semaines.
Un tutorat individualisé en ligne sera également mis en place, et les stagiaires devront fournir un travail individuel sur une étude de cas avec remise d'un rapport.

Objectifs

Le développement rapide des plateformes technologiques manipulant des flux importants de données sensibles (cloud computing, mobilité, Internet des objets, etc.), ainsi que la transformation numérique de l'ensemble des secteurs d'activité, entraînent une demande croissante en compétences dans le domaine de la cybersécurité.
Face à la multiplication et à la sophistication des attaques ciblant les administrations et les entreprises, il devient indispensable d'étudier et d'analyser l'ensemble des composantes des réseaux et des systèmes informatiques. Ces composantes couvrent l'ensemble de la chaîne technologique, depuis les infrastructures de transport des données jusqu'aux services applicatifs, en passant par les équipements matériels, les systèmes d'exploitation et les logiciels de communication.
Cette formation vise ainsi à analyser ces différentes composantes afin de comprendre les menaces, d'identifier les vulnérabilités et de mettre en œuvre les contre-mesures appropriées. Une compréhension approfondie des mécanismes d'attaque constitue en effet un préalable indispensable à la mise en œuvre de stratégies de défense efficaces.
La sécurité des systèmes et des réseaux informatiques est devenue un élément critique qui doit être abordé à la fois sous des angles conceptuels, méthodologiques et pratiques : tel est l'objectif principal de cette formation.

Compétences visées

Cette formation couvre l'ensemble des compétences fondamentales nécessaires à l'analyse, la conception, et la mise en œuvre de solutions de sécurité pour les systèmes et les réseaux informatiques.
À l'issue de cette formation, les participants seront capables de :
- Contribuer à l'ensemble du processus d'une étude de sécurité, depuis l'identification des besoins et l'analyse des risques jusqu'à la mise en œuvre des solutions de protection ;
- Maîtriser les techniques, outils et protocoles utilisés dans la sécurisation des infrastructures numériques ;
- Concevoir et déployer des architectures de sécurité adaptées aux besoins des organisations.

Moyens pédagogiques

La formation repose sur une alternance d'enseignements théoriques, de travaux dirigés, et de travaux pratiques utilisant des outils et des plateformes représentatifs des technologies du marché.

Perspectives professionnelles

À l'issue de la formation, les participants pourront accéder notamment aux fonctions suivantes :
- Responsable de la sécurité des systèmes d'information (RSSI)
- Chef de projet sécurité
- Administrateur systèmes, réseaux et sécurité
- Consultant en cybersécurité

Comment nous rejoindre ?

Conditions d'admission :

Ce diplôme, proposé uniquement en formation continue, s'adresse à des salariés, des adultes en reprise d'études ou des demandeurs d'emploi titulaires :

- d'un Master 2 en Informatique et/ou Réseaux
- d'un Master 2 MIAGE
- d'une Licence générale ou professionnelle, spécialité Informatique et/ou Réseaux, avec au moins deux années d'expérience professionnelle dans le domaine
- d'un DUT ou d'un BTS en Informatique et/ou Réseaux, avec au moins deux années d'expérience professionnelle dans le domaine.

Les candidatures sont examinées sur dossier et peuvent être complétées par un entretien.

Les candidatures doivent être déposées via la plateforme eCandidat.

Plus d'informations sont disponibles sur le site de l'IUT.

Financement et coût :

Coût du cycle de formation continue : 3 000,00 €

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, Pôle Emploi...

Droits d'inscription universitaire obligatoires, ils sont fixés chaque année par arrêté à paraître en juillet.

Le contenu pédagogique

Le Diplôme Universitaire (DU) est composé de cinq certificats (modules) combinant enseignements théoriques, travaux dirigés et travaux pratiques. Un tutorat individualisé est également proposé afin d'accompagner les participants dans leur progression. Les stagiaires devront réaliser également un travail individuel sous la forme d'une étude de cas appliquée, donnant lieu à la rédaction et à la soutenance d'un rapport.

Module 1 : Systèmes cryptographiques

- Cryptographie symétrique et cryptographie asymétrique
- Fonctions de hachage et mécanismes d'intégrité
- Signature numérique et authentification
- Gestion, distribution et partage des clés secrètes
- Introduction aux technologies blockchain et aux registres distribués

Module 2 : Sécurité des réseaux et des systèmes informatiques

- Concepts fondamentaux et typologie des cyberattaques
- Protocoles et mécanismes de sécurité des réseaux
- Architectures de défense et cloisonnement des infrastructures
- Systèmes de détection et de prévention d'intrusions (IDS/IPS)
- Protocoles de tunneling et mécanismes d'authentification sécurisée

Module 3 : Audit et analyse des réseaux et des systèmes

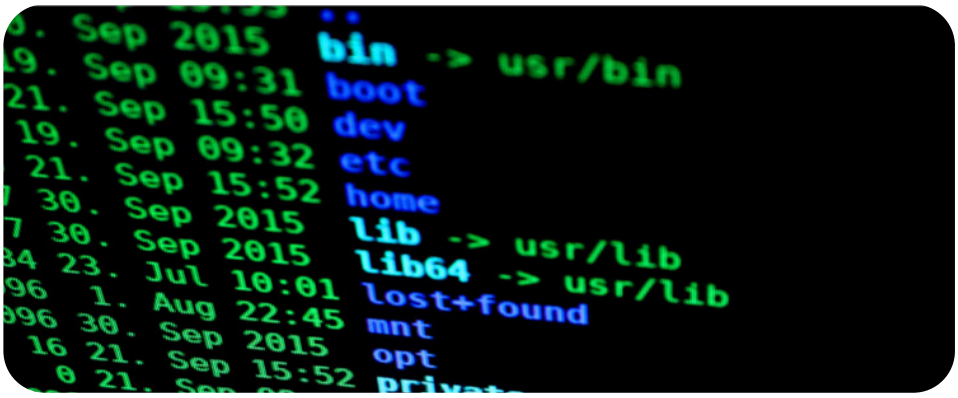
- Méthodologies d'audit de sécurité des systèmes d'information
- Audit de vulnérabilités et analyse de configuration
- Analyse et interprétation des flux réseau
- Outils d'analyse et de supervision du trafic réseau
- Techniques d'identification et de gestion des vulnérabilités

Module 4 : Infrastructures de confiance et mise en oeuvre

- Architectures de sécurité et infrastructures de confiance
- Infrastructures à clés publiques (PKI) et gestion des certificats
- Protocoles cryptographiques pour la sécurisation des communications
- Politiques de sécurité et gouvernance des systèmes d'information
- Déploiement et gestion opérationnelle des infrastructures sécurisées

Module 5 : Sécurité des infrastructures logicielles et matérielles

- Sécurité des systèmes d'exploitation et des plateformes logicielles
- Protection des données et sécurité de l'information
- Typologie des attaques logicielles et matérielles
- Méthodes d'analyse et de détection des attaques
- Mécanismes de défense et stratégies de protection des infrastructures



Comment nous contacter ?

Obtenir les informations pégagogiques :
Département Informatique
· 01 76 53 47 25
· veronique.bedos@u-paris.fr

Obtenir un devis et remplir le dossier de financement :
Service Formation Continue et Alternance
· f-continue.iutparis-seine@u-paris.fr

IUT de Paris - Rives de Seine
143, avenue de Versailles
75016 Paris
Tél : 01 76 53 47 00
iutparis-seine.u-paris.fr

- Exelmans, Mirabeau, Eglise d'Auteuil, Chardon Lagache
- BUS 22, 62, 72, PC1
- RER Ligne C station Pont du Garigliano
- T3 station Pont du Garigliano

IUT de Paris - Rives de Seine
Université Paris Cité