



BLOC DE COMPÉTENCES

Analyser et mettre en œuvre des systèmes sécurisés

Dans le contexte de la transformation numérique, alors que la cybercriminalité se professionnalise et que les enjeux de souveraineté numérique se font plus prégnants, la maîtrise de la sécurité des systèmes d'information devient un sujet majeur pour les entreprises, et plus largement toutes les organisations. Ce bloc de compétences permet aux professionnels du numérique, travaillant dans le domaine des systèmes d'information, du développement logiciel, etc... d'acquérir les compétences nécessaires pour travailler dans le domaine de la cybersécurité, analyser et mettre en œuvre des systèmes sécurisés. Cette formation est l'un des blocs de compétences constitutifs du **Diplôme d'ingénieur en informatique de l'École Nationale Supérieure des Sciences Appliquées et de Technologie**.

CONTACTS

ENSSAT

Service Formation Continue et
Alternance (SFCA)

Rue Édouard Branly
22300 Lannion
02 96 46 93 58
sfca-lannion@univ-rennes1.fr

Responsable pédagogique

Julien LOLIVE

Docteur en cybersécurité
Ingénieur enseignant

Philippe QUÉMERAIS

07 87 70 70 72
responsable.formation-
continue@enssat.fr

Chargée de mission

Marie JEZEQUEL

02 96 46 93 58
marie-
christine.jezequel@univ-
rennes1.fr

Publics

Cette formation s'adresse aux salariés et aux demandeurs d'emploi, ingénieurs, titulaires d'un master ou équivalent, souhaitant acquérir des compétences de haut niveau en cybersécurité. Un bon niveau de maîtrise des technologies de l'information et de la programmation logicielle est nécessaire.

Objectifs et compétences visées

A l'issue de la formation le professionnel sera en mesure :

- Connaître les différents champs de la cybersécurité,
- Déployer et manager la cybersécurité au sein d'une organisation ou d'un projet;
- Analyser, concevoir et mettre en œuvre la sécurité d'un système d'information dans le cadre d'un processus d'amélioration continue ;
- Intégrer la sécurité dans les réseaux et dans les systèmes d'exploitation;
- Développer des logiciels sécurisés.

Les plus de la formation

- Bloc de compétences éligible au Compte Personnel de Formation.
- Les compétences constitutives du bloc sont suivies sur un semestre universitaire.
- Le bloc de compétences est associé au diplôme d'ingénieur en informatique.



PROGRAMME

Organisation de la cybersécurité	Durée : 21 h Dates : 2021
Compétences : organiser la cybersécurité au sein d'une organisation ou d'un projet	
Contenu	<ul style="list-style-type: none">- Organisation de la cybersécurité au sein d'une entreprise - au sein des projets- Contexte normatif et juridique- Services de chiffrement et signature électronique- Bases cryptographiques- Les certificats numériques- Les signatures- Logiciels, programmation, exemples- Cadre légal et juridique
Pentest et Forensic	Durée : 40 h Dates : 2021
Compétences : réaliser des tests d'intrusion et analyser les traces numériques après une attaque	
Contenu	<ul style="list-style-type: none">- Pentest - Les vulnérabilités sont abordées ainsi que la recherche d'informations, l'exploitation et la correction de vulnérabilités. Des TP's pratiques avec un attaquant et une cible sont mis en oeuvre.- Forensic - Dans le premier chapitre, deux notions sont abordées : le cadre réglementaire qui encadre les systèmes de traitement automatisé de données et l'anatomie d'une attaque informatique. Dans la deuxième section, le Digital Forensics & Incident Response est abordé et mis en pratique : Qu'est-ce que la réponse à incident ? Qu'est-ce que le forensics ? Quelles méthodes de travail ? Comment collecter les supports ?
Logiciels sécurisés	Durée : 20 h Dates : 2021
Compétences : développer des logiciels sécurisés	
Contenu	<ul style="list-style-type: none">- Sécurité par conception- Vulnérabilités web- Recherche de vulnérabilités- Vulnérabilité binaire
Données	Durée : 20 h Dates : 2021
Compétences : protéger les données et la vie privée	
Contenu	<ul style="list-style-type: none">- Protection de la vie privée : RGPD, technologie de protection de la vie privée, assainissement de données, contextes- Les accréditations anonymes- Réseaux de communication anonyme- Protocoles anonymes- La cryptographie dans les protocoles respectueux de la vie privée
Sécurité des réseaux avancée	Durée : 20 h Dates : 2021
Compétences : sécuriser des réseaux	
Contenu	<ul style="list-style-type: none">- Sécurité des réseaux- IMS et SBC- Gestion de clé de chiffrement, PKI- Open Test lab- AAA-Radius



Organisation pédagogique

Durée : la formation se déroule sur le premier semestre de l'année universitaire entre septembre 2021 et février 2022.

Volume total : 121 h - prévoir 80 heures de travail personnel

Lieu de la formation : Lannion, ENSSAT

Modalités de validation

Devoirs sur table et/ou devoirs maison.

Travaux pratiques et rapports écrits.

Projet, rapports écrits et restitutions orales.

ET APRÈS ?

Exercer dans l'un des domaines de la cybersécurité

CANDIDATURE

Pré-requis

Ingénieurs, titulaires d'un master 1 ou équivalent.

Avoir une expérience solide dans le domaine du développement logiciel, des réseaux ou de l'administration des systèmes d'informations.

Sélection

Accès sur dossier et entretien.

Nombre de places : 4

Cout de la formation

4840 euros

REFERENTIEL

Type de diplôme

Bloc de compétences

N° RNCP : 35782BC04

Formation support :

Ingénieur en informatique

Intitulé bloc :

Analyser et mettre en œuvre des systèmes sécurisés

CPF :

Cette formation est éligible au Compte Personnel de Formation :

<https://www.moncompteformation.gouv.fr/espace-prive/html/#/formation/recherche/>

MAJ : Juin 2021