Programme de formation
CSB.SCHOOL

N'ÉTUDIEZ PAS LA CYBERSÉCURITÉ, VIVEZ-LA

Bachelor spécialiste en cybersécurité

Objectifs de la FORMATION

A l'issue de la formation les alternants seront capables de contribuer à l'amélioration de la posture de cybersécurité des organisations.

Ils apprendront à maitriser les technologies et les systèmes d'information de gestion ou d'exploitation. Ils feront également l'acquisition de capacités d'analyse sur le fonctionnement des organisations et l'impact du cadre réglementaire et normatif.

Avec l'arrivée des nouvelles technologies de l'information et de la communication (NTIC) telles que l'internet, le cloud computing, l'intelligence artificielle, les objets connectés, la cybersécurité s'impose comme un sujet transverse qui englobe la sécurité informatique, la sécurité des systèmes d'information, ainsi que des composantes géopolitiques, géoéconomiques et géostratégiques.

Les titulaires du Bachelor Spécialiste Cybersécurité seront aptes à comprendre et à contribuer à résoudre les problématiques majeures de la cybersécurité : préserver la confidentialité, l'intégrité et la disponibilité des systèmes, des réseaux informatiques et des données.

La formation leur fournira tout le bagage nécessaire à leur insertion professionnelle. Ils seront en mesure d'exécuter des projets de cybersécurité en cohérence avec la stratégie globale de leur organisation.

Titre RNCP de niveau 6 en cours d'instruction

CONTENU PÉDAGOGIQUE

Bachelor, spécialiste en cybersécurité 3ème année

01. Conduire des tests d'intrusion éthiques

Panorama des menaces & attaques
Conduite d'un test d'intrusion

02. Concevoir et maintenir une architecture sécurisée

Modèle d'infrastructure Cloud
Infrastructures informatiques industrielles
ISMS & PSSI : déclinaison et déploiement de standard
Enjeux et risques cyber IT pour les organisations
Protection du matériel informatique
Sécurité des réseaux de télécommunication
Protection de la Donnée et de l'Information
Cybersécurité dans la conception et management des projets IT/OT
Gestion du processus d'achat en cybersécurité
Sécurisation des échanges de données
Gestion de l'authentification et des identités
Cybersécurité des architectures réseaux
Gestion des Réseaux de télécommunication
Sécurisation des IoT
Sécurisation des infrastructures cloud
Sécurisation des infrastructures informatiques industrielles

03. Détecter et analyser les événements de cybersécurité (SOC)

SOC : présentation et objectifs
Déploiement d'un Security Operations Center
SOC : Analyse de niveau 1 & 2

CONTENU PÉDAGOGIQUE

Bachelor, spécialiste en cybersécurité 3ème année

04. Sécuriser les infrastructures et les réseaux

ISMS & PSSI : déclinaison et déploiement de standard
Protection du matériel informatique
Sécurité des réseaux de télécommunication
Protection de la Donnée et de l'Information
Déploiement d'un Security Operations Center
IoT: objet connecté
Sécurisation des échanges de données
Gestion de l'authentification et des identités
Cybersécurité des architectures réseaux
Cybersécurité et Intelligence Artificielle
Sécurisation des IoT
Sécurisation des infrastructures cloud
Sécurisation des infrastructures informatiques industrielles

05. Modules transverses

Droit français
Système d'information
Concepts et bases des réseaux de télécommunication
Protocoles de communication et panorama du marché
Système d'exploitation
Scripting Python
Scripting OS
Environnements industriels
Méthode de travail
Ethique, Déontologie et Cybersécurité
Développement logiciel pour l'informatique industrielle

INFORMATIONS PÉDAGOGIQUES

Public Concerné

Public en formation initiale/alternance ou en reconversion souhaitant exercer un métier dans la cybersécurité.

Pré-requis

Pour être admissible, vous devez justifier d'une culture générale et/ou connaissances en cybersécurité/informatique. Un bon niveau d'anglais est exigé pour pouvoir, sans effort, suivre les différents cours/modules dispensés.
Pour les personnes n'ayant pas d'expérience dans le domaine de la cybersécurité, il est recommandé d'avoir une certification professionnelle ou un équivalent de niveau 5 en informatique

Moyens pédagogiques

Après une période de formation intensive au démarrage de l'année, les étudiants alterneront les périodes à l'école et en entreprise à raison de 1 mois en entreprise et 2 semaine sà l'école. Les enseignements alterneront entre le présentiel, le e-learning, le tutorat, les cas pratiques, les projets tutorés et en autonomie. Un suivi sera réalisé pour assurer le lien entre les apprentissages à l'école et dans l'entreprise.

Notre école dispose de laboratoires et de simulateurs reproduisant le système d'information d'une entreprise permettant aux étudiants de tester leurs compétences sur des cas pratiques en situation quasi réelle.

L'école utilisera en outre les modalités d'évaluations suivantes :

- Mise en situation simulée
- Mise en situation reconstitué
- Etude de cas pratique
- Soutenances orales pour présenter la méthodologie et les résultats des travaux réalisés ci-dessus.

Supports pédagogiques

Les étudiants auront accès aux ressources pédagogiques sur notre plateforme Moodle. Ils auront aussi accès aux différents simulateurs et laboratoires pour se former. Une bibliographie sera également proposée pour approfondir chaque domaine de formation.

ADRESSE

Venez nous rendre visite

39, rue de la Cité
69003 LYON

COORDONNÉES

Mail, téléphone & site web

contact@csb.school
+33651263702
www.csb.school

RÉSEAUX

Linkedin, Twitter & Facebook

Linkedin : csb.school
Twitter : @csb_school
Facebook : @schoolcsb

DÉMARREZ L'AVENTURE

CSB.SCHOOL

CYBERSECURITY
BUSINESS.SCHOOL