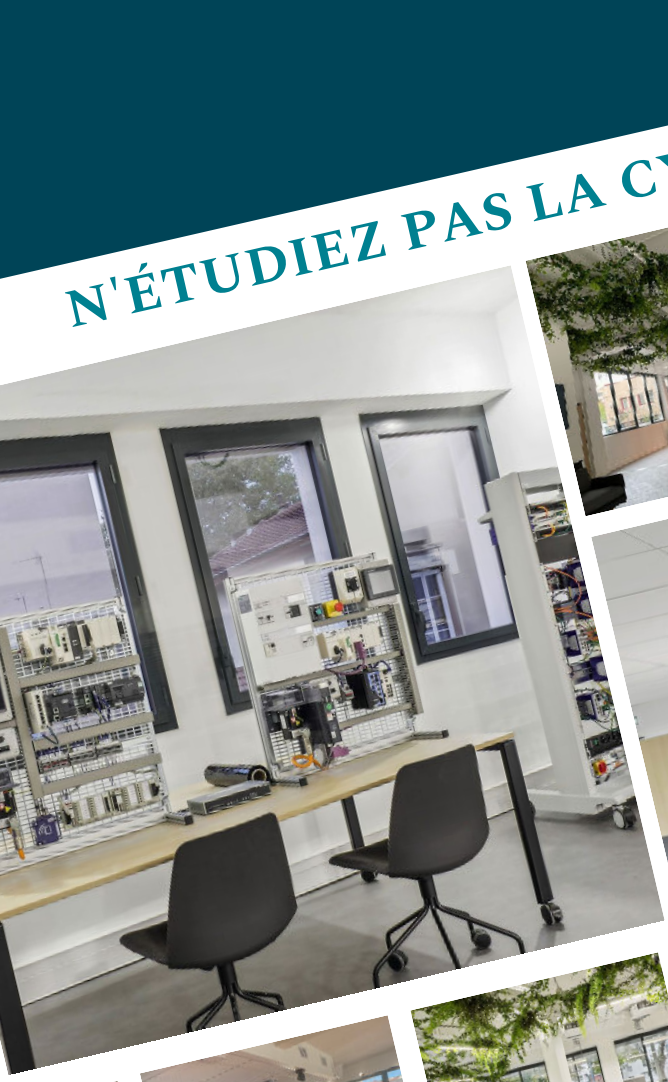
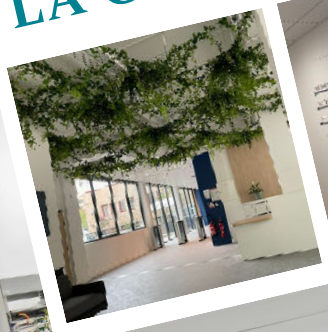
Programme de formation

CSB.SCHOOL

N'ÉTUDIEZ PAS LA CYBERSÉCURITÉ, VIVEZ-LA





Mastère Responsable

cybersécurité

Objectifs de la FORMATION

La cybersécurité est un élément essentiel dans la transformation numérique en cours, ce que nous rappellent des cyberattaques qui gagnent en volume, en impact et en sophistication.

Elle est essentielle afin de préserver la confidentialité, l'intégrité et la disponibilité des systèmes, des réseaux informatiques et des données. La cybersécurité est omniprésente ; tous les secteurs se dématérialisent et ont l'obligation de mettre en œuvre les technologies et d'attirer et de former les talents indispensables à leur protection.

La cybersécurité représente également un véritable avantage concurrentiel pour des organisations qui doivent la prendre en compte dans l'élaboration de leur stratégie. 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.

Habilité à former et organiser l'évaluation du titre RNCP de niveau 7 "Expert en Système d'Information" n°17285

La certification vise à développer les compétences pour le métier de responsable en cybersécurité. Elle/il est capable de concevoir et de mettre en œuvre les réponses adaptées afin d'assurer la cybersécurité des organisations, grâce à sa maîtrise des technologies et des systèmes d'information de gestion ou d'exploitation, du cadre réglementaire et normatif, et de la stratégie des organisations. Il s'agit d'un métier en tension parmi les plus recherchés sur le marché de l'emploi. La pénurie de ressources et de talents formés dans le domaine de la cybersécurité représente un frein à la transformation numérique.

Les titulaires de la certification Responsable Cybersécurité sont aptes à comprendre ces problématiques majeures, avec 3 possibilités de spécialisation :

- cybersécurité industrielle,
- gestion d'incidents
- et de crise cyber et conformité.

La certification leur fournit tout le bagage nécessaire à leur insertion professionnelle sur le marché. Ils seront en mesure de gérer des projets de cybersécurité en cohérence avec la stratégie globale de leur organisation.

CONTENU PÉDAGOGIQUE

Mastère Responsable Cybersécurité, 1ère année

01. Evaluer l'exposition aux risques de cybersécurité

Fondamentaux en gestion de la menace
Mise en place d'une veille en cybersécurité
CERT
Géopolitique de la cybersécurité

02. Concevoir et mettre en œuvre un SMSI

Management des infrastructures informatiques
Stratégie et Gouvernance d'entreprise
Gouvernance et Management des Données
Management du Matériel Informatique
Conformité et impact en cybersécurité
Déploiement d'infrastructure de Gestion de Clés - PKI
Conception et déploiement des systèmes de management de la sécurité de l'information - ISMS & PSSI
Détection et catégorisation des actifs
Administration et sécurisation des identités et des accès
Management des signatures électroniques

03. Mettre en œuvre les moyens organisationnels et humains

Stratégie et gouvernance des SI
Management de risque, audit et Contrôle Interne
Diagnostic organisationnel en cybersécurité
Stratégie de Formation et de Sensibilisation à la Cybersécurité
Pilotage des Audits ISO 27001
Pilotage des Audits techniques en cybersécurité
Pilotage des tests d'intrusion IT/OT
Pilotage des Audits NIST CSF

04. Modules transverses

Introduction à la gestion des processus et à la modélisation avec BPMN
Management de projet complexe et conduite du changement
Sécurisation des réseaux industriel
Réglementations de données personnelles et de santé

CONTENU PÉDAGOGIQUE

Mastère Responsable Cybersécurité, 2ème année

01. Répondre à un incident de cybersécurité

Conception d'un Plan de Réponse à Incident de Sécurité (PRIS)
Conception d'exercices de simulation d'incidents cyber (walkthrough, table-top, functional, full-scale)
Analyse d'arbre des causes d'un incident de cybersécurité (root cause analysis)
Gestion de la preuve en cybersécurité - Forensic

02. Assurer la résilience de l'organisation au cours d'un incident

Conception de Plan de Continuité d'Activités (PCA)
Norme ISO 22300
Conception des Plans de Reprise d'Activités (PRA)

03. Modules transverses

Préparation CISSP /ISO
Gestion du sourcing / procurement / vendor management (contrat, SLA, pilotage)
Urbanisme et Architecture en cyber
Management de projet complexe et conduite du changement
Blockchain et Cybersécurité
Informatique Quantique et Cybersécurité
Darknet : utilisation et risques
Implémentation d'une architecture Zero Trust
NIST : présentation des différents frameworks

L'étudiant devra, en plus du tronc commun, choisir une spécialité au choix parmi les 3 ci-dessous :

Cybersécurité industrielle (OT)

Concevoir et maintenir la cybersécurité d'un environnement industriel en fonction des objectifs et des risques de l'organisation
Réglementation et framework pour l'OT
Sécurisation des infrastructures informatique industrielles
Sécurité des communications en milieu industriel
Protocoles spécifiques à l'informatique Industrielle

Gouvernance, Risques et Conformité (GRC)

Garantir l'adéquation entre les exigences de conformité (réglementaires et normatives) et les mesures de cybersécurité
Réglementations pour la protection des données personnelles en cybersécurité (RGPD, PDPA, CCL, LGPD)
Réglementation des systèmes sensibles ou controlés en cybersécurité (LPM, CCL, DFARS)
Réglementations relatives aux données soumises à un processus d'exportation (EAR, ITAR, EU-Dual Use)
Réglementations des données de santé en cybersécurité (HDS, HIPAA)
Cloud Controls Matrix
Veille réglementaire et normative
Déclinaison des réglementations dans la PSSI/ ISMS
Création de politique de sécurité

Gestion de crise et incidents (SOC)

Analyse de niveau 2 en Centre Opérationnel de Sécurité
Analyse de niveau 3 en Centre Opérationnel de Sécurité
Déploiement d'un Centre Opérationnel de Sécurité
Gestion de la preuve en cybersécurité - Forensic
Gestions des crises de niveau 1 ou 2
Gestion des crises de niveau 3 à 5
Intelligence Artificielle pour les Centres Opérationnels de Sécurité
Pilotage de la performance des Centres Opérationnels de Sécurité

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 significative dans le domaine, il est recommandé d'avoir une certification professionnelle ou un diplôme de niveau 6 en informatique ou cybersécurité.

Moyens pédagogiques

Après une période de formation intensive au démarrage de chaque année, les étudiants alterneront les périodes à l'école et en entreprise à raison de 1 mois en entreprise et 2 semaines à l'école.

Les enseignements alterneront entre le présentiel, le e-learning, le tutorat, les cas pratiques, le 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 se basant sur la simulation d'une entreprise fictive et la réplication d'un système d'information

- 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