CSB
.school

École de Cybersécurité

1 Ils nous font confiance
page 2

2 Le campus
page 3

3 Les formations
page 5

4 Nos actions
page 16

Ils nous font confiance

Le campus

VOTRE AVENIR EN CYBERSÉCURITÉ COMMENCE ICI

Rejoignez l'école qui forme les experts en cybersécurité les plus recherchés.
Fondée par des experts en cybersécurité et en pédagogie, notre école combine expertise technique et excellence éducative. Doté d'équipements et de technologies de pointe, notre campus offre un environnement immersif, reproduisant les conditions réelles des entreprises. Située au cœur du Campus Région du numérique, notre école fait partie d'un écosystème unique fédérant 150 formations, 6 écoles résidentes, et plus de 950 étudiants, le tout sur un site exceptionnel favorisant collaboration et innovation.

Excellence numérique

Le campus accueille et fédère l'ensemble des acteurs de l'écosystème cyber - étudiants, professionnels, associations, chercheurs... - afin de stimuler la collaboration et l'émergence de projets entrepreneuriaux.

Innovation

Au quotidien, les étudiants côtoient professionnels, chercheurs et porteurs de projets, et découvrent au plus près les innovations de la filière cyber.

Pédagogie

Salles de travaux pratiques, laboratoires réseau et industriel (OT), SOC simulé et plateforme de pentest.

Modernité

Le Campus Région du numérique, c'est aussi un environnement moderne et connecté, offrant des infrastructures de qualité :

- Espaces de coworking et salles de créativité
- Équipements high-tech et connexion ultra-rapide
- Espaces de détente pour favoriser les échanges
- Accessibilité facilitée par les transports en commun et les infrastructures locales

NOS POINTS FORTS

Titres RNCP et formations labellisées SecNumedu
Formations accessibles dès Bac+2
Alternance dès Bac+3, gratuite pour l'étudiant
+200 entreprises partenaires
Certifications professionnelles incluses
Environnement immersif avec simulateurs, labos, cas réels

Les Formations

Formations d'excellence en cybersécurité

À la CSB.school, nous formons les experts de demain grâce à une pédagogie immersive et orientée terrain : **80%** des cours sont basés sur la **pratique**.

Nos étudiants évoluent sur un campus moderne, équipé des dernières technologies, pour **apprendre en conditions réelles.**

Les enseignements sont assurés par des **professionnels en activité**, pour une formation en phase avec les défis actuels du secteur.

Enregistrées au RNCP et labellisées SecNumedu par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), nos formations incluent chaque année la **préparation** et le **passage** de **certifications professionnelles**, véritables leviers de différenciation sur le marché de l'emploi.

Rejoignez un parcours d'excellence, au sein d'un écosystème dynamique, au cœur du Campus Région du numérique.

Les parcours

	Spécialiste cybersécurité (Bac+3)	Responsable cybersécurité (Bac+5)
Admission	Après un Bac+2	Après un Bac+3
Durée	1 an	2 ans
Type de formation	Initiale ou alternance	Alternance
Coût	7 500€ ou prise en charge employeur (1)	Prise en charge employeur (2)
Et après ?	Accès à l'emploi ou poursuite d'études	Accès à l'emploi
Certification	CEH	Ebios RM - ISO27001 - CISSP

(1) Frais de formation de 10 500€ pris en charge par l'employeur
(2) Frais de formation de 15 000€ pris en charge par l'employeur

Parcours
Spécialiste Cybersécurité (Bac+3)
Formation initiale et en alternance

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

Ils apprendront à maîtriser 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'essor des technologies numériques 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 diplôme 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.

Des organismes à nos côtés pour vous accompagner

+ de 200 entreprises et organismes sont partenaires de notre établissement grâce au travail de notre Pôle Relations Entreprises.

Titre RNCP de niveau 6
"Spécialiste en cybersécurité"
RNCP42503
Certificateur : CSB Education Group

Tout savoir sur la formation

Moyens pédagogiques

En alternance comme en formation initiale (stage alterné), les étudiants suivent un rythme de cinq semaines en entreprise pour deux semaines à l'école. Les enseignements combinent présentiel, e-learning, tutorat, cas pratiques et projets tutorés, avec un suivi assurant la cohérence entre théorie et pratique.

Des laboratoires et simulateurs reproduisant un système d'information d'entreprise permettent de travailler sur des situations proches du réel.

Les évaluations reposent sur des mises en situation, des études de cas pratiques et des soutenances orales.

Supports pédagogiques

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

Une formation labellisée

SecNumedu
ANSSI

CAMPUS RÉGION DU NUMÉRIQUE

FRANCE compétences
CERTIFICATION
enregistrée au RNCP

Contenu pédagogique

Gouvernance et risques

Stratégie et gouvernance des systèmes d'information
Principes de conformité réglementaire en cybersécurité
Savoir utiliser l'IA générative en entreprise

Cybersécurité industrielle

Environnement et infrastructures industrielles
Approche par les risques de la sécurité industrielle
IoT : Internet of Things
Sécuriser les IoT

Infrastructure et architecture

IT infrastructure and cloud models
Concepts et bases des réseaux de télécommunication
Protocoles de communication et panorama du marché
Sécurité des réseaux de télécommunication
Sécuriser une architecture réseau – Cybersecurity of network architectures
Gestion des réseaux de télécommunication
Organisation et pilotage d'un support IT

Sécurité des systèmes d'informations

Fondamentaux en cryptographie
SOC - Enjeux et objectifs
Protection du matériel informatique
Gestion de l'authentification
Protection de la donnée et de l'Information
Création de Playbook SOC
SOC - Analyste niveau 1
Sécurité des mails & Sécurisation des échanges de données
Active Directory

Intrusion

13 jours de test d'intrusion (pentests):

- Introduction au Pentest et aspect juridiques
- Reconnaissance passive / Reconnaissance active (externe)
- Reconnaissance passive / Reconnaissance active (Web)
- Fuites d'informations & Entrées utilisateurs
- Metasploit : utilisation basique et pivot dans zone protégée
- Elévations de privilèges sur serveur Linux
- Reconnaissance passive & active / écoute et empoisonnement du réseau / attaques et utilisation des hashs (cracking, relay, pass-the-hash)
- Analyses PingCastle et Bloodhound / Quick wins Windows - Low hanging fruits
- Attaques basiques Stack / Heap overflow et Format String et protections
- Exploitation de CVEs simples avec pivot, introduction à la persistance Linux

OSINT

Modules complémentaires

Anglais
Art oratoire & prise de parole en public niveau 1

Préparation et passage de la certification CEH

Parcours
Responsable Cybersécurité (Bac+5)
Formation en alternance

La formation vise à développer les compétences pour le métier de responsable en cybersécurité. Les étudiants acquièrent la capacité de concevoir et de déployer des réponses adaptées aux menaces, en s'appuyant sur la maîtrise des technologies, des systèmes d'information, du cadre réglementaire et normatif, ainsi que sur une compréhension des enjeux stratégiques des organisations.

Le métier de responsable en cybersécurité figure parmi les plus recherchés du marché. La pénurie de profils qualifiés constitue un frein majeur à la transformation numérique. Les titulaires de la certification sont préparés à répondre à ces enjeux critiques. Le programme couvre notamment trois grands domaines :

- cybersécurité industrielle
- détection d'incidents et gestion de crise cyber
- gouvernance, risques et conformité

La formation apporte l'ensemble des compétences nécessaires à une insertion professionnelle réussie. Elle prépare à la gestion de projets de cybersécurité alignés sur la stratégie globale des organisations.

Des organismes à nos côtés pour vous accompagner

Notre établissement entretient des liens avec plus de 200 entreprises et organismes, un réseau développé grâce à l'engagement et au travail de notre Pôle Relations Entreprises.

Moyens pédagogiques

Les étudiants alterneront les périodes à l'école et en entreprise à raison de cinq semaines en entreprise et deux semaines à l'école.

Les enseignements alterneront entre le présentiel, le e-learning, le tutorat, les cas pratiques et les projets tutorés. 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 suivantes :

- Mise en situation simulée
- Etude de cas pratiques
- Soutenances orales

Supports pédagogiques

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

Titre RNCP de niveau 7
«Expert en développement de solutions de cybersécurité» n°38463

Une formation labellisée

Tout savoir sur la formation

SecNumedu ANSSI

CAMPUS RÉGION DU NUMÉRIQUE

FRANCE compétences CERTIFICATION enregistrée au RNCP

Contenu Pédagogique première année

Gouvernance et risques

Management de risque, Audit et Contrôle Interne
Diagnostic organisationnel en cybersécurité
Mise en oeuvre de la cyber résilience
Stratégie de formation et de sensibilisation à la Cybersécurité
SMSI & ISO 27001 – Audit, conception et management
L'essentiel du RGPD
Enjeux géopolitique et risques cyber pour les organisations
NIST CSF
Gestion de projet : méthodologie

Cybersécurité industrielle

Protocoles spécifiques industriel
Fondamentaux développement industriel
Sécurité des infrastructures et communications en environnement industriel
Arduino : implémentation et configuration

Infrastructure et architecture

Architecture des SI
Management des infrastructures IT
Management du Matériel Informatique
Architecture :

- Réseau
- Cloud
- Technique

Intrusion

5 jours de test d'intrusion (pentests):

- Metasploit utilisation basique et pivot dans zone protégée
- Reconnaissance passive & active écoute et empoisonnement du réseau attaques et utilisation des hashs (cracking, relay, pass-the-hash)
- Analyses PingCastle et Bloodhound Quick wins Windows - Low hanging fruits
- Bruteforce et défauts de configuration (externe)

Sécurité des Systèmes d'informations

PKI - Infrastructure de Gestion de Clés
SOC - Analyste niveau 2 et DFIR
Architecture SOC
Gestion des identités et des accès (IAM)
Chiffrement - implémentation

Module complémentaire

Anglais

Préparation et passage certification Ebios Risk Manager

Contenu Pédagogique deuxième année

Gouvernance et risques

La protection des données personnelles dans le monde
Vendor Management : Gestion des fournisseurs et des contrats
Plan de Continuité d'Activité et Plan de Reprise d'Activité
Conception d'un Plan de Réponse à Incident de Sécurité (PRIS)
Réglementations des données de santé en cybersécurité : HDS, HIPAA
Gestion de la preuve en cybersécurité - Forensic
Plan Assurance Sécurité
Gestion de Crise
IA en entreprise : vers une intégration responsable et stratégique
Sécurité dans les projets (ISP)
Mise en conformité :

- CRA
- NIS 2
- DORA

Infrastructure et architecture

Architecture 0 Trust

Intrusion

5 jours de test d'intrusion (pentests):

- Attaques physiques basiques sur un PC (ou VM) Attaques réseau interne en blackbox et greybox
- Mise en place d'un Phishing mail
- Introduction au bug bounty et application des connaissances acquises sur de vrais périmètres
- Introduction aux rapports de pentest

Cybersécurité industrielle

Sécurisation d'un projet industriel
IEC 62443
Analyse de risque & cybersécurité embarquée

Sécurité des systèmes d'information

Analyse forensics
SOC Niveau 3 - Administration d'un SOC
L'implémentation et empoisonnement d'Intelligence artificielle

Modules complémentaires

Anglais
Négociation Salariale

Préparation et passage certification ISO 27001 Implementer

Préparation et passage certification CISSP

Parcours

CyberExpert - Dispositif Former pour l'emploi

Vous êtes en recherche d'emploi ou en reconversion ? Dans le cadre du dispositif « Former pour l'Emploi » de la Région Auvergne-Rhône-Alpes, CSB.school propose trois parcours financés, sans frais pour l'apprenant.

Chaque parcours associe formation en centre, accompagnement individualisé et immersion en entreprise, en lien avec France Travail, les Missions locales et les structures d'insertion.

Trois parcours vers l'emploi

Chaque parcours dure 1 400 heures : 805 h en centre et 595 h en entreprise.

Technicien sécurité réseau : certification professionnelle RNCP42503 (CSB Education Group). Débouchés : technicien systèmes et réseaux, administrateur junior, technicien sécurité.

Analyste SOC : certification professionnelle RNCP42503 (CSB Education Group). Débouchés : analyste SOC junior, technicien sécurité, opérateur cybersécurité.

Chargé(e) de GRC : parcours de professionnalisation, avec préparation à la certification ISO 27001 Lead Implementer. Débouchés : chargé(e) de GRC, assistant(e) RSSI, consultant(e) junior, coordinateur(trice) cybersécurité.

Le programme détaillé (modules et volumes horaires) est disponible sur demande à admission@csb.school.

Les chiffres clés

0 € de frais de formation pour l'apprenant

1 400 h de formation par parcours

595 h d'immersion en entreprise

100 % financé par la Région Auvergne Rhône-Alpes et le Fonds social européen

Comment candidater ?

Les formations Région sont ouvertes aux personnes en recherche d'emploi, en reconversion ou en sécurisation de parcours, orientées par les prescripteurs du service public de l'emploi.

Pour vous inscrire : demandez à votre conseiller France Travail de vous positionner sur la session, postulez sur le portail Ma Formation Mon Emploi ou écrivez à admission@csb.school. La participation à une information collective en présentiel, au Campus Région du numérique, est obligatoire.

Les étapes de l'admission

Trois étapes, après votre inscription :

1. Réunion collective : tests de positionnement technique et de motivation sur place.

2. Entretien individuel : si vos tests sont concluants.

3. Décision : une réponse définitive vous est communiquée peu après.

Tout au long du parcours, CSB.school assure un accompagnement individualisé : bilans intermédiaires, suivi pendant la période en entreprise et appui à l'insertion professionnelle, en lien étroit avec les prescripteurs. Les formations intègrent aussi des modules transversaux : citoyenneté, techniques de recherche d'emploi, communication professionnelle.

Avec le soutien de

La Région Auvergne-Rhône-Alpes

Cofinancé par l'Union européenne

Des débouchés concrets,

Selon l'ANSSI, il manque environ 15 000 experts spécialisés pour répondre aux besoins actuels. D'où l'importance de former, de reconvertir et d'ouvrir le secteur à des profils diversifiés.

Une formation adaptée à tous les métiers de la cybersécurité

CSB.school forme à 30 métiers clés, dans tous les domaines de la cybersécurité :

Technique et opérationnel : Analyste SOC, Pentester, Expert en réponse à incidents...

Stratégie et management : RSSI, Consultant en cybersécurité, Responsable Gouvernance, Risques et Conformité...

Cybersécurité industrielle : Sécurité des systèmes OT/ICS, Architecte en cybersécurité industrielle...

Que deviennent nos diplômés ?

46 % entreprises de services numériques (ESN)

43 % industrie, télécoms, énergie

8 % banque, assurance, finance

3 % secteur public, défense, collectivités

et des témoignages

Esther, alumni - Consultante en cybersécurité
Cette formation se distingue par son approche très concrète. L'alternance et l'accompagnement personnalisé, avec un mentor et un tuteur, favorisent la progression et la prise de confiance.

Werner, alumni - Expert en cybersécurité
Je recommande vivement cette école à toute personne souhaitant évoluer en cybersécurité dans un environnement bienveillant et stimulant.

Rahma, alumni - RSSI adjointe
Cette école a été une véritable opportunité de développement personnel et professionnel. La formation a apporté des outils, des réflexes et une vision globale aujourd'hui pleinement utiles en audit.

Céline Mansuy, intervenante en Finance d'entreprise
Contribuer à la construction professionnelle et préparer au monde de l'entreprise les étudiants est un joli challenge.

Thiébaut Meyer, Director, Office of the CISO, Google Cloud
Avec le développement durable, la formation fait partie des piliers de l'engagement de Google Cloud en France. Nous portons la conviction qu'il faut soutenir la filière cybersécurité à travers des formations professionnalisantes.

Nos actions

Crédit photo Fondation FACE

Crédit photo ADIRA

UNE ÉCOLE ANCRÉE AU SEIN DE L'ECOSYSTÈME CYBER

Au-delà de notre mission de formation, nous contribuons pleinement au dynamisme de l'écosystème cyber. Notre implication se traduit autant par notre participation aux grands rendez-vous du secteur que par l'organisation d'événements dédiés, offrant à nos étudiants des immersions concrètes, une compréhension opérationnelle des enjeux et des connexions durables avec les acteurs du terrain.

Forum InCyber (FIC)

Pour nos étudiants, le FIC est une immersion directe dans l'écosystème européen de la cybersécurité et un accélérateur de compréhension des métiers. Il leur permet de découvrir les enjeux de sécurité et de confiance numérique actuels, d'explorer les innovations du secteur et de rencontrer experts, entreprises, institutions et décideurs.

Journées de la Cyber

Un rendez-vous annuel de deux jours au Campus Région du numérique qui réunit décideurs publics et privés, experts et professionnels autour des enjeux actuels de la cybersécurité et permet à nos étudiants de relier les enseignements théoriques aux problématiques opérationnelles rencontrées dans les organisations.

CSB.Talks

Les CSB.Talks, notre cycle de conférences, créent un pont naturel entre la formation et le monde professionnel. Ils offrent à nos étudiants des interventions d'experts reconnus, des échanges directs sur les parcours et métiers de la cybersécurité, des retours d'expérience concrets, et leur permettent d'élargir leurs perspectives sur l'ensemble de la filière.

Les 24h de la Cyber

Un apprentissage fondé sur l'immersion et le défi. Les 24h de la Cyber combinent exercices techniques, travail en équipe, gestion du stress et du temps, ainsi qu'une réflexion stratégique et opérationnelle. Organisé par le BDE et l'école, ce challenge offre aux étudiants l'occasion de se dépasser.

Ancrage territorial et réseau professionnel

Membre de l'ADIRA et de Digital League, CSB.school s'inscrit pleinement dans l'écosystème numérique régional. Cette double appartenance nous permet de contribuer aux réflexions sur les enjeux IT et cyber des organisations, de renforcer notre proximité avec les entreprises et de préparer nos étudiants aux compétences attendues aujourd'hui et demain.

Une école mobilisée pour l'inclusion et l'accès aux compétences

CSB.school, c'est aussi une école engagée pour l'accès à la formation, la diversité des profils et l'égalité des chances.

La Fondation Cyber Pour Tous

Placée sous l'égide de la Fondation FACE, la Fondation Cyber Pour Tous repose sur une conviction : dans une société où 15 % de la population ne possède pas les compétences numériques de base, la cybersécurité ne doit pas être un domaine réservé à quelques experts, mais un levier d'inclusion, d'autonomie et d'opportunités professionnelles.

La mission de notre Fondation : rendre les métiers de la cybersécurité accessibles au plus grand nombre, afin de faciliter l'insertion et la réinsertion par l'emploi, et sensibiliser le grand public aux enjeux et risques liés au numérique.

Intervention dans les établissements scolaires

CSB.school intervient régulièrement dans les collèges et lycées pour aborder les menaces du quotidien tel que le phishing, les réseaux sociaux, ou l'usurpation d'identité, et développer une culture numérique citoyenne. Au travers de la Fondation Cyber Pour Tous, ces actions s'élargissent à la prévention du cyberharcèlement et à la promotion d'un usage responsable du numérique. Elles permettent aussi de présenter la diversité des métiers cyber, d'aider les jeunes à identifier les débouchés et d'encourager les élèves à envisager des parcours techniques sans se sentir freinés ou illégitimes.

Actions auprès des structures d'insertion

L'école mène également des actions en direction des publics éloignés de l'emploi, en collaboration avec les structures d'insertion telles que les Missions Locales, France Travail ou la Maison Métropolitaine pour l'Insertion et l'Emploi. À travers des ateliers dédiés, nous sensibilisons aux enjeux clés de la cybersécurité, présentons les formations et les métiers de la filière, et apportons les repères nécessaires pour envisager une insertion ou une réinsertion professionnelle dans un secteur en forte demande. Cette démarche vise à ouvrir l'accès aux opportunités offertes par la filière et à répondre aux besoins croissants du marché de la cybersécurité.

Fondation cyber pour tous sous l'égide de FACE

Ces initiatives sont au cœur de notre approche éducative. En participant à des actions de sensibilisation, nos étudiants développent des compétences humaines et citoyennes, tout en se confrontant à des enjeux réels du secteur. Cette articulation entre expertise technique et responsabilité sociale contribue à former des professionnels conscients de leur rôle, capables d'agir pour la protection du numérique et pour un accès plus équitable aux opportunités qu'il offre.

UN CONTEXTE D'ENTREPRISE RÉPLIQUÉ INCLUANT :

Laboratoire réseau

Le laboratoire réseaux est composé de cinq baies complètes intégrant routeurs, switchs et pare-feux professionnels. Il permet aux étudiants de concevoir, configurer et sécuriser des architectures réseaux complexes. Les apprenants y pratiquent le routage, le filtrage, la segmentation et la gestion des flux. Des scénarios d'incidents et d'attaques sont mis en place pour tester la résilience des infrastructures. Ce laboratoire favorise une approche concrète des enjeux de sécurité réseau en entreprise.

Laboratoire industriel (OT)

Le laboratoire industriel comprend trois automates programmables industriels et une sonde de détection dédiée aux environnements OT. Il permet de comprendre les spécificités des systèmes industriels et leurs vulnérabilités. Les étudiants apprennent à sécuriser des chaînes de production et des systèmes critiques.

Environnement simulé de SOC

L'environnement SOC reproduit le fonctionnement d'un centre opérationnel de sécurité en entreprise. Les étudiants y analysent des journaux, des alertes et des incidents de sécurité en temps réel. Ils apprennent à utiliser des outils de détection, de corrélation et de réponse aux incidents. Cet environnement prépare aux métiers de la surveillance et de la réponse à incident.

Plateforme interne de pentest

La plateforme interne de pentest permet de s'exercer aux techniques d'audit et de tests d'intrusion dans un cadre maîtrisé. Les étudiants identifient des vulnérabilités, exploitent des failles et rédigent des rapports d'audit. Cette plateforme développe les compétences offensives indispensables à une vision défensive globale.

LES + DE NOTRE MÉTHODE

Cet équipement immerge les étudiants dans des environnements proches de ceux de l'entreprise et favorise l'apprentissage par la pratique. Ils développent ainsi une compréhension concrète des systèmes, des enjeux de sécurité et des méthodes d'intervention. Cette approche professionnalisante renforce leur employabilité et leur efficacité opérationnelle.

Pour aller plus loin dans les métiers

La cybersécurité est aujourd'hui **au cœur de tous les enjeux numériques**. Les métiers du domaine offrent des carrières variées, durables et en constante évolution, au service de la protection des organisations et des citoyens. CSB.school accompagne les étudiants dans la découverte de ces métiers et la construction de leur avenir professionnel.

Quels sont les métiers les plus recherchés en cybersécurité ?

Le secteur de la cybersécurité est en forte croissance, notamment en raison de la multiplication des cyberattaques. Les métiers les plus demandés actuellement sont :

- Analyste en cybersécurité : il surveille les systèmes et détecte les incidents.
- Ingénieur en sécurité informatique: il conçoit et renforce les infrastructures informatiques.
- Consultant en cybersécurité : il accompagne les entreprises dans leur stratégie de protection des données.
- Pentester (testeur d'intrusion) : il simule des attaques pour identifier les failles de sécurité.
- RSSI (Responsable de la sécurité des systèmes d'information) : il définit et pilote la politique de sécurité d'une organisation.

Ces professions sont recherchées dans de nombreux secteurs : santé, finance, industrie, services publics...

Documentations à consulter

Le guide des futurs professionnels de la cybersécurité
Afin d'accompagner au mieux ces futurs professionnels, nous publions un livret de 28 pages, conçu comme une véritable porte d'entrée vers les métiers et les formations de la cybersécurité.

Les fiches métiers
Découvrez les métiers de la cybersécurité : des professions variées, accessibles à différents niveaux d'études, et particulièrement recherchées sur le marché du travail.

Comment nous rejoindre ?

PARCOURS SPÉCIALISTE CYBERSÉCURITÉ (BAC+3)

Après un Bac+2 en informatique ou en cybersécurité, ou une expérience professionnelle équivalente, avec un niveau d'anglais professionnel.

PARCOURS RESPONSABLE CYBERSÉCURITÉ (BAC+5)

Après un Bac+3 en informatique ou en cybersécurité, ou une expérience professionnelle équivalente, avec un niveau d'anglais professionnel.

FORMATIONS RÉGION

Technicien sécurité réseau, Analyste SOC, Chargé(e) de GRC. Pour les personnes en recherche d'emploi ou en reconversion : inscription par votre conseiller France Travail, sur le portail Ma Formation Mon Emploi ou par e-mail. Une information collective en présentiel est obligatoire (tests de positionnement), suivie d'un entretien individuel.

CONTACT ADMISSIONS

admission@csb.school

ACCESSIBILITÉ ET HANDICAP

Référent handicap : Vianney Wattinne – contact@csb.school

JOURNÉES PORTES OUVERTES, RENTRÉES ET PROCHAINES SESSIONS

Toutes les dates sont sur www.csb.school

N’étudiez pas la cybersécurité, vivez-la !

Réseaux

CSB.school
@schoolcsb

Coordonnées

contact@csb.school
07 49 69 38 11
www.csb.school

Adresse

78 route de Paris, 69260
Charbonnières-les-Bains
Visite du campus possible