Cybersécurité

Responsable en sécurité des systèmes d'information

Mentor individuel Diplôme de niveau 7 (bac +5) *

Mettez en œuvre une stratégie de cybersécurité dans votre entreprise et déployez-la en continu

PÉRIODE DE FORMATION
12 mois à temps plein
24 mois en alternance**

DURÉE DE LA FORMATION
1135 heures supervisées

OPENCLASSROOMS

La formation demande un investissement en temps estimé à 2270 heures : 1135 heures de formation supervisée (projets encadrés par des mentors) et 1135 heures de formation guidée (cours et des ressources pédagogiques). En alternance, la durée totale ne comprend pas le temps passé en entreprise.
La période de formation peut être rallongée en cas de formation à temps partiel. La durée est estimée et dépend du niveau d'entrée en formation, de la disponibilité, du temps alloué par semaine et des capacités et rythmes d'apprentissage de l'étudiant.

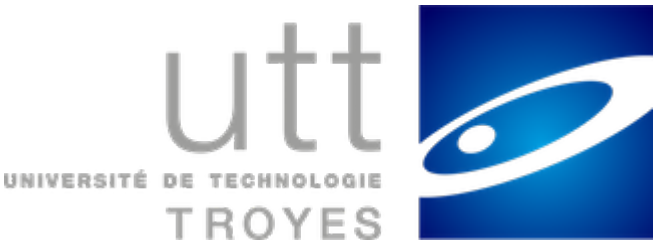
*Master - Ingénierie des systèmes complexes - code NSF 110 - Diplôme de niveau 7 (bac +5) - certification professionnelle enregistrée au Répertoire National des Certifications Professionnelles (RNCP) par décision de France compétences publiée le 01/09/2019

** Vérifiez l'éligibilité du parcours en fonction de votre contrat d'alternance (professionnalisation ou apprentissage).

Formation mise à jour le 9 déc. 2024

Financez ce parcours grâce à vos crédits CPF directement depuis la plateforme Mon Compte Formation :

Temps complet - 12 mois
Temps partiel - 18 mois



Université de Technologie de Troyes (UTT)

Qu'est-ce qu'un responsable en sécurité des systèmes d'information ?

L'objectif de la cybersécurité, c'est de protéger les systèmes d'information (serveurs, réseaux, PC, mobile, objets connectés...), les applications et les données traitées par ces différents systèmes. En effet, aucun système n'est parfait et le risque zéro n'existe pas. La cybersécurité consiste à diminuer ce risque et réagir efficacement aux attaques. Chaque jour, dans tous les domaines (e-commerce, défense, banques), les systèmes d''information sont attaqués. En réponse, les entreprises s'équipent de mieux en mieux : en 2015, 81 % des entreprises déclaraient avoir eu un problème de sécurité de l'information, et 60 % avaient augmenté le budget consacré à ce poste. Au niveau mondial, d'après une étude cabinet Gartner, 90 milliards de dollars ont été consacrés à la cybersécurité en 2017.

Si le secteur est en forte croissance, les experts sont encore rares. D'après l'agence nationale de la sécurité des systèmes d'information (ANSSI), 25 % seulement des besoins en recrutement du domaine sont couverts.

Le Responsable en Sécurité des systèmes d'information (RSSI - en anglais CISO) est le garant de la sécurité informatique d'une organisation. C'est lui ou elle qui définit la stratégie de gestion des risques, en lien avec la DSI et la Direction Générale. Il est chargé de définir la politique de sécurité SI adaptée aux besoins, et d'établir les indicateurs de performance. Enfin, il veille à la mise en œuvre de la politique et des plans de sécurité SI dans le respect du cadre réglementaire.

Depuis mai 2018, la nouvelle réglementation européenne sur la Protection des données (RGPD) renforce les responsabilités du RSSI et obligations des entreprises dans le domaine de la protection des données. En conséquence, il devient une nécessité pour

les entreprises d'avoir un RSSI qui s'occupe exclusivement de la Sécurité SI.

Selon la taille de l''entreprise, il peut travailler sous la direction du DSI ou mais peut également avoir un rôle transversal (à la fois organisationnel et technique) qui a tendance à s'émanciper de la DSI. Parfois même, il peut être recruté en tant que consultant afin d'accompagner les entreprises dans cette stratégie.

Suivez cette formation en ligne pour obtenir le Master 2 "Sciences, technologies, Santé, Mention Ingénierie des systèmes complexes, Spécialité sécurité des systèmes d'information*" (Bac+5) enregistré au RNCP délivré par l'Université de technologie de Troyes (UTT).

Les prérequis pour postuler

Pour accéder à la formation, vous devez obligatoirement justifier des prérequis suivants :

- Être titulaire d'un bac+5, ou d'une certification professionnelle de niveau 7, ou d'un Bac+4 en :
  - Informatique
  - Réseaux et télécommunications
  - Systèmes d'information et réseaux
- ou, être titulaire de la certification Administrateur systèmes, réseaux et sécurité délivrée par OpenClassrooms

Langues

Pour les candidats dont le français n'est pas la langue maternelle, un justificatif d'un niveau de français B2 minimum (niveau courant) sur l'échelle européenne du CECRL sera également demandé.

La maîtrise de l'anglais au niveau B1 du CECRL est exigée. Un justificatif officiel valide, parmi les suivants, devra être transmis avant la fin de la formation pour obtenir votre diplôme :

- Linguaskill - min. score 140 pour un niveau B1
- Bulats - min. score 40
- TOEIC - min. score 550
- IELTS - min. score 3.5
- TOEFL ibt - min. score 57
- CAMBRIDGE FCE / CAE / BEC HIGHER / BEC VANTAGE - score/grade B ou 140 minimum.

Il est donc essentiel que vous l'ayez obtenu en fin de formation.

Matériel

Pour suivre la formation et être évalué, vous devez avoir accès à un ordinateur (PC ou Mac avec processeur Intel), muni d'un micro et d'une webcam et disposer d'une bonne connexion Internet (3.2 Mbps en envoi et 1.8 Mbps en réception de données). Vous pouvez tester la qualité de votre connexion via cet article. Pour mettre en œuvre les compétences, vous devrez également :

- travailler sur un ordinateur muni au minimum d'un processeur multi-cœurs, de 8Go de RAM et de 100Go d'espace de stockage disponibles ;
- être administrateur de votre ordinateur afin de pouvoir installer des programmes complémentaires.

Vous ne répondez pas aux critères d'admissibilité ?
Nous vous invitons à déposer votre candidature, un conseiller en formation étudiera votre dossier et vous recontactera pour identifier des voies d'accès alternatives, comme par exemple la **valorisation des acquis professionnels (VAP)** dans le cas d'une expérience significative en informatique.

Ce que vous saurez faire

- Définir et mettre en œuvre la politique de sécurité
- Procéder à un audit des systèmes d'information et préconiser des évolutions
- Gérer les risques de l'entreprise dans le respect des réglementations (GDPR...)
- Conduire et accompagner des projets de sécurité des SI
- Mettre en place des techniques de sécurité afin de détecter des intrusions
- Organiser les processus de traitement et de gestion des incidents
- Mettre en œuvre le processus forensic
- Sécuriser les infrastructures réseaux et systèmes et les applications web
- Développer et promouvoir la politique auprès de tous les acteurs

Quels métiers vous pourrez exercer

Ce parcours donne accès aux métiers suivants :

- Responsable Sécurité des SI
- Responsable cybersécurité
- Consultant en sécurité des SI
- Ingénieur sécurité informatique
- Auditeur sécurité des SI

Retrouvez sur cette page les indicateurs de performance des formations

OpenClassrooms.

Les rémunérations

En suivant la formation "Responsable en sécurité des systèmes d’‘information", vous pouvez prétendre aux rémunérations suivantes :

- Débutant : 40 000 € à 75 000 € annuels bruts
- Expérimenté : 80 000 € à 100 000 € annuels bruts (parfois même jusqu'à 200 000 € !)

Comment obtenir ce diplôme ?

Pour obtenir le diplôme national de Master 2 "Sciences, Technologies, Santé, Mention Ingénierie des systèmes complexes, Spécialité sécurité des systèmes d'information", vous devrez :

- Effectuer votre **inscription administrative** auprès de l'Université Technologique de Troyes, par l’intermédiaire d’OpenClassrooms.
- Fournir un **justificatif de niveau d'anglais B1 en cours de validité ;**
- Réaliser et valider **la totalité des projets** du parcours OpenClassrooms (400h).
- Réaliser une application professionnelle obligatoire (20 à 26 semaines, à temps plein) en lien avec la sécurité informatique :
    - Si vous êtes en formation initiale : effectuer un **stage obligatoire** et rédiger un rapport de stage (soit 735h).
    - Si vous êtes salarié.e ou en alternance : effectuer une **mission en entreprise** et rédiger un rapport de mission.

Projet 1 - 10 heures

Démarrez votre formation de Responsable en sécurité des Systèmes d'information

Mettez-vous dans les meilleures conditions pour réussir votre parcours : projetez-vous dans votre formation, définissez votre planning et appropriez-vous les outils essentiels pour apprendre.

Compétences cibles

- Définir le cadre de votre formation

Cours associés

Engagez-vous dans votre formation OpenClassrooms

Facile 2 heures

Prenez en main votre parcours OpenClassrooms et réalisez votre premier projet en suivant ce cours conçu pour vous accompagner dans ces premières étapes de formation.

Projet 2 - 10 heures

24h dans la peau d'un Responsable en sécurité des Systèmes d'information

A partir de témoignages, vous découvrirez les missions au quotidien d'un RSSI et commencerez à clarifier votre projet professionnel

Compétences cibles

- Construire pas à pas son projet professionnel
- Identifier vos compétences existantes et vos motivations pour ce métier

Cours associés

Construisez votre projet professionnel

Facile 6 heures

Vous souhaitez booster votre carrière ? Construisez votre projet pas à pas et ouvrez-vous de nouvelles perspectives professionnelles !

Découvrez l'univers de la cybersécurité

Facile 4 heures

Comprenez le déroulement des cyberattaques, enjeu majeur de société, et découvrez l'ensemble des métiers qui participent à la cybersécurité. Peut-être vous demain ?

Optimisez votre apprentissage avec l'Intelligence Artificielle

Facile 6 heures

Utiliser l’IA en gardant un esprit critique, pour acquérir plus rapidement des compétences, gagner en productivité et mieux organiser votre planning d’apprentissage.

Projet 3 - 50 heures

Sécurisez l'infrastructure SI d'une entreprise

À partir d'une demande d'un client, vous proposerez une architecture SI sécurisée.

Compétences cibles

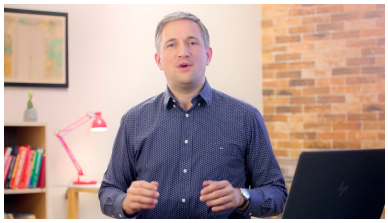
- Sécuriser un serveur web Apache
- Sécuriser Windows avec Active Directory
- Configurer des VLAN avec un switch
- Configurer un pare-feu
- Installer une infrastructure virtuelle
- Configurer un serveur Linux sécurisé

Cours associés

Centralisez et sécurisez votre annuaire Active Directory

Moyenne 8 heures

Avec ce cours, apprenez à maîtriser Active Directory. Ce service d'annuaire basé sur LDAP vous aidera à centraliser l'identification et l'authentification des ressources.



Sécurisez vos infrastructures

Difficile 10 heures

Apprenez à sécuriser vos infrastructures des attaques physiques mais aussi des cyber attaques grâce aux protocoles, firewalls et autres techniques ! Dans ce cours, vous aborderez les types de hacking les plus connus et comment vous en protéger.

Initiez-vous à Linux

Facile 8 heures

Dans ce cours débutant, découvrez Linux : un système d'exploitation gratuit et fascinant qui vous donnera un contrôle sans précédent sur votre ordinateur ! Créé par des passionnés d'informatique, Linux est un vecteur important de la philosophie du libre et l'alternative parfaite à Windows ou macOS.

Simulez le schéma de votre réseau avec Cisco Packet Tracer

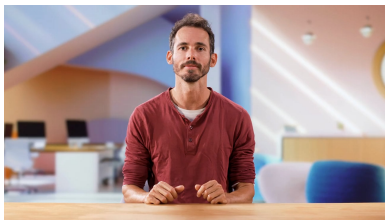
Moyenne 12 heures

Apprenez à simuler votre schéma de réseau d'entreprise avec l'outil Cisco Packet Tracer : configurez et sécurisez votre réseau.

Administrez un système Linux

Moyenne 10 heures

Initiez-vous à l'administration d'un serveur Linux : utilisez le terminal et le shell, manipulez des fichiers, configurez un réseau et surveillez l'activité du système !



Virtualisez vos environnements de travail

Facile 6 heures

Découvrez la virtualisation et les machines virtuelles. Distinguez les types d'hyperviseurs et virtualisez vos environnements de test et l'architecture de vos systèmes d'information !

Projet 4 - 50 heures

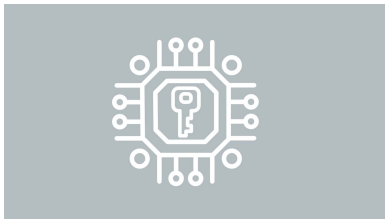
Sécurisez une application du SI

Afin d'aider votre entreprise à réaliser une application web sécurisée pour accéder à son SI existant, vous proposerez la liste des vulnérabilités et rédigerez votre proposition pour présenter votre solution technique.

Compétences cibles

- Rédiger des tests de sécurité
- Détecter les vulnérabilités dans le code
- Définir les exigences de sécurité

Cours associés



Sécurisez vos données avec la cryptographie

Moyenne 8 heures

Maîtrisez les bases de la cryptographie afin de chiffrer vos données et ainsi, développer par exemple des signatures électroniques, des certificats, hacher les mots de passe, faire de la communication sécurisée, etc.

Sécurisez vos applications

Moyenne 10 heures

Les applications sont vulnérables aux cyber-attaques. Dans ce cours, vous apprendrez à identifier les vulnérabilités et à proposer des bonnes pratiques à vos développeurs pour vous en protéger : mécanismes d'authentification, échappements de caractères, TLS...

Sécurisez vos applications web avec l'OWASP

Moyenne 10 heures

Pour créer une application de qualité, vous devez définir son modèle de sécurité ! Apprenez à appliquer les techniques de OWASP, une communauté qui fournit des outils inestimables pour réduire les risques de sécurité dans le développement web.

Projet 5 - 60 heures

Auditez la sécurité SI de l'entreprise

A partir de l'architecture SI de l'entreprise et de la politique SSI, vous proposerez un plan d'audit de sécurité contenant un audit externe et un audit interne.

Compétences cibles

- Conduire des tests d'intrusion
- Rédiger un plan d'audit

Cours associés

Construisez votre stratégie d'audits et de contrôles cybersécurité

Moyenne 6 heures

Cartographiez les différentes typologies d'audits et contrôles existants, et construisez sur cette base une stratégie d'audits adaptée à vos besoins.

Réalisez un test d'intrusion web

Moyenne 10 heures

Mettez-vous dans la peau d'un attaquant et réalisez un test d'intrusion de A à Z sur une application web, grâce à la méthode et aux outils d'un pentester professionnel !

Planifiez une politique d'audit au sein de votre entreprise

Difficile 8 heures

Déterminez une stratégie d'audit, puis planifiez les audits, préparez-les et réalisez-les pour apporter de la valeur à votre entreprise.

Projet 6 - 50 heures

Mettez en place la surveillance de la sécurité SI

A partir de l'architecture Si d'une entreprise, vous proposerez une architecture de surveillance SI, ses règles et des procédures de traitement d'alertes.

Compétences cibles

- Configurer la journalisation des éléments du SI
- Proposer des scénarios de corrélation
- Concevoir une architecture de surveillance de la sécurité SI

Cours associés

Optimisez la sécurité informatique grâce au monitoring

Difficile 8 heures

Apprenez à sécuriser votre système d'information en optimisant la collecte et la remontée de logs pour en tirer des scénarios de corrélation pertinents.

Simulez le schéma de votre réseau avec Cisco Packet Tracer

Moyenne 12 heures

Apprenez à simuler votre schéma de réseau d'entreprise avec l'outil Cisco Packet Tracer : configurez et sécurisez votre réseau.

Plongez dans l’univers de la détection et des réponses aux incidents cyber

Moyenne 6 heures

Découvrez comment détecter et traiter les incidents de cybersécurité en participant à la création et à l'amélioration d'un SOC.

Projet 7 - 60 heures

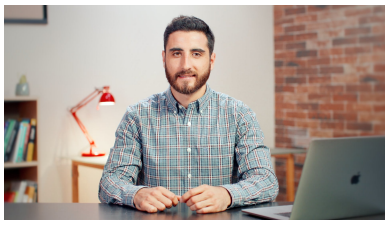
Investiguez un incident de sécurité

A partir de logs réseau, systèmes et applicatifs, vous effectuerez une analyse forensique pour détecter les attaques qui ont été menées et rédigerez un rapport d'incident qui évalue l'impact des attaques SI.

Compétences cibles

- Réaliser une analyse forensics
- Rédiger un rapport d'incident de sécurité

Cours associés



Menez une investigation d’incident numérique forensic

Difficile 20 heures

Menez une investigation numérique forensic suite à une cyber attaque. Identifiez vos indicateurs de compromission et rédigez des recommandations dans un rapport d'incident de sécurité.

Projet 8 - 10 heures

Créez et présentez votre CV pour un entretien

Dans ce projet, vous réalisez votre CV pour rechercher votre stage ou votre premier job dans la sécurité des SI !

Compétences cibles

- Réaliser un CV

Projet 9 - 90 heures

Gérez le risque SI d'une organisation

A partir des informations métier et organisationnelles d'une entreprise, du contexte des menaces et des obligations légales, vous identifierez les menaces sur la sécurité SI et évaluerez l'impact des attaques pour proposer une politique de sécurité.

Compétences cibles

- Analyser les risques SI
- Rédiger une Politique de Sécurité SI

Cours associés

Analysez et gérez des risques SI

Moyenne 4 heures

Grâce à ce cours, vous maîtriserez les différentes étapes d'analyse de risques de votre Système d'Information, de l'analyse de votre contexte à l'élaboration et la mise en œuvre d'un plan d'action. Vous découvrirez comment identifier, analyser et traiter les risques.

Définissez la politique de sécurité de votre entreprise

Difficile 8 heures

Mettez en place une politique de sécurité (PSSI) ! Découvrez les standards de sécurité, mettez en place un système de management de sécurité info (SMSI) et rédigez la politique de sécurité SI.

Gérez un projet digital avec une méthodologie en cascade

Facile 8 heures

Vivez la gestion de projet avec une méthodologie classique. Apprenez à gérer les 5 phases d'un projet en cascade : l'initialisation, le lancement, la conception, la production et l'exploitation.

Initiez-vous à la gestion de projet agile

Facile 6 heures

Formez votre équipe agile, prenez en compte le besoin des utilisateurs et développez des pratiques agiles comme le Planning Poker, les méthodes Kanban et Lean...

Mettez en place un plan de continuité d'activité (PCA)

Difficile 6 heures

Découvrez comment mettre en place un plan de continuité d'activité (PCA), en vous appuyant sur la norme ISO 22301, afin de réduire les impacts des sinistres et assurer une reprise d'activité efficace.

Maîtrisez les risques juridiques liés au numérique

Moyenne 12 heures

Mener un projet numérique nécessite de maîtriser certains risques juridiques, en particulier à l'heure du RGPD. Suivez ce cours pour mieux comprendre ces enjeux et connaître les fondamentaux pour ne pas faire de faux pas en droit du numérique !

Gérez vos risques cyber avec EBIOS RM

Difficile 8 heures

Découvrez comment maîtriser la méthode EBIOS RM pour gérer les risques cybersécurité, de l'analyse stratégique à la mise en œuvre d'actions concrètes.

Projet 10 - 10 heures

Réalisez une veille sur les menaces et les solutions

Réalisez une veille technologique sur les vulnérabilités, les attaques et la réglementation, et rédigez un rapport de veille en évaluant des produits de sécurité du marché.

Compétences cibles

- Effectuer une veille technologique, réglementaire, économique sur la sécurité des SI

Cours associés

Mettez en place un système de veille informationnelle

Facile 4 heures

Apprenez à faire de la veille pour vous adapter aux évolutions de votre métier et à utiliser des outils de veille informationnelle.

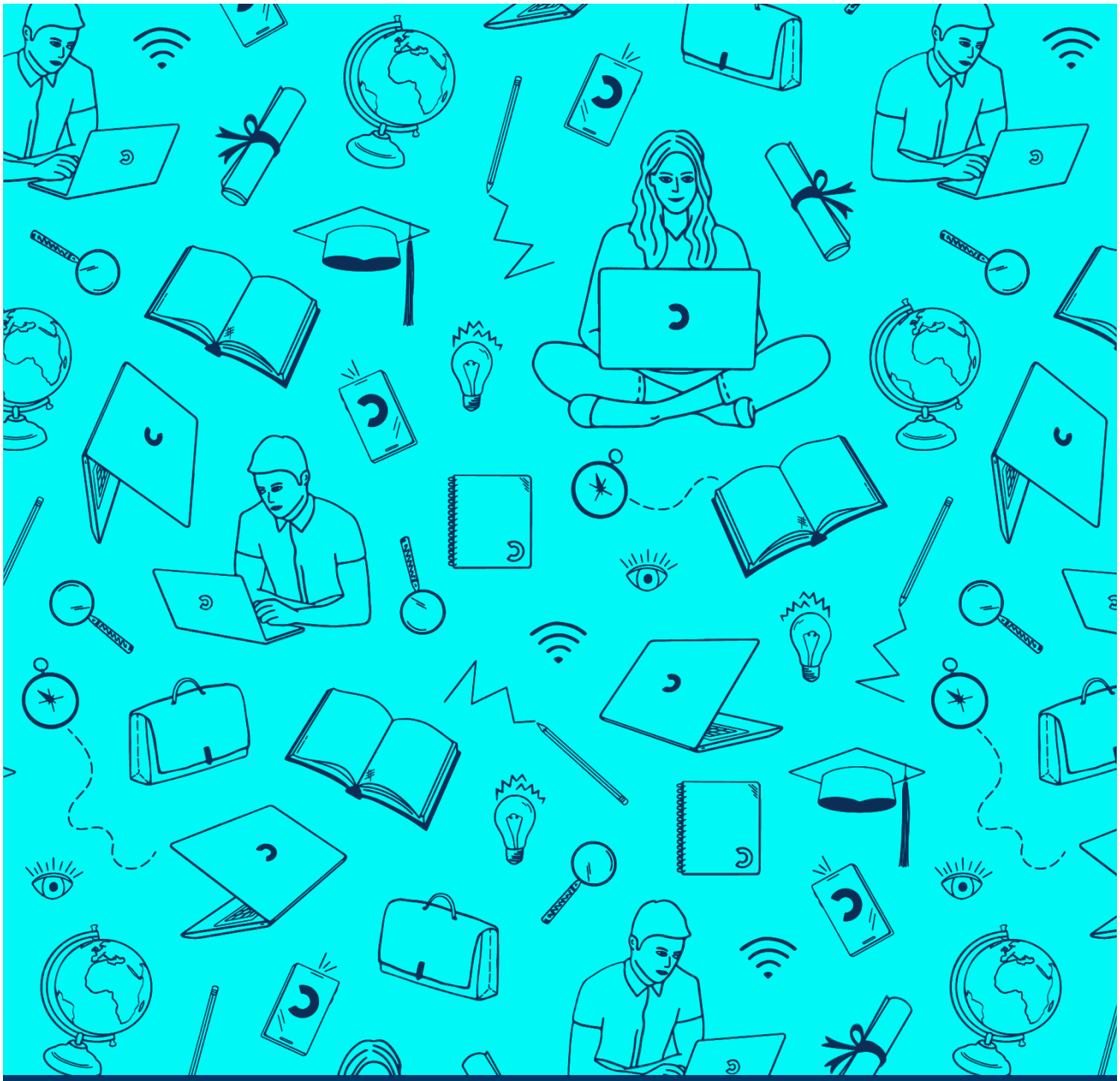
Projet 11 - 735 heures

Réalisez un stage (ou une mission en entreprise) dans la sécurité des systèmes d'information

Pour valider votre formation, vous allez devoir effectuer un stage de 6 mois (20 à 26 semaines) afin de mettre en pratique vos compétences de futur Responsable en sécurité des systèmes d'information.

Compétences cibles

- Effectuer un bilan de formation



L'alternance par OpenClassrooms. Pratique et pratique.

Apprenez où que vous soyez

Pas besoin de déménager pour se former : choisissez une entreprise près de chez vous et formez-vous en ligne

Côté étudiant :

L' alternance à tout âge avec OpenClassrooms

Démarrez une nouvelle carrière avec nos formations en alternance 100% en ligne ! Véritables accélérateurs de carrière, elles sont diplômantes, rémunérées et financées par des entreprises partout en France. Débutez où vous voulez, pendant toute l’année.

La pédagogie et l'expérience OpenClassrooms, les clés de votre réussite

- **Apprenez où que vous soyez**

Pas besoin de déménager pour se former : choisissez une entreprise près de chez vous et formez-vous en ligne.

- **Travaillez sur des projets professionnalisants**

Réalisez des projets concrets, issu de scénarios métiers, directement applicables en entreprise.

- **Un mentor pour vous accompagner**

Bénéficiez chaque semaine des conseils d'un expert du métier qui vous aide à progresser tout au long de votre formation.

- **Un salaire et aucun frais**

L'entreprise paie votre formation et vous verse un salaire mensuel, calculé selon votre situations personnelle.

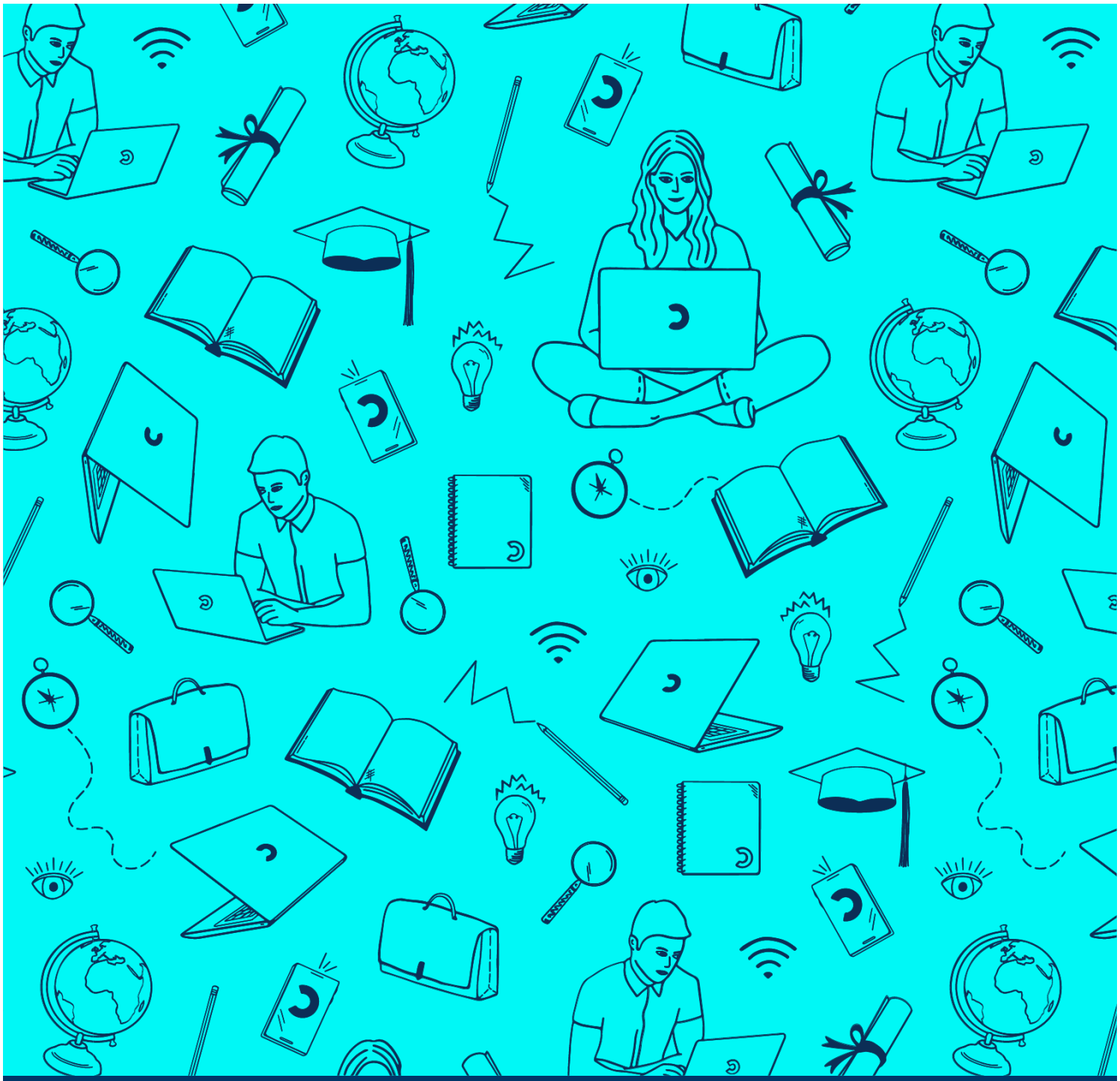
Côté employeur :

Recrutez et formez les talents de demain avec l'alternance

Recrutez parmi notre base de candidats et formez vos futurs talents sur les métiers en tension grâce à l'alternance.

Accédez gratuitement aux alternants OpenClassrooms

- **Découvrez des profils motivés et de qualité**
  Trouvez des candidats qui correspondent réellement à vos besoins.
- **Recrutez rapidement grâce à notre base d'alternants.**
  Dénichez vos futurs talents via votre espace recruteur.
- **Réalisez vos démarches administratives facilement**
  Finie la paperasse : nos équipes s'occupent aussi de l'administratif.



Pourquoi l'alternance en ligne ?

Les avantages de l’alternance OpenClassrooms sont nombreux : **date de début flexible, formations créées par des experts métiers, accompagnement personnalisé, formation financée...**

1. Un salaire et une formation financée par l'entreprise, qui dit mieux ?

La formation en alternance, c'est 0 frais pour l'étudiant car financée par l'entreprise. Et comme pour toute alternance, vous percevrez un salaire durant votre formation.

2. Un rythme d'alternance flexible : pratique pour vous et pour votre entreprise

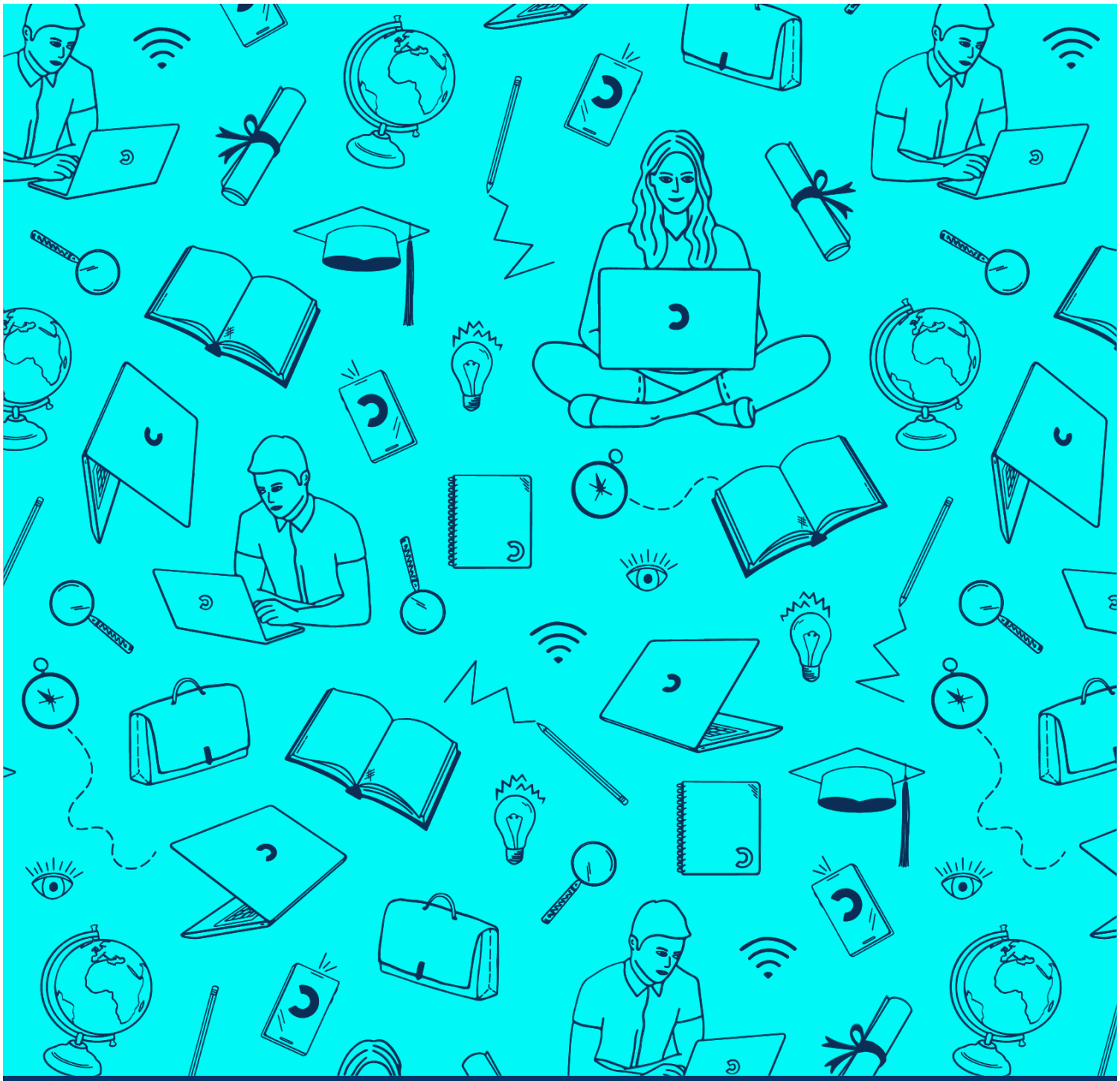
Votre contrat peut démarrer à tout moment de l'année, plus besoin d'attendre septembre ou janvier ! Le rythme d'alternance prévoit 3 ou 4 jours en entreprise par semaine et les jours de formation peuvent être adaptés.

3. Une formation au plus proche de la réalité du métier

Nos formations sont conçues avec des experts reconnus dans leur domaine, pour répondre aux besoins des entreprises. Elles sont inscrites au Répertoire national des certifications professionnelles (RNCP) et sont reconnues par l'Etat.

4. En ligne, mais toujours bien accompagné

Parce que se former n'est jamais facile, vous êtes suivi individuellement par un mentor, qui vous aide à progresser. Notre équipe de conseillers pédagogiques est aussi là pour vous accompagner à chaque étape de votre parcours.



Tout savoir sur les contrats d'alternance

Une question ? Un projet ?

Contacter : **job.placement@openclassrooms.com**

Contrat de professionnalisation

4 jours par semaine (jours au choix) avec présence réduite à 3 jours 1 à 2 fois par mois.

- L'entreprise embauche l'étudiant en CDD sur 12 ou 24 mois (selon le parcours de formation).
- La formation est financée par un OPCO. OpenClassrooms est référencé dans les principaux OPCO grâce à ses titres certifiés et sa certification Datadock.
- L'entreprise fait la démarche de demande de prise en charge auprès de son OPCO. Nos équipes sont présentes à chaque étape pour l'accompagner.
- L'étudiant est rémunéré **sur une base qui va de 65% à 100% du SMIC** (pour un étudiant de plus de 26 ans).
- Si l'étudiant a plus de 26 ans et est demandeur d'emploi, France Travail octroie une aide à l'emploi à l'entreprise.