



Responsable en sécurité des systèmes d'information

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



Durée de la formation :
1135 heures



Emploi garanti**



Durée de la formation en alternance :
24 mois



Temps d'études conseillé à temps plein :
12 mois



Master (Bac+5)

*Sciences, technologies, Santé, Mention Ingénierie des systèmes complexes, Spécialité sécurité des systèmes d'information - NSF 326p - Master (Bac+5) - enregistré au RNCP par arrêté du 25/04/2002 publié au JO du 27/04/2002

**Conditions disponibles sur la page <https://openclassrooms.com/fr/job-guarantee>

Financez ce parcours grâce à vos crédits CPF directement depuis la plateforme Mon Compte Formation. [Plus d'infos](#) (Temps complet - 12 mois). [Plus d'infos](#) (Temps partiel - 18 mois).



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).

Prérequis

Pour accéder à cette formation, vous devez **obligatoirement** remplir ces prérequis :

- Niveau exigé : Diplôme national ou Titre de niveau I ou Bac +4 ou Diplôme d'ingénieur en :
 - Informatique
 - Réseaux et télécommunications
 - Systèmes d'information et réseaux
- La maîtrise de l'anglais au niveau B1 du CECRL est exigée.

Un **justificatif officiel valide de niveau d'anglais B1** vous sera demandé pour obtenir votre diplôme. C'est donc essentiel que vous l'ayez obtenu en fin de formation.

- Pour les apprenants étrangers, un niveau de français B1-B2 (utilisateur indépendant) est conseillé pour la réussite de la formation.
- Accès à un ordinateur (PC ou Mac), muni d'un micro, d'une webcam ainsi que d'une bonne connexion internet pour les séances de mentorat (3.2 Mbps en envoi et 1.8 Mbps en réception de données). Pour tester la qualité de votre connexion, cliquez sur ce [lien](#). De plus, pour mettre en œuvre les compétences, vous devrez :
 - 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 n'avez pas ces prérequis mais vous pensez avoir un niveau équivalent de par vos expériences ? Si vous avez un niveau licence et de l'expérience professionnelle significative dans le domaine visé, c'est quand même possible ! Remplissez ce [formulaire de validation](#) afin que nous puissions confirmer votre niveau.

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 :

- Réaliser et valider **la totalité ses projets** du parcours OpenClassrooms (400h).

- Si formation initiale : Effectuer un **stage obligatoire de 21 semaines** et rédiger un rapport de stage (soit 735h).
- Si formation en alternance : Effectuer votre alternance en **entreprise** et rédiger un rapport d'alternance.
- Si vous êtes salarié.e : Effectuer une mission dédiée dans votre entreprise et rédiger un rapport de mission.

Un **justificatif officiel valide de niveau d'anglais B1** vous sera également demandé pour obtenir votre diplôme.

Votre dossier sera ensuite étudié et validé par **le jury de l'Université de Technologie de Troyes**.

Si vous en avez besoin, utilisez les cours que nous vous proposons pour vous préparer aux projets.

Projet 1 - 10 heures

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

Dans ce projet, vous préparez votre méthodologie d'apprentissage en ligne en réalisant un plan.

Compétences cibles

- Personnaliser un programme de formation
- Fixer des objectifs clairs
- Créer et mettre à jour votre CV
- Comprendre votre environnement de travail

Cours associés



Apprenez à apprendre

 Facile

 6 heures

Être capable d'apprendre vite et bien est une compétence clé dans n'importe quel domaine. Suivez ce cours pour améliorer votre capacité d'apprentissage !

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

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

Cours associés



Construisez votre projet professionnel

 Facile  8 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  1 heure

La cybersécurité devient chaque jour un enjeu majeur pour les citoyens, les gouvernements et les entreprises. Pourquoi faut-il s'en préoccuper et comment s'organiser ?

Projet 3 - 50 heures

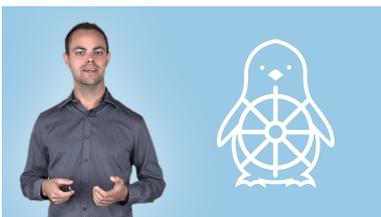
Sécurisez l'infrastructure SI d'une entreprise

A partir de la description de la SI d'une entreprise et de la feuille de route RSSI, vous proposerez une architecture SI sécurisée.

Compétences cibles

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

Cours associés



Reprenez le contrôle à l'aide de Linux !

Facile 30 heures

Linux est un système d'exploitation qui fait tourner les programmes de votre machine, à l'instar de Windows et Mac OS X. Créé par des communautés de passionnés d'informatique, il vous donne un contrôle sans précédent sur votre machine... et il est gratuit !



Simulez des architectures réseaux avec GNS3

Facile 6 heures

Apprenez à simuler votre architecture réseau à l'aide du simulateur GNS3, afin d'optimiser votre production en réalisant vos tests.



Centralisez et sécurisez votre annuaire Active Directory

 Moyenne  8 heures

Active Directory est un service d'annuaire basé sur LDAP. Vous apprendrez à le maîtriser pour centraliser l'identification et l'authentification des ressources d'un réseau.



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.

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

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

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...

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



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.



Conduisez un test d'intrusion

 Difficile  8 heures

Apprenez à réaliser, pas à pas, un test d'intrusion (ou pentest) en mettant en place une méthodologie et des outils ! Vous saurez effectuer vos tests d'intrusion et finaliser votre audit, par la rédaction d'un rapport.

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

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

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.

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

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

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

Cours associés



Rédiger un CV efficace



Facile



2 heures

Votre CV est un document évolutif, vivant, qui va devenir votre passeport ! Suivez nos conseils : vous en serez fier et il vous permettra de susciter l'intérêt des recruteurs pour aller décrocher un entretien de recrutement.

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 évalueriez l'impact des attaques pour proposer une politique de sécurité.

Compétences cibles

- Rédiger une Politique de Sécurité SI
- Analyser les risques 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

Vous devez vous approprier les bonnes pratiques de l'intelligence collective et de l'expérience utilisateur pour coacher votre équipe.



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 !

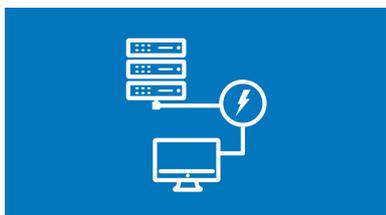
Réalisez une veille sur les menaces et les solutions

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



Effectuez votre veille en cybersécurité

 Facile  1 heure

L'univers de l'IT et de la cybersécurité évolue très vite ! Il est donc important que vous appreniez à effectuer votre veille en ayant les sources les plus fiables.



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.

Réalisez un stage dans la sécurité des systèmes d'information

Pour valider votre formation, vous allez devoir effectuer un stage de 6 mois (21 semaines) afin de mettre en pratique vos compétences de futurs Responsable en sécurité des systèmes d'information.

Compétences cibles

- Effectuer un bilan de formation

Cours associés



Rédigez votre rapport de stage

 Facile

 30 minutes

Le stage en entreprise est une étape décisive de votre formation. Afin d'en tirer le maximum et d'en rendre compte au mieux, vous allez produire un rapport de stage. Suivez ce mini-cours pour apprendre à rédiger un rapport de stage aussi enrichissant que convaincant !



alternance

OpenClassrooms, 1^{ère} école en ligne
à proposer des formations diplômantes

L'alternance en ligne permet à l'entreprise et à l'étudiant de trouver le **meilleur rythme** adapté à leurs besoins respectifs.

Côté étudiant :

une formation diplômante et 100% financée

L'alternance est une modalité de formation qui mêle acquisition des connaissances (en ligne) et des compétences (en entreprise).

Comment se déroule un parcours en alternance OpenClassrooms ?

- Après avoir choisi le parcours de formation qui lui convient, **l'étudiant bénéficie d'un accompagnement gratuit de 2 mois pour trouver son entreprise.**
- La formation peut se réaliser en contrat de professionnalisation ou d'apprentissage. Rendez-vous à la page suivante pour savoir lequel choisir !

Est ce que la formation en alternance a un coût pour l'étudiant ?

- La formation en alternance est gratuite ! Une rémunération est également prévue : jusqu'à 100% du SMIC en fonction de votre âge et de votre année de formation.
- Pour se lancer, une seule adresse : openclassrooms.com/fr/apprenticeship

Côté entreprise :

l'accès à des profils qualifiés toute l'année, en toute simplicité !

OpenClassrooms est la 1ère école en ligne à proposer des **formations en alternance, aux titres reconnus par l'État** de niveau Bac+2 à Bac+5, sur des **métiers en tension, très recherchés par les recruteurs**. Les formations en alternance **peuvent être financées, soit par la taxe d'apprentissage, soit par les OPCO (Opérateurs de Compétences)**.

Comment lancer des parcours d'alternance au sein de l'entreprise ?

- Pour chercher des profils à recruter en alternance ou lancer le recrutement d'un étudiant déjà identifié, n'hésitez pas à contacter :

job.placement@openclassrooms.com

- Les équipes d'OpenClassrooms vous accompagnent à chaque étape d'une démarche d'alternance, du dossier de financement au suivi de vos alternants.

Quand peut-on lancer une démarche d'alternance au sein de l'entreprise ?

- À tout moment : le contrat peut démarrer tout au long de l'année, il n'y a pas de date de rentrée imposée.



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. Une formation gratuite pour l'étudiant et financée pour l'entreprise

- La formation est gratuite.
- Dans le cadre d'un **contrat de professionnalisation, elle est 100% financée** par votre OPCO.
- Dans le cadre d'un **contrat d'apprentissage**, elle est financée par la taxe d'apprentissage que paient les entreprises privées.

3. Une formation de qualité, conçue pour une application directe au sein de l'entreprise.

- Les formations OpenClassrooms sont **professionnalisantes**. Elles sont conçues par et pour l'entreprise, sur des métiers recherchés.
- Les formations OpenClassrooms sont de qualité, avec des **diplômes inscrits au RNCP** (Répertoire National des Certifications Professionnelles) et dont les niveaux sont reconnus par l'État.
- Une plateforme collaborative favorise les échanges entre apprentis et aide à la recherche d'emploi.
- Des espaces de coworking sont proposés dans toute la France.

2. Une solution flexible, adaptée aux besoins de l'étudiant et de l'entreprise

- Le contrat peut démarrer **à tout moment de l'année**.
- Il est possible de faire soit un contrat de professionnalisation, soit un contrat d'apprentissage.
- Le(s) **jour(s)** dédié(s) à la **formation** est (sont) **flexible(s)** en fonction de l'organisation de l'étudiant et de l'entreprise.

4. Un accompagnement dédié à chaque étape, pour l'étudiant comme pour l'entreprise

- Des **profils d'étudiants disponibles et pré-sélectionnés par nos experts pour répondre à vos besoins en recrutement sur toute la France**.
- Un accompagnement par nos conseillers pédagogiques **à chaque étape de l'alternance**.
- Un point de suivi hebdomadaire par un **mentor individuel** pour **motiver l'étudiant et l'accompagner** pendant toute sa formation.



Tout savoir sur les contrats d'alternance

Une question ? Un projet ?

Contactez : job.placement@openclassrooms.com

Contrat de professionnalisation

1 jour en formation / 4 jours en entreprise.

- 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, Pôle Emploi octroie une aide à l'emploi à l'entreprise.