



Analyste Cybersécurité SOC

 Mentor individuel  Certification OpenClassrooms

Détectez les incidents de cybersécurité et agissez pour la protection de votre entreprise

 PÉRIODE DE FORMATION

9 mois à temps plein

18 mois en alternance**

 DURÉE DE LA FORMATION

843 heures supervisées

OPENCLASSROOMS

La formation demande un investissement en temps estimé à 1686 heures : 843 heures de formation supervisée (projets encadrés par des mentors) et 843 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.

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

Devenez analyste cybersécurité SOC **en 12 mois grâce à l'alternance !**

Devenir Analyste Cybersécurité SOC : surveillez le système d'information pour détecter les activités suspectes ou malveillantes et agir pour la sécurité de votre entreprise

Au sein d'un Security Operation Center (SOC), vous serez chargé de surveiller l'état de cybersécurité du système d'information. En première ligne des alertes de sécurité et incidents potentiels, vous mènerez les qualifications puis contribuerez activement aux investigations et à la réponse aux incidents lorsque nécessaire. Vous réaliserez notamment de premières actions d'endiguement, proposerez un plan d'action et prendrez part à la coordination des différentes parties prenantes. Vous participerez également à l'évolution du système global de sécurité de l'entreprise, que ce soit via l'accompagnement des utilisateurs, l'apport de conseils sur les questions relatives à la sécurité ou encore l'amélioration continue des systèmes de détection.

En tant qu'Analyste Cybersécurité SOC, quelles sont vos missions ?

Les missions types que vous pourrez mener :

1. Investiguer des incidents de sécurité
2. Qualifier des alertes
3. Résoudre des incidents
4. Améliorer des processus et des systèmes de sécurité
5. Automatiser des réponses à incident
6. Contenir une propagation d'incident

Vous maîtriserez les ressources, technologies et outils les plus demandés : IOC, TTP, TLP, killchain, MITRE ATT&CK, MITRE D3FEND, les SIEM, SIIRP, SOAR, EDR, le sandboxing, les composants de sécurité réseau (pare-feux, IDS/IPS, proxies, WAF), le langage Python, les outils ELK, Splunk, TheHive, Cortex, Wireshark / tshark ou encore n8n

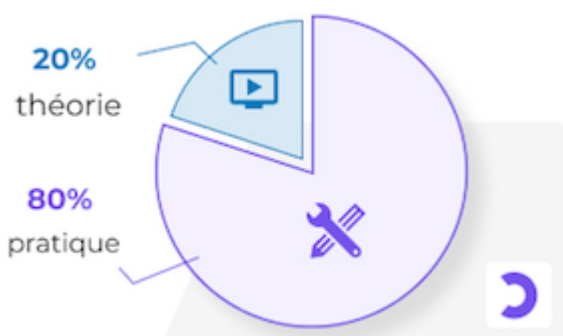
La cybersécurité est un secteur en recherche durable de nouveaux talents, avec des effectifs en hausse constante à travers le monde. En France, d'après [\(ISC\)²](#), 60 000 postes pourraient ainsi compléter les 189 000 personnes agissant déjà dans le secteur pour répondre aux besoins. L'État français appelle quant à lui à la création de 37 000 emplois dans le secteur d'ici à 2025, dans le cadre de sa [stratégie nationale pour la](#)

[cybersécurité.](#)

Le rôle d'Analyste SOC se hisse à la deuxième place des métiers cybersécurité les plus recherchés par les entreprises d'après l'étude "[Cybersecurity skills gap survey](#)" publiée par Fortinet en 2022.

Nos formations vous permettent d'apprendre par la pratique

Réalisez des projets concrets basés sur des mises en situation professionnelles.



Savoir c'est bien, savoir-faire c'est mieux !

Vous êtes accompagnés par un mentor, professionnel du métier, tout au long de votre formation



Thomas ROCCIA, Senior Security Researcher chez Microsoft, et mentor sur les parcours Cybersécurité OpenClassrooms

"En tant que mentor, mon rôle est d'accompagner les étudiants et de partager mon expérience professionnelle dans le domaine de la cybersécurité. Ce qui est passionnant, c'est de guider et d'accompagner des étudiants enthousiastes et motivés, car cela nous permet de développer nos compétences pédagogiques et de transmettre notre passion pour ce domaine en constante évolution." Thomas

Autonomes, mais jamais seuls !

Chez OpenClassrooms, vous pourrez compter sur de nombreux soutiens :

- Les professeurs, experts du domaine.
- Les conseillers pédagogiques dédiés à votre réussite.
- Une communauté d'étudiants sur Slack.

Quelles sont vos opportunités de carrières et d'emplois à la suite de cette formation ?

En suivant notre formation en ligne, vous pourrez exercer de nombreux métiers dont celui d'**analyste SOC**, **veilleur-analyste** et **analyste détection d'incidents cybersécurité**. Plus largement, vous pourrez aisément agir dans le domaine de la sécurité opérationnelle.

Le salaire dépend notamment du niveau d'ancienneté*

- **31 000 €** brut annuel pour un profil **débutant**

- **54 000 €** brut annuel pour un profil **confirmé**

Cette fourchette peut toutefois varier selon la taille de l'entreprise et la région.

* [CIDJ](#)

Vous pourrez évoluer vers d'autres métiers dédiés à la gestion des incidents et des crises de cybersécurité, comme spécialiste en investigation numérique, analyste de la menace, responsable SOC, responsable CSIRT ou gestionnaire de crise après quelques années d'expérience ou en poursuivant vos études dans ce cursus.

Découvrez les regards croisés de professionnels sur les métiers de la cybersécurité



[Apprenez en plus sur les métiers de la cybersécurité à travers l'épisode dédié de notre podcast.](#)

Nos alumni racontent



Jean-Marie KOKA EKWALANGA, étudiant sur un de nos parcours “Systèmes & Réseaux”

Dans la formation, c'est vous qui lisez les cours et effectuez les projets. Si vous êtes bloqué, le mentor peut vous donner des pistes. Nous avons une bonne relation.

Les pré-requis pour postuler

Pour accéder à la formation Analyst cybersécurité - SOC, les candidats doivent obligatoirement :

- être titulaire d'une **certification professionnelle de niveau 5** (ou équivalent) en informatique

ou,

- être titulaire du **baccalauréat** ou d'une **certification professionnelle de niveau 4** (ou équivalent) avec une **expérience professionnelle d'au moins 2 ans en support et/ou maintenance informatique**.

Langue : un niveau B2 minimum en français.

L'anglais technique est recommandé.

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 tous les candidats, la procédure de sélection s'effectue au travers d'un **formulaire de candidature validant les pré-requis** académiques ou dérogatoires, ainsi que l'adéquation du projet professionnel avec les objectifs de la formation. Sont collectées les pièces justificatives constituant le dossier d'admission. Si nécessaire, un entretien individuel de motivation est organisé.

- **Matériel** : avoir accès à un ordinateur (PC ou Mac avec processeur Intel), 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 16Go de RAM et de 150Go d'espace de stockage disponibles ;
 - être administrateur de votre ordinateur afin de pouvoir installer des programmes complémentaires.

Comment obtenir ce diplôme?

Pour obtenir le diplôme, vous devrez :

- Réaliser et valider la totalité des projets du parcours. Le dernier projet vous proposera de réaliser une application professionnelle facultative de 3 mois (stage ou mission en entreprise).

Projet 1 - 10 heures

Démarrez votre formation d'Analyste Cybersécurité SOC

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.



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 ?

Découvrez l'écosystème de détection et de traitement des incidents et les bonnes pratiques de cybersécurité

Intégrez le SOC d'une grande entreprise. Immergez-vous en conditions réelles en découvrant les outils, les processus et l'organisation de la défense opérationnelle et rédigez vos premiers éléments de documentation interne.

Compétences cibles

- Alimenter la documentation interne
- Sensibiliser des utilisateurs de SI aux bonnes pratiques de sécurité

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.



Découvrez les bases de la sécurité numérique

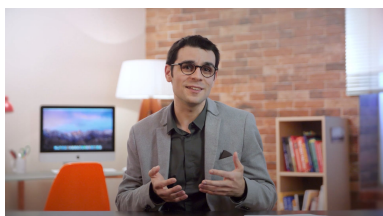


Facile



6 heures

Apprenez à sécuriser votre ordinateur et votre navigation sur Internet, en utilisant des mots de passe robustes, en protégeant l'atteinte à la vie privée en ligne, en reconnaissant les tentatives de fraude.



Rédigez des écrits professionnels



Facile



4 heures

La communication écrite est primordiale dans le monde professionnel. Quel que soit votre métier, si vous voulez maîtriser la rédaction d'un écrit de la structuration à la relecture, ce cours vous sera utile !



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 3 - 35 heures

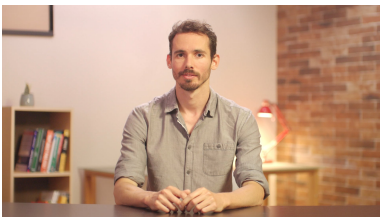
Collectez, analysez vos premiers logs et classez les alertes

Collectez et analysez les logs d'un organisme de formation en ligne afin de classer ses alertes de cybersécurité.

Compétences cibles

- Qualifier des alertes de cybersécurité en faux positif ou incident potentiel
- Recueillir des données techniques, matérielles et humaines sur un incident

Cours associés



Virtualisez votre architecture et 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 - 30 heures

Rédigez vos premiers scripts en Python

Un hébergeur de sites Web supervisant ses IP publiques souhaite automatiser la neutralisation des fichiers compromis. Automatisez le nettoyage des fichiers compromis avec Python.

Compétences cibles

- Automatiser une réponse à incident

Cours associés



Initiez-vous à Python pour l'analyse de données



Facile



6 heures

Dans ce cours, vous apprendrez un langage de programmation indispensable pour l'analyse de données : Python. Nous aborderons ensemble les notions fondamentales de la programmation Python, à l'aide d'exemples simples et d'exercices pratiques.



Apprenez les bases du langage Python

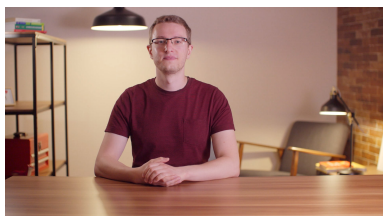


Facile



6 heures

Python est très demandé et accessible pour les débutants. Apprenez à coder avec Python pour écrire des programmes simples mais puissants, et pour automatiser les tâches.



Mettez en place votre environnement Python



Facile



6 heures

Installez votre environnement Python en utilisant pip pour gérer des paquets, virtual env pour créer un environnement virtuel pour chaque projet, et PyCharm comme IDE.

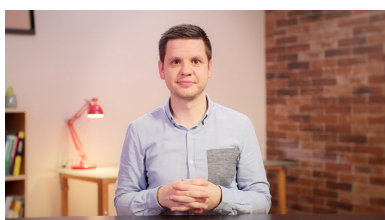
Contenez vos premiers incidents

À partir d'éléments observables collectés, vous identifierez les actions possibles d'endiguement de l'incident sur le système d'information d'une banque internationale.

Compétences cibles

- Contenir une propagation d'incident cybersécurité simple
- Résoudre un incident de sécurité simple en respect des procédures internes du SOC

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.



Apprenez les bases du langage Python

■ Facile ⌚ 6 heures

Python est très demandé et accessible pour les débutants. Apprenez à coder avec Python pour écrire des programmes simples mais puissants, et pour automatiser les tâches.

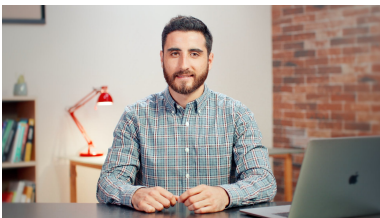
Enquêtez sur vos premiers incidents de cybersécurité

Réalisez des analyses approfondies de l'incident de cybersécurité d'un industriel de l'agro-alimentaire.

Compétences cibles

- Qualifier des alertes avancées de cybersécurité en faux positif ou incident potentiel
- Cadrer l'investigation d'un incident de cybersécurité sur une infrastructure SI
- Analyser des données et des traces réseaux d'incident grâce aux outils adaptés

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.

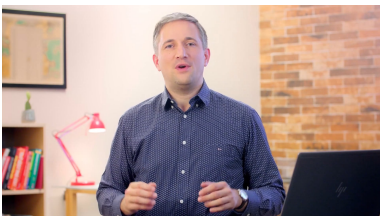
Résolvez les incidents de sécurité de bout en bout

Présentez votre résolution de l'incident de cybersécurité d'un acteur de la grande distribution doté d'un système d'information complexe.

Compétences cibles

- Présenter une résolution de l'incident intermédiaire aux équipes métiers et sécurité.
- Résoudre un incident de sécurité intermédiaire en respect des procédures internes du SOC

Cours associés




Sécurisez vos infrastructures

 Difficile  10 heures

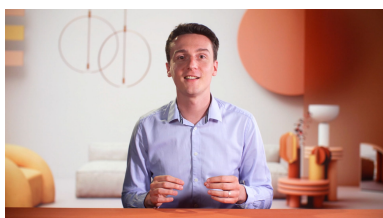
Apprenez à sécuriser vos infrastructures des attaques physiques mais aussi des cyber attaques grâce aux protocoles, firewalls et autres techniques ! Dans ce cours, vous aborderez les types de hacking les plus connus et comment vous en protéger.



Prenez la parole en public

 Facile  6 heures

Mobilisez des techniques de communication en public. Créez votre contenu avec le storytelling et le mind mapping, et entraînez-vous pour maîtriser votre prestation orale.



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 !

Limitez les faux positifs

Une entreprise de vente en ligne souhaite améliorer la détection des incidents potentiels de cybersécurité. Aidez votre client à améliorer les règles de détection.

Compétences cibles

- Optimiser en continue le système de gestion de connaissances interne
- Préconiser une amélioration de la détection des incidents potentiels

Cours associés



Apprenez les bases du langage Python

Facile

6 heures

Python est très demandé et accessible pour les débutants. Apprenez à coder avec Python pour écrire des programmes simples mais puissants, et pour automatiser les tâches.

Appuyez-vous sur le bouton rouge ?

Une grande entreprise de l'énergie subit une propagation rapide d'une attaque. Intégrez la cellule de crise pour participer à sa résolution. Proposez des actions de mitigation.

Compétences cibles

- Contenir une propagation d'incident cybersécurité complexe
- Présenter une résolution de l'incident complexe aux clients, équipes métiers et sécurité.
- Résoudre un incident de sécurité complexe en respect des procédures internes du SOC

Cours associés



Prenez des décisions efficaces



Facile



4 heures

Prendre des décisions est une soft skill indispensable pour résoudre des problèmes. Qu'il s'agisse de choix personnels ou professionnels, apprendre à trancher rapidement et efficacement vous aidera dans votre carrière.



Améliorez l'impact de vos présentations



Moyenne



8 heures

Découvrez le design de présentation, avec des techniques de facilitation visuelle. Faites passer un message à impact émotionnel positif grâce à des diaporamas créatifs et modernes.

Améliorez et automatisez la détection et le traitement des alertes

Aidez une entreprise de l'aéronautique à niveau de sensibilité élevé à déployer des outils d'analyse afin d'améliorer la qualité de la détection des alertes de cybersécurité.

Compétences cibles

- Automatiser des détections d'alertes

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.



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.

Constituez votre portfolio et démontrez vos compétences d'Analyste Cybersécurité SOC

Valorisez l'acquisition de vos compétences d'Analyste en Cybersécurité et constituez votre portfolio ou réalisez une expérience de terrain.

Compétences cibles

- Présenter ses compétences d'analyste cybersécurité

Cours associés



Prenez la parole en public



Facile



6 heures

Mobilisez des techniques de communication en public. Créez votre contenu avec le storytelling et le mind mapping, et entraînez-vous pour maîtriser votre prestation orale.



Travaillez efficacement en équipe



Moyenne



10 heures

Le travail en équipe est une compétence essentielle... Et cela s'apprend ! Mobilisez des techniques comportementales pour profiter d'un levier formidable de l'équipe : l'intelligence collective.

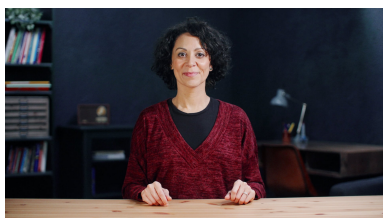


Élaborez votre stratégie de recherche d'emploi

 Facile

 8 heures

Dans ce cours, vous apprendrez à rédiger un CV percutant, à soigner votre présence sur les réseaux sociaux comme LinkedIn et à chercher des offres. Prêt pour l'aventure ?

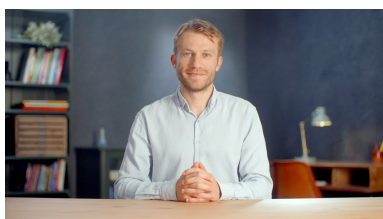


Réussissez votre première semaine en entreprise

 Facile


 4 heures

Intégrer une entreprise n'est pas toujours une chose évidente. Jeune actif ou non, apprenez dans ce cours les bonnes pratiques pour réussir votre prise de poste, être à l'aise et vous intégrer facilement dans votre nouveau travail !



Développez vos soft skills

 Facile

 6 heures

Les soft skills, comme l'adaptabilité, la collaboration, la résolution de problèmes, sont des compétences de plus en plus recherchées. Développez ces compétences transversales et comportementales.



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, issus 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 situation 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

1 à 2 jours en formation / 3 à 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, France Travail octroie une aide à l'emploi à l'entreprise.