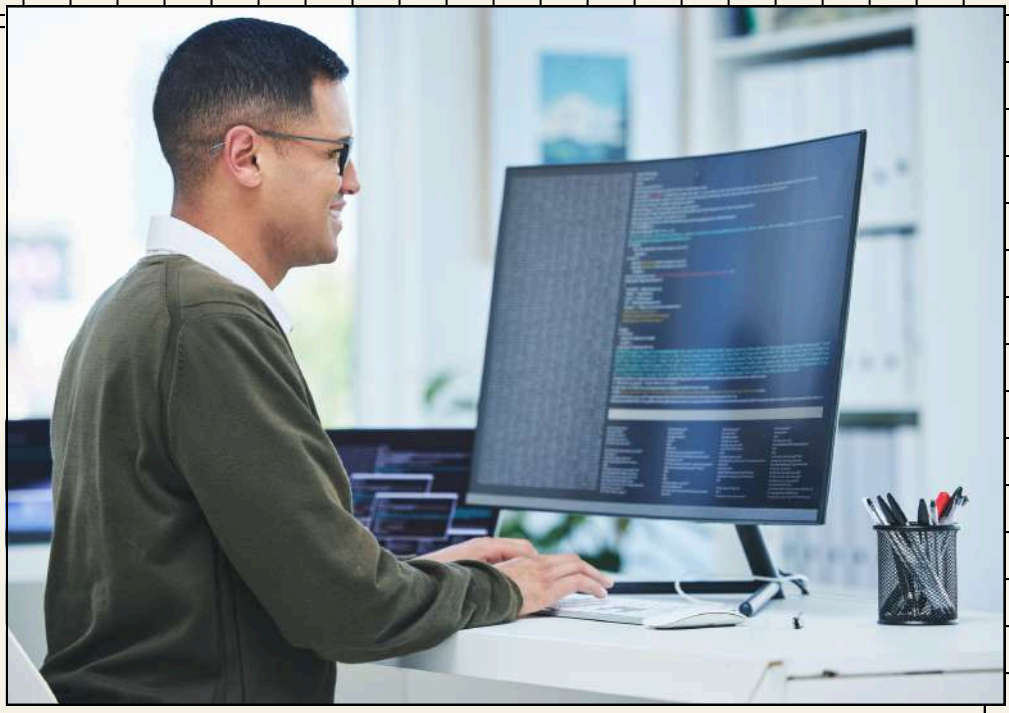
SYLLABUS INGÉNIEUR CYBERSÉCURITÉ

EN ALTERNANCE



Devenez Ingénieur en Cybersécurité et défendez les données et systèmes de votre entreprise contre les cybermenaces

DataScientest

SOMMAIRE

QUI SOMMES-NOUS ?

DataScientest est le leader de la formation en Cybers en France. Nous offrons des formations orientées métier aussi bien aux professionnels qu'aux particuliers qui souhaitent monter en compétences ou se reconvertir.

+35 Groupes du **CAC 40** formés

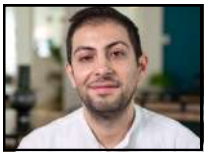
+15k **Alumni**

+3k Heures de **contenu**

Ils nous font confiance

NOTRE ÉQUIPE

L'équipe pédagogique de DataScientest est uniquement composée de professeurs internes à l'organisme. Ils se consacrent entièrement à l'enseignement et à la recherche pour nos différentes formations et cursus experts.



Charles S.

CTO &
Responsable Académique
(9 ans d'expérience)

Diplômé de l'École Polytechnique, Charles est spécialisé en programmation, Machine Learning et Deep Learning.
CTO de DataScientest, il est à la tête du corps professoral et des développeurs qui travaillent sur la plateforme.

Raphael K.

Directeur pédagogique
(9 ans d'expérience)

Titulaire du master ISF spécialisé en Apprentissage Statistique et Science des données de l'Université Paris-Dauphine, Raphaël a conçu la formation Data Analyst grâce à ses connaissances en programmation, Data Visualisation, et Machine Learning.

Intervenants

Lors de la formation Ingénieur Cybersécurité, vous rencontrez plusieurs intervenants diplômés des plus grandes écoles d'ingénieurs de France (Polytechnique, L'école des Mines, Centrale Supélec, Université Paris Dauphine…). Ils ont été recrutés pour leur sens de la pédagogie et leur connaissance dans le domaine.

Corentin S.

Responsable des formations en cybersécurité

Certifié Bureau Veritas et Stormshield, il est également devenu instructeur des formations certifiantes Stormshield. Corentin est chargé du management des formateurs techniques et travaille sur la conception des supports de cours. Il dispose de plus de 5 ans d'expérience en tant que Directeur du département Cybersécurité chez Aforssic.

Anthony M.

Responsable des formations en cybersécurité organisationnelle

Diplômé à l'origine d'une licence AES et Assurance, Anthony s'est ensuite reconverti dans la cybersécurité à travers des missions d'accompagnement ISO 27001 LI, HDS, ISO 20000, ainsi que dans les campagnes de sensibilisation. Suite à l'obtention de ses diverses certifications en cybersécurité organisationnelle avec notamment l'ISO 27001 Lead Implementer, il a également acquis une qualification en tant que formateur ISO reconnu.

Rencontrez notre équipe

NOTRE PÉDAGOGIE

DataScientest offre une formation 100% en distanciel en format hybride avec une pédagogie basée sur le Learning By Doing.

Objectifs de la formation

Développer les compétences nécessaires à l'exercice du métier d'ingénieur cybersécurité.
Ainsi au terme de la formation, l'apprenant sera capable de :

- Définir la stratégie de cybersécurité d'une organisation
- Elaborer et piloter des processus de cybersécurité d'une organisation
- Maintenir la sécurité du système d'information d'une organisation
- Gérer les incidents et crises de cybersécurité d'une organisation

Moyens pédagogiques

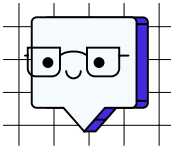
- **Travaux pratiques :** Pendant 80% du temps, vous travaillez sur notre plateforme d'enseignement personnalisée Train, développée par DataScientest. Tous les modules de formation intègrent des exercices en ligne permettant de mettre progressivement en œuvre les concepts développés dans le cours.
- **Masterclass :** Près de 20% de la formation se déroule en Masterclass. Ces temps de formation en direct avec un formateur permettent d'aborder les problématiques actuelles des technologies, méthodes et outils du domaine.
- **Pédagogie par projet :** permettant de mettre l'apprenant en situation professionnelle (pédagogie active).

Simulateur d'attaque

Le TP de simulation d'attaque est un exercice de pratique qui vise à simuler une attaque informatique réelle pour vous permettre de mieux comprendre les différentes techniques utilisées par les cybercriminels mais aussi pour vous former à détecter, prévenir et contrer ses attaques informatiques. Durant ce TP vous occuperez différents postes tels que l'attaquant, la victime ou encore l'administrateur système, le but est d'avoir une expérience pratique et les compétences nécessaires pour détecter, prévenir et répondre aux attaques informatiques.

Accompagnement et assistance

Tous les jours de la semaine de 9h00 à 17h00, l'ensemble des formateurs experts en data se relaient sur un forum dédié pour proposer une **assistance technique personnalisée** à tous les apprenants. De nombreuses séances de questions-réponses sont également organisées en synchrone avec nos formateurs.



Les certifications à l'issue de la formation

- CSNA Stormshield
- ISO 27001 Bureau Veritas
- Certificat de ECE tech
- RNCP 7 «Gestionnaire de la sécurité des données, des réseaux et des systèmes »

Modalités d'évaluation

Mise en place d'un dispositif d'évaluation complet : recueil des attentes et besoins à l'inscription, test de positionnement, évaluation des acquis, recueil des appréciations.

- Travaux pratiques individuels en ligne
- Des évaluations continues sous la forme de cas pratiques en ligne jalonnent le parcours de formation, leur modalités seront explicitées par le formateur en début de module.

Formation certifiante : Reconnaissance étatique et académique

La formation vise l'obtention de la certification RNCP de niveau 7 "Gestionnaire de la sécurité des données, des réseaux et des systèmes ", délivrée par CALTEA . Consulter la fiche. Chaque bloc peut être acquis individuellement.

Consulter la fiche.

Bloc de compétences	Modalité de validation
Bloc 1 : "Formuler et formaliser la politique de la sécurité des systèmes d'information d'une organisation, en adéquation avec son environnement et les risques auxquels elle doit faire face"	Étude de cas et mise en situation reconstituée
Bloc 2 : "Mettre en place les outils techniques nécessaires à la sécurisation du système d'information d'une organisation"	Mise en situation professionnelle reconstituée et TP
Bloc 3 : " Suivre l'évolution du niveau de sécurité d'un système d'information d'une organisation"	Étude de cas et questionnaires à visée professionnelle
Bloc 4 : "Organiser une réponse adaptée en cas de crise"	Mise en situation professionnelle

En savoir plus

Projet fil rouge

Dès le début de votre formation en cybersécurité, vous serez impliqué dans un projet pratique. Ce projet vise à appliquer progressivement toutes les compétences acquises durant le cours. Il requiert jusqu'à 300 heures de travail tout au long de la formation, constituant une étape essentielle pour devenir pleinement opérationnel.

Au cours de ce projet, vous devrez réaliser une étude approfondie du contexte de l'entreprise pour cerner ses enjeux spécifiques. Cette étape est suivie par une analyse des risques, l'élaboration d'une Politique de Sécurité des Systèmes d'Information (PSSI), ainsi que d'autres tâches connexes.

Sur la base de ces analyses, vous sélectionnerez et mettrez en oeuvre les meilleures pratiques de sécurité adaptées aux enjeux identifiés. De plus, il sera essentiel de définir des stratégies de réponse à une éventuelle cyberattaque, témoignant ainsi de votre préparation efficace.

Ce projet facilite la transition de la théorie à la pratique et garantit la maîtrise des compétences requises dans les différents modules du programme. Il est également très valorisé par les employeurs car il atteste de vos compétences et connaissances en tant que consultant en cybersécurité. À l'issue de la formation, vous serez en mesure de présenter ce projet lors de vos entretiens pour justifier concrètement vos compétences en cybersécurité.

En savoir plus

"Une vraie expertise en Data Science, délivrée avec un accompagnement sur mesure dans le souci constant de la satisfaction du client."

Xavier Bocher
Head of Credit Risk Internal Models & Operational Research @Groupe Crédit Agricole

Pré-requis

Afin d'intégrer la formation Ingénieur Cybersécurité, il convient d'avoir obtenu un diplôme ou un titre de niveau 6 (équivalent à un bac +3) dans le domaine de l'informatique.

Pour suivre la formation, l'apprenant doit détenir un ordinateur avec une bonne connexion internet et une webcam.

La formation en alternance

Faites financer votre formation intégralement par votre entreprise et bénéficiez d'une expérience professionnelle en Cybersécurité

Formez-vous rapidement, en suivant un programme intensif.

- **Durée** : 24 mois
- **Durée totale** : 900h
- **Rythme** : 3 semaines en entreprise
  1 semaine en formation

Je prends rendez-vous

LE PARCOURS

1 - Fondamentaux des systèmes et réseaux

2 - Fondamentaux de la cybersécurité et du SOC

3 - Sécurité des réseaux avec Stormshield

4 - Cryptographie & Durcissement des systèmes

5 - SIEM Splunk

6 - SIEM Splunk avancée

7 - Ethical Hacking

8 - APT & Mitre ATT&CK

9 - Détection d'intrusion

10 - Forensique et réponses aux incidents

11 - Le métier d'ingénieur Cybersécurité

12 - L'implémentation des normes liées à la SSI

13 - Indicateur et suivi de projet

14 - Les analyses de risque

15 - Gestion des incidents et continuité d'activité

En savoir plus

Fondamentaux des systèmes et réseaux

- Les bases du réseau
- Fondamentaux des systèmes Linux & Windows
- Programmation et scripting
- **Les compétences acquises à l'issue :**
  - Configurer des équipements réseau
  - Appréhender les principaux services et procotoles : TCP, IP, UDP,
  - ARP, HTTP, DHCP, DNS, etc…
  - Configurer un serveur Windows
  - Maitriser les commandes de bases sur Linux

Fondamentaux de la cybersécurité et du SOC

- Introduction à la cybersécurité
- Guide juridique
- Architecture et organisation d'un SOC
- **Les compétences acquises à l'issue :**
  - Connaître les bonnes pratiques de sécurité
  - Connaître les définitions et les typologies de menaces
  - Connaître les bases du RGPD
  - Comprendre l'aspect juridique du Hacking
  - Comprendre le fonctionnement d'un SOC
  - Connaître les métiers du SOC

Sécurité des réseaux avec Stormshield

- Certified Stormshield Network Administrator
- **Les compétences acquises à l'issue :**
  - Prendre en main et comprendre le fonctionnement d'un firewall SNS
  - Configurer un firewall dans un réseau
  - Définir et mettre en oeuvre des politiques de filtrage et de routage

Cryptographie & Durcissement des systèmes

- Cryptographie et IGC
- Durcissement des systèmes
- **Les compétences acquises à l'issue :**
  - Comprendre les notions de cryptographie
  - Connaître les recommandations de chiffrements
  - Comprendre le système des infrastuctures à clés publiques
  - Savoir sécuriser les systèmes Windows et Linux

SIEM Splunk

- Introduction Splunk
- Les commandes de base
- Rapports et visualisation
- **Les compétences acquises à l'issue :**
  - Comprendre les objectifs de l'outil Splunk
  - Appréhender l'interface graphique de Splunk
  - Prendre en main les commandes de bases
  - Connaître les bases du langage SPL
  - Mettre en oeuvre des rapports
  - Savoir configurer les visualisations

Ethical Hacking

- Méthodologie des tests d'intrusion
- Techniques de Hacking
- Rédaction de rapports
- **Les compétences acquises à l'issue :**
  - Connaître les méthodologies de pentest
  - Savoir préparer son environnement et ses outils
  - Pratiquer les techniques de hacking
  - Effectuer une reconnaissance via l'OSINT
  - Repérer les failles de sécurité
  - Savoir exploiter les failles de sécurité
  - Mettre en oeuvre des actions de post-exploitation
  - Maîtriser la rédaction de rapport
  - Savoir structurer un rapport de pentest

APT & Mitre ATT&CK

- Etude d'attaque APT
- Framework Mitre ATT&CK
- Adversary Emulation
- **Les compétences acquises à l'issue :**
  - Connaître le fonctionnement d'une cyberattaque avancée
  - Etudier les techniques d'attaques d'un groupe APT
  - Maîtriser les notions du framework MITRE ATT&CK
  - Utiliser le framework pour étudier une cyberattaque
  - Maîtriser les outils d'adversary emulation
  - Simuler des cyberattaques

Détection d'intrusion

- Règle de détection d'intrusion
- Analyser les évènements et qualifier les incidents
- Cyber Threat Intelligence
- **Les compétences acquises à l'issue :**
  - Maitriser la création des règles de détection
  - Comprendre la syntaxe des règles de détection
  - Savoir tester ses règles de détection
  - Connaître la méthodologie d'analyse des événements
  - Apprendre à qualifier les incidents
  - Connaître les outils de Threat Intelligence
  - Comprendre la collecte d'informations sur les menaces

Forensique & réponses aux incidents

- Réponse aux incidents
- Computer Forensics
- Préparation et gestion de Cybercrise
- **Les compétences acquises à l'issue :**
  - Comprendre tout le processus de réponse aux incidents
  - Anticiper et préparer la réponse aux incidents
  - Savoir initier et clôturer la réponse aux incidents
  - Maîtriser les outils de l'analyste forensique
  - Pratiquer les techniques forensique pour investiguer un incident
  - Récupérer les informations cachées par l'attaquant
  - Anticiper et préparer les cybercrises
  - Savoir gérer une cybercrise

Le métier d'ingénieur Cybersécurité

- Le rôle de l'ingénieur Cybersécurité
- Veille Cyber
- Sensibilisation
- **Les compétences acquises à l'issue :**
  - Acquérir les compétences, capacités d'un ingénieur cyber et savoir mettre en oeuvre les tâches lui incombant
  - Savoir effectuer une veille cyber
  - Identifier les besoins de sensibilisations et mettre en oeuvre cette dernière

L'implémentation des normes liés à la SSI

- Introduction à la GRC
- ISO 27001 Lead Implementer
- Autres référentiels de sécurité
- **Les compétences acquises à l'issue :**
  - Comprendre les tenants et aboutissants de la GRC
  - Savoir préparer, mettre en oeuvre, contrôler et améliorer un SMSI
  - Identifier et comprendre les exigences des principaux référentiels de sécurité cyber

Indicateur et suivi de projet

- Les audits en Cybersécurité
- Les indicateurs de sécurité
- **Les compétences acquises à l'issue :**
  - Identifier les différents types d'audits en cybersécurité et savoir mettre en oeuvre les grands principes d'audit
  - Créer et mettre en oeuvre des indicateurs de performance et d'efficacité

Les analyses des risques

- ISO 27005 RM
- Ebios Risk Manager
- Autres méthodologies d'analyse des risques
- **Les compétences acquises à l'issue :**
  - Comprendre et mettre en oeuvre les principes de la gestion des risques
  - Mettre en pratique la méthode EBIOS-RM
  - Identifier et mettre en oeuvre les principales méthodes de gestion de risque cyber

Gestion des incidents et continuité d'activité

- ISO 27035
- PCI/PRI
- Autres référentiels de sécurité
- **Les compétences acquises à l'issue :**
  - Comprendre et mettre en oeuvre une procédure de gestion des incidents de sécurité
  - Comprendre comment mettre en place la continuité et la reprise d'un système d'information

Je prends rendez-vous

DÉMARCHES D'INSCRIPTION

Prenez rendez-vous avec un conseiller

Avant de vous inscrire à nos formations, vous aurez l'occasion d'échanger avec nos équipes d'admissions qui répondront à vos questions et vous redirigeront vers la formation qui correspondra à vos attentes.

Par la suite, nos conseillers vous enverront un test de positionnement afin de vérifier vos connaissances. Celui-ci porte principalement sur les systèmes d'exploitation, les réseaux et les langages de programmation.Si vos résultats sont concluants et après analyse de votre candidature, nous pourrons entamer les démarches relatives à l'établissement de votre contrat d'apprentissage.

Puis nous vous accompagnons dans votre recherche d'entreprise avec des ateliers de coaching, comprenant des sessions sur la rédaction de CV, la préparation aux entretiens, le développement des compétences interpersonnelles, et d'autres sujets pertinents.

De plus, nous vous présenterons à nos entreprises partenaires, augmentant ainsi vos chances de trouver une entreprise correspondant à vos objectifs et à notre programme de formation.

Je prends rendez-vous

Coût de la formation : 21.000*€

OPCO EP
Opérateur de compétences des Entreprises de Proximité

*La formation est prise en charge par l'OPCO et par l'entreprise qui bénéficie d'un certain nombre d'aides financières.

NOS PARTENAIRES

DataScientest a développé des partenariats avec des institutions mondialement reconnues. D'une part avec des établissements académiques comme l'Ecole des Mines de Paris et d'autre part, avec des éditeurs de logiciels comme AWS ou Microsoft. Ces partenariats ont pour but d'aider les différents apprenants à se démarquer des différents profils en décrochant des certifications reconnues auprès des entreprises.

Amazon Web Services

Partenaire éditeur

Aujourd'hui, DataScientest jouit du statut exclusif d'Amazon Digital Partner. Nous sommes donc habilités par Amazon à former des équipes sur les produits et services de la compagnie américaine. Grâce à ce partenariat, nous avons établi plusieurs formations qui préparent au passage de certifications officielles AWS. Les frais d'inscription à l'examen officiel sont inclus dans le prix de la formation. Dans certaines de nos formations, vous serez préparés au passage de la certification fondamentale d'**AWS : Cloud Practitioner**.

Microsoft

Partenaire éditeur

DataScientest bénéficie du statut de Microsoft Learning Partner, nous sommes ainsi habilités à vous former aux certifications officielles de Microsoft. Ces certifications attestent d'un niveau d'expertise sur Azure, l'ensemble de produits et services de cloud computing et sur Power BI, l'outil de Business Intelligence de Microsoft. Les frais d'inscription à l'examen officiel sont inclus dans le prix de la formation. Avec la formation Data Analyst, DataScientest vous permet de vous préparer au passage de la certification PL-900 et de devenir **Microsoft Certified: Power Platform Fundamentals**.

ECE Tech - Ecole d'Ingénieurs

Partenaire académique

Notre parcours de formation Administrateur Cybersécurité est certifié par l'école d'ingénieurs l'ECE Tech, permettant ainsi aux apprenants de bénéficier de la reconnaissance d'une école de rang national. Cette reconnaissance académique garantit un contenu complet et adapté à chacun de nos apprenants.

Qualiopi

Critère de qualité

Cette certification reconnaît que les processus mis en oeuvre par l'organisme de formation répondent aux exigences du référentiel national qualité au titre des catégories :

- Actions de formation
- Actions de formation par apprentissage

CAREER MANAGEMENT

Un accompagnement de A à Z

Notre équipe **Career Management** se met à votre entière disposition pour vous aider à trouver l'alternance de vos rêves. Fort de sa renommée, DataScientest a tissé de nombreux partenariats avec des entreprises recherchant leurs futurs talents. Aussi, notre **Service Relations Entreprises et Alumni** travaille activement à développer et entretenir un réseau solide de professionnels, ce qui ouvre de nouvelles opportunités pour nos étudiants en recherche d'alternance. Grâce à notre **réseau établi** et à **l'expertise de notre équipe**, nous mettons tout en oeuvre pour faciliter votre accès à des entreprises prestigieuses, offrant des missions enrichissantes et correspondant à vos aspirations professionnelles.

Nous vous accompagnons dans chaque étape du processus, de la **recherche d'offres** à la **préparation des entretiens** en passant par l'amélioration de votre CV, afin de maximiser vos chances de décrocher une alternance et de démarrer une carrière prometteuse.
Votre réussite est notre priorité, et nous sommes impatients de vous aider à concrétiser vos ambitions professionnelles au sein de notre communauté d'élèves et d'anciens étudiants talentueux.

Une fois que vous avez intégré la formation, notre équipe vous accompagne tout au long de votre parcours et vous offre la possibilité de profiter d'un **coaching carrière individualisé** et de participer à de nombreux évènements. Enfin, tout au long de votre alternance, vous pourrez bénéficier des conseils **personnalisés**. Grâce à notre collaboration avec de **nombreuses entreprises**, vous bénéficiez d'interventions professionnelles pour des sessions de **webinar** et de coaching.

Salon de recrutement

Grâce à son large réseau d'entreprises, DataScientest organise deux à trois fois par an des salons de recrutement avec ses entreprises partenaires afin de vous aider à trouver votre alternance.

"Notre objectif est d'accompagner les apprenants, quel que soit leur parcours, à l'aide d'un accompagnement personnalisé afin qu'ils puissent avoir toutes les chances de leurs côtés pour trouver un emploi."

Estelle Molto
Head of Career Management @DataScientest

Je prends rendez-vous

Customer Care

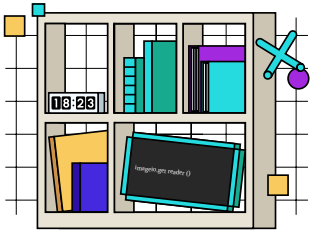
L'équipe Customer Care est composée de **référents techniques** et de **program managers** qui travaillent ensemble pour offrir un **accompagnement** encadré à chaque promotion. Le côté technique de la formation est géré par les référents techniques, tandis que le côté humain est pris en charge par les program managers.

Les promotions et les apprenants sont **suivis individuellement** afin de les aider à atteindre leurs objectifs. Pour cela, nous organisons des **entretiens de suivi** de formation qui mettent l'accent sur la dimension humaine et permettent d'adapter les règles en cas de complications personnelles. Nous offrons également des **conseils** pour gérer son temps et améliorer sa manière d'apprendre tout au long de la formation. Des **événements** sont aussi organisés pour renforcer la cohésion de groupe et éviter l'isolement des apprenants en formation à distance.

Nous sommes attentifs aux commentaires de nos utilisateurs pour continuer à **améliorer** nos programmes de formation. Pour ce faire, nous recueillerons vos **feedbacks** tout au long de votre parcours de formation. Nous proposons également des profils dédiés au support et au traitement des questions de l'ensemble des apprenants.

"La bienveillance envers nos apprenants est notre objectif principal. Nous veillons à ce que leur formation se passe bien grâce à un suivi individuel, des conseils et une oreille attentive aux besoins de chacun."

Pauline Messager
Head of Customer Care Service @DataScientest



COMMUNAUTÉ ALUMNI

DataScientest voue une importance particulière à sa communauté alumni.

Celle-ci ne cesse de s'agrandir, et avec elle l'ensemble de ses alumni. Ainsi, pour garder le contact et permettre aux anciens élèves de communiquer entre eux, DataScientest a mis en place la **communauté DatAlumni**, un groupe qui partage et échange sur divers thèmes autour de la Data Science. Vous serez invité à la rejoindre en début de votre formation ! Au programme : veille technologique, opportunités business, networking, événements (afterworks, salons, Data Challenges…).

Si vous souhaitez découvrir les formations DataScientest de l'intérieur, sachez que **nos alumni** se tiennent disponibles pour **échanger et vous partager leur expérience**. Ils seront ravis de vous apporter les réponses à vos questions et de vous guider sur la formation adapté à vos attentes. Vous pourrez les contacter par mail ou sur Linkedin en cliquant sur le lien suivant.

Contactez nos alumni

Ateliers méditation

Tous les apprenants et alumni DataScientest sont invités une fois toutes les deux semaines à participer à des **ateliers méditation** animés par Xavier Horem, enseignant en méditation appliquée. L'objectif est de lutter contre l'abandon et de les accompagner dans la gestion de leur stress.

Afterworks

Tous les deux mois, les équipes Communication et Customer Care organisent des **afterworks en présentiel** à destination de tous les apprenants et alumni afin de réunir les apprenants, de maintenir le **lien social** et d'éviter les ruptures de parcours.

Veille technologique

En parallèle, afin de gagner en connaissance Data et d'assurer la veille technologique, des **newsletters** élaborées par nos Data Scientists vous sont régulièrement envoyées et sont une source fiable d'informations spécialisées en Cybersécurité.

FOIRE AUX QUESTIONS

À quel salaire peut prétendre un ingénieur Cybersécurité ?

Pour un ingénieur cybersécurité en France, les salaires varient en fonction du niveau d'expérience. Les juniors peuvent s'attendre à un salaire débutant autour de 38.000€ à 45.000€ par an. Les profils avec une expérience intermédiaire peuvent viser entre 45.000€ et 60.000€, tandis que les seniors peuvent prétendre à des salaires allant de 60.000€ à 75.000€ ou plus, selon l'expertise et la localisation.

Quel est le délai d'accès à la formation ?

Après votre prise de contact sur le site, nous vous contactons une première fois pour une présentation de DataScientest de ce que nous pouvons vous offrir, mais aussi de votre parcours et vos souhaits. L'idée est d'aligner dès ce moment notre offre à vos besoins. Un dossier d'admission et un test permettront ensuite d'évaluer votre niveau.

Une fois cette étape réalisée, un membre de l'équipe d'admission prendra contact avec vous pour échanger sur vos résultats et valider votre projet professionnel, vos motivations, et enfin sur la pertinence de votre projet pédagogique.

Une fois votre projet confirmé, soit vous passez directement en phase d'inscription avec nos équipes, soit, dans le cas de l'alternance, il sera nécessaire de signer un contrat d'apprentissage avec un employeur.

Quelles sont les équivalences et passerelles possibles avec la formation ?

Après analyse des certifications comparables, aucune équivalence du titre RNCP37796 enregistrée au RNCP ou au RSCH de France Compétences n'est recensée.

En terme de passerelle, l'ingénieur cybersécurité peut s'orienter vers les métiers de la gestion et du pilotage des projets de la sécurité (RSSI, Directeur cybersécurité) ou de la conception et du maintien d'un SI sécurité (architecte, auditeur de sécurité organisationnelle, etc.)

- p-1 : Administrateur de solutions de sécurité
- p+1 : Responsable de la sécurité des systèmes d'information (RSSI)

Pour connaître les conditions requises dans le cadre d'une passerelle durant la formation, il faudra vous rapprocher des établissements dispensant le titre visé.

Quels sont les suites et débouchés de la formation ?

La formation de Ingénieur cybersécurité offre de nombreux débouchés dans un secteur en pleine croissance. Certains débouchés incluent :

- Ingénieur cybersécurité
- Consultant en cybersécurité ;
- Auditeur sécurité des systèmes d'informations
- Architecte sécurité des systèmes d'information
- Expert en sécurité des systèmes d'information
- Spécialiste en cybersécurité ;
- Analyste SOC Security Operations Center.
- Chef de projet en sécurité des systèmes d'information

Ainsi, à l'issue de l'obtention du titre RNCP37796 vous pouvez poursuivre votre formation en visant la maîtrise de compétences complémentaires.

Quelques exemples de certifications :

- Lead Implementer ISO27001 RS6244
- Concevoir des solutions cloud sécurisées et robustes à l'aide des technologies AWS RS5611
- Concevoir et mettre en œuvre la gestion des données dans Microsoft Azure RS5307

Vous êtes en situation de handicap ?

DataScientest analysera toutes les possibilités d'aménagement (pédagogie, matériel, moyens techniques, humains) afin de compenser votre handicap et vous permettre de suivre votre formation dans de bonnes conditions. Nos locaux sont accessibles aux personnes en situation de handicap. Vous pouvez contacter notre référente handicap pour toute demande concernant votre situation : **mathilde.v@datascientest.com**
Pour découvrir le parcours d'un ancien apprenant atteint de surdité qui a réussi à décrocher son diplôme avec DataScientest, n'hésitez pas à **cliquer ici.**

Pour plus d'informations, n'hésitez pas à nous contacter :

contact@datascientest.com

+33 9 80 80 79 49

www.datascientest.com

DataScientest

VOUS SOUHAITEZ DEVENIR INGÉNIEUR CYBERSÉCURITÉ ?

datascientest.com

contact@datascientest.com

+33 9 80 80 79 49

Version du 29/05/24