Book de stages 2023

Almond

Almond se positionne comme un acteur français indépendant incontournable de l'audit et du conseil dans les domaines de la Cybersécurité, du Cloud et des Infrastructures.

INFRASTRUCTURE SECURITY

SOC / CERT CWATCH

OFFENSIVE SECURITY

GOVERNANCE, RISKS & COMPLIANCE

STRATEGY, GOVERNANCE & TRANSFORMATION

ARCHITECTURE & DIGITAL PLATFORM

board of cyber security rating®

INFRASTRUCTURE SECURITY

L'équipe est constituée de consultants spécialistes et certifiés dans leurs domaines, permettant de traiter des thématiques de sécurité selon le contexte client : la sécurité des infrastructures Cloud, on premise ou hybrides (firewalls, WAF, VPN), la gestion des identités et des accès (IAM, MFA), la sécurité du poste de travail, y compris en mobilité (chiffrement, accès conditionnels, EDR), la sécurité des données (DLP, CASB).

Découvrez nos missions

1. Un stage au sein de l'équipe Infrastructure Security, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.

2. Un accompagnement et un suivi de stage par des experts qui garantissent un véritable apprentissage du domaine.

3. Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

Sécurisation des APIs

Depuis plusieurs années, les entreprises souhaitent **raccourcir les délais de mise à disposition** de nouvelles applications ou de nouvelles fonctionnalités au sein d'une application existante. La méthode de développement **Agile**, le **déploiement continu, l'orchestration** des infrastructures sont quelques-unes des évolutions technologiques apparues au cours des dernières années pour répondre à ce besoin.
En parallèle, les **communications entre applications** se sont généralisées et standardisées, au sein des entreprises comme entre entreprises. Elles se font maintenant avec des appels basés sur le **protocole HTTP**, sous le format REST ou SOAP.
La **sécurité applicative** doit **s'adapter** à cette tendance afin de couvrir les applications exposées de cette façon, qui sont de plus en plus nombreuses et diverses, principalement avec le développement d'infrastructures multi-Cloud.
Les outils utilisés couramment dans la sécurisation applicative sont-ils adaptés aux API ? Quelles méthodes **d'authentification**, de **contrôle d'accès**, de **logging** sont les plus adaptés ?

› Tes missions

L'objectif du stage sera de répondre à ces différentes questions en réalisant un **état de l'art** sur les menaces concernant les API puis en étudiant techniquement les **mécanismes de sécurisation envisageables**.

Les travaux à réaliser seront les suivants :

Etat de l'art de la sécurisation des API

> Evaluation des formes que prennent les API aujourd'hui,

> Etude des différents formats des APIs et des attaques connues sur les API,

> Etat de l'art des mécanismes de sécurité possibles sur les APIs et de leurs implémentations : méthodes d'authentification , analyse de contenu des requêtes, API Gateway, contrôle des permissions, etc.

Etude technique

> Mise en place d'une maquette d'une application avec une solution de sécurisation des appels API,

> Tests d'attaques sur la maquette avec et sans sécurisation pour évaluer la sécurité des mesures choisies.

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité.
Tu bénéficies de connaissances générales sur les infrastructures IT et le Cloud Computing.

> Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).

> Tu as un goût pour la mise en pratique technique.

Stage de 6 mois - basé à Sèvres
1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Authentification SSO & MFA

Les interconnexions croissantes des systèmes d'informations avec une **multitude d'applications et de services en ligne** posent aux organisations plusieurs défis en termes de sécurité. **La gestion des accès et des identités** est devenue un **enjeu de cybersécurité majeur**.

En effet, la multiplication des services Cloud et des applications accessibles sur internet augmente significativement l'exposition des identités des entreprises ainsi que le risque d'intrusion au sein du SI. C'est pourquoi la **fédération d'identités** et **l'authentification unique (SSO)** sont aujourd'hui indispensables pour garantir une **gestion unifiée et sécurisée des comptes utilisateurs.** Par ailleurs, l'ajout de mécanismes **d'authentification multi-facteurs (MFA)** permet également de **renforcer la sécurité des accès** pour les services les plus exposés ou les plus critiques.

L'objectif du stage sera dans un premier temps de comprendre les **principaux concepts, le fonctionnement technique et les enjeux de sécurité** liés aux problématiques d'authentification unifiée. Par la suite, l'étude portera sur **les principales solutions et architectures** mises en œuvre en entreprise pour utiliser le SSO et l'authentification forte. Il s'agira également d'acquérir **des convictions fortes sur le sujet, en identifiant les bonnes pratiques et des recommandations adaptées** à un contexte client. Enfin, **deux dispositifs SSO/MFA devront être implémentés au travers d'une maquette**, pour tester les fonctionnalités, mieux appréhender techniquement le SSO et la MFA, et comparer les solutions.

> Tes missions

> **Comprendre les concepts, le fonctionnement et les enjeux de sécurité associés au SSO et à la MFAEtude des différents formats des APIs et des attaques connues sur les API**

- Identifier les risques associés à la gestion des identités, et plus précisément aux traitements des authentifications
- Exprimer les cas d'usages des applications à protéger et les besoins d'infrastructure
- Comprendre les principaux protocoles d'authentification unique (SAML, OpenID Connect, FIDO, etc.)
- Comprendre le fonctionnement de la MFA, ses atouts et ses impacts techniques et opérationnels en entreprise

> **Etudier les principales solutions et architectures**

- Etudier des architectures pour répondre aux cas d'usages infrastructures explorés
- Réaliser un état de l'art et comparatif des solutions SSO/MFA du marché
- Identifier les tendances et ouvertures vers les nouvelles solutions d'authentification sans mots de passe

> Identifier les bonnes pratiques et mettre en œuvre une solution SSO

- Proposer un ensemble de recommandations et de bonnes pratiques concernant le SSO et la MFA
- Implémenter deux solutions SSO/MFA du marché dans un environnement de maquette, afin d'évaluer les fonctionnalités, les avantages, les contraintes techniques et opérationnelles, et les comparer

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité. Tu bénéficies de connaissances générales sur les infrastructures IT et le Cloud Computing.

> Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).

> Tu as un goût pour la mise en pratique technique.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Sécurisation des E-mails

Depuis plusieurs années, l'email est le vecteur principal d'infection initiale des SI par les attaquants. L'inventivité de ces derniers requiert des adaptations permanentes sur les mesures de défense pour se prémunir des risques.

Dans le même temps, **le marché des solutions de gestion des emails s'est nettement transformé vers un modèle de service en SaaS dans le Cloud**. Par la même occasion, ces services Cloud n'offrent plus seulement un service de messagerie, mais tout un écosystème dédié à la collaboration, qui implique ainsi une ouverture croissante du périmètre du SI. Ainsi, les solutions de protection des emails se transforment pour intégrer ces changements.

Almond, société de conseil experte en sécurité des systèmes d'informations, souhaite évaluer les architectures et les solutions de protection des emails, évoluant vers la protection de la collaboration.

Le stage aura pour principaux objectifs **de comprendre les enjeux et identifier les problématiques** liés aux solutions actuelles de protection des emails, d'**étudier l'état de l'art des solutions du marché** dans ce domaine, puis de **mettre en œuvre techniquement une maquette de solutions de ce type**, sur des cas d'usages listés au préalable.

> Tes missions

> **Comprendre les enjeux & identifier les problématiques liées aux solutions actuelles**

- Comprendre les architectures de messagerie et de collaboration, classiques et dans le Cloud
- Comprendre les mécaniques et les techniques d'attaques par email utilisées par les attaquants
- Evaluer les risques auxquels font face les entreprises sur le périmètre de la collaboration

> **Etudier l'état de l'art des solutions de sécurisation des emails**

- Comprendre les différentes topologies de solutions de sécurité emails (Cloud provider, SEG, ICES)
- Etudier les fonctions techniques et opérationnelles de sécurité de la messagerie (anti-spam, anti-phishing, anti-malware, SPF/DKIM/DMARC, URL rewriting, sandboxing, UEBA, campagnes de phishing, etc.)
- Etudier le marché des solutions actuelles et mener une étude comparative sur une sélection de celles-ci

> **Etudier fonctionnellement et techniquement des solutions de sécurisation des emails**

- Proposer une étude technique sur quelques solutions choisies
- Identifier les cas d'usages et les scénarios de sécurité des emails, puis construire un outil d'évaluation des solutions
- Mettre en œuvre les solutions dans un environnement de maquette, et évaluer les fonctionnalités

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité. Tu bénéficies de connaissances générales sur les infrastructures IT.

> Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).

> Tu es autonome tout en sachant communiquer et partager.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

SOC / CERT CWATCH

L'équipe CWATCH opère des services SOC et CERT depuis 2016 avec l'objectif de proposer des services managés cyber défense complets, simples et accessibles pour les PME et ETI. Nous intervenons également en mode conseil, en particulier dans les grands comptes, pour accompagner dans la recherche, la mise en place et l'opération des solutions de cyber défense.

Découvrez nos missions

1. Un stage au sein de l'équipe SOC et CERT permettant de voir ces deux activités complémentaires en un seul stage.

2. Un stage dans le vif des opérations de cyber défense, avec un projet fil rouge en complément.

3. Un stage est vu comme une période de pré-embauche. Un poste au sein du SOC et CERT CWATCH pourrait donc être proposé à son issue.

Analyste SOC / CERT

Tu intègres l'équipe constituée de 30 spécialistes SOC et CERT passionnés dédiés à la veille sur les menaces, la gestion des vulnérabilités, la détection des attaques et la réponse aux incidents de sécurité.

L'activité, principalement composée de services managés (mode MSSP), est au service de la défense des systèmes d'information de plusieurs entreprises et bien sûr de la sécurité interne de notre groupe. Nos experts interviennent également régulièrement en « opération extérieure » pour accompagner des clients sur différents sujets liés aux SOC et aux CERT.

A ce titre, tu es impliqué dans des opérations à forte teneur technique, avec des phases projet de prise en charge sur de nouveaux périmètre à surveiller, des phases opérationnelles & des projets internes d'amélioration des outils, capacité de détection et réaction (SOC), et des opérations de réponse sur incident / forensic (CERT).

> Tes missions

- Tu interviens au côté d'experts sur nos opérations SOC, en rotation sur différentes positions (« shift ») : traitement d'alertes, amélioration des règles de détection, veille sur les menaces, amélioration des outils…
- Tu opères dans un environnement technique riche : SIEM, EDR, SOAR…
- Tu es impliqué, toujours en doublon avec des experts, sur des engagements du CERT en réponse sur incident, recherche de compromission, forensic ou gestion de crise.
- Tu portes un sujet mode projet « fil rouge » lié à l'amélioration d'un outil ou d'un process de nos opérations SOC ou CERT : par exemple amélioration d'un module de détection, d'un système de d'automatisation de remédiation, d'une procédure d'investigation…

Étudiant(e) en dernière année d'école d'ingénieur ou en Master 2, tu recherches un stage de fin d'étude de 6 mois en prévision d'une embauche. Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).

- Tu réalises une veille sécurité personnelle, as une connaissance des techniques d'attaque utilisées par nos adversaires et tu souhaites utiliser ces informations pour construire et opérer une cyber défense efficace.
- Tu maîtrises les aspects théoriques de la sécurité informatique (architecture, environnements cloud, protocoles, cryptographie, authentification, failles classiques et moins classiques, etc.)
- Tu souhaites travailler en équipe et est prêt à délivrer de l'expertise cyber défense dans toutes les conditions et modèles de service possibles.
- Tu sais coder / scripter et refaire 5 fois une opération inintéressante t'exaspère.
- Tu sais faire des points de situation clairs sous tension et rédiger des analyses et recommandations percutantes.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

OFFENSIVE SECURITY

Notre équipe est composée d'environ 20 consultants 100% dédiés à ces missions : tests d'intrusion, audit sécurité de code source, analyse sécurité d'architecture, analyse sécurité des configurations, pédagogie. Les consultants sont tous des passionnés, experts du domaine et certifiés (PASSI, OSCP, CISSP, SANS, certifications cloud Azure et AWS, etc.)

Découvrez nos missions

1. Un stage au sein de l'équipe Offensive Security, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années, ayant rédigé plusieurs articles techniques sur des sujets divers de la sécurité offensive.

2. L'équipe offre une grande liberté sur l'environnement de travail : outils, système d'exploitation, etc.

3. C'est également un stage qui permet une forte montée en compétence : participation à de nombreux tests d'intrusions sur de multiples systèmes et technologies.

4. Ce stage est vu comme une période de pré-embauche. Un poste de pentester en CDI peut donc être proposé à son issue.

Ethical Hacker / Pentester

L'équipe Offensive Security, constituée d'une quinzaine de pentesters passionnés, est 100% dédiée aux tests d'intrusions et audits techniques en sécurité des systèmes d'information.

L'équipe réalise des audits à forte teneur technique sur des sujets variés allant du test intrusif d'application web ou mobile aux audits à grande envergure sur les réseaux internes de nos clients.

> Tes missions

- Intervention sur des tests d'intrusion en conditions réelles avec des pentesters expérimentés
- Recherche de vulnérabilités sur les systèmes audités et exploitation avec des outils au choix ou développés pour l'occasion
- Participation à des analyses d'architectures réseaux et systèmes complexes
- Possibilité de participer au développement de nos outils internes, nouveaux ou existants, et à la R&D sur de nouvelles vulnérabilités ou techniques d'attaques

Étudiant(e) en dernière année d'école d'ingénieur ou en Master 2, en recherche d'un stage de fin d'études de 6 mois en prévision d'une embauche.

- Compréhension et maîtrise aisée de nouvelles techniques
- Maîtrise des aspects théoriques de la sécurité informatique (architecture, protocoles, cryptographie, authentification, failles classiques et moins classiques, etc.)
- Maîtrise des concepts à la base des techniques d'intrusion, y compris les plus manuels (forge de paquets, écriture de scripts/programmes d'attaques dédiés, désassemblage/debugging, etc.)
- Maîtrise d'un ou plusieurs langages de programmation ou de scripting
- Réalisation d'une veille technique spécialisée via la lecture de publications techniques, la participation à des conférences de sécurité…
- Maîtrise suffisante de l'anglais pour lire des articles techniques ainsi que pour communiquer à l'oral et à l'écrit.

Le profil présenté est le profil idéal, toutes les candidatures seront étudiées, même celles ne correspondant pas parfaitement

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

GOVERNANCE, RISKS & COMPLIANCE

La mission de notre équipe GRC : permettre d'accéder à l'équilibre autorisant la juste protection des actifs et des activités, et de réussir la mise en place d'une approche holistique de la sécurité, grâce à une approche pragmatique de la gestion de risques.

Découvrez nos missions

1. Un stage au sein de l'équipe Governance, Risks & Compliance, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.

2. Un accompagnement et un suivi de stage par des experts qui garantissent un véritable apprentissage du domaine.

3. Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

PCI DSS dans le Cloud

Ta mission principale sera de participer à la mise en conformité PCI DSS d'une plateforme de démonstration hébergée sur le Cloud Azure avec du trafic de données cartes bancaires simulé, ayant vocation à être présentée à nos clients.

Cela consistera à définir les processus de sécurité nécessaires, et les mettre en œuvre (rédaction de la documentation associée, identification des solutions et mise en œuvre technique) et te permettra de monter en compétence de manière ludique sur l'industrialisation de nos processus de contrôle.

> Tes missions

Après une prise de connaissance et une formation interne sur le standard PCI DSS, la mission consistera plus précisément :

- A t'auto-former sur Microsoft Azure
- A découvrir notre plateforme PCI DSS hébergée sur Azure et mise en place depuis le premier semestre 2022
- A auditer cette plateforme avec le référentiel v4.0 PCI DSS pour produire un « gap analysis » et un « plan de remédiation »
- A mettre en œuvre une partie de ce plan de remédiation :
  - Faire évoluer l'architecture de la plateforme (ie. ajout de nouveaux services et/ou composants)
  - Mettre en place les processus et exigences PCI DSS non couvertes jusqu'ici (exemples : chiffrement des données stockées, dashboard pour monitorer les évènements de sécurité, mise en place d'un processus de patch management, mise en place d'une solution antimalware et/ou EDR, mise en place du durcissement des configurations, etc.)
- A documenter l'ensemble de tes travaux au sein de documents de référence qui seront utilisés par les consultants experts PCI DSS d'ALMOND
- A présenter tes travaux lors de différents points d'équipe

Lors de cette mission, tu seras amené à étudier les thématiques de sécurité suivantes :

- Scoping PCI DSS et Chiffrement
- Modèles du Cloud computing (SAAS, IAAS, PAAS …) et Virtualisation
- Sécurité réseau, sécurité système, sécurité organisationnelle, sécurité applicative, sécurité physique. En parallèle, tu interviendras avec nos consultants sur des missions secondaires en lien avec la sécurité de l'information et la gestion des risques SSI :
- Missions d'audit et/ou d'accompagnement à la mise en conformité, avec intervention en clientèle au côté d'un collaborateur expérimenté
- Elaboration de supports de formations
- Rédaction d'articles de sécurité pour publication dans la presse Tu pourras intervenir sur différents référentiels de sécurité (PCI DSS, ISO 27k, HDS, RGPD…).

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité. Tu bénéficies de connaissances générales sur les infrastructures IT.

- Tu aimes travailler en équipe et partager tes connaissances.
- Tu es dynamique, curieux et tu fais preuve d'initiatives.
- Tu es doté d'un grand sens de l'organisation, rigoureux, et a de solides capacités organisationnelles.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Construction d'un référentiel de maturité des dispositifs DLP

Les fuites de données représentent l'un des risques majeurs pour les organisations. C'est dans ce cadre que les organisations définissent au sein de leur politique de sécurité des mesures permettant de réduire leur exposition à cette typologie de risque.

L'implémentation de dispositifs de détection des fuites de données (DLP) est l'une des mesures permettant aux organisations de mitiger le risque de fuites de données. Ces dispositifs regroupent les moyens techniques et organisationnels permettant d'identifier, de limiter et de remédier aux fuites d'informations sensibles d'une organisation.

Almond accompagne ses clients dans la mise en œuvre et dans l'exploitation de ces dispositifs DLP, notamment à travers un centre de services qui traite les alertes générées par différentes sondes DLP.

> Tes missions

Dans cette optique, l'équipe opérant le centre de services DLP recherche un ou une stagiaire pour la construction d'un référentiel de maturité des dispositifs de détection des fuites de données. L'objectif d'un tel référentiel est de mesurer l'écart existant entre les moyens mis en œuvre au sein d'une organisation et les bonnes pratiques / normes relatives aux dispositifs DLP.

- C'est dans ce contexte que le ou la stagiaire aura pour mission de :
- Comprendre les objectifs ciblés par la mise en place de moyens techniques et organisationnels pour lutter contre les fuites de données ;
- Identifier les éléments pertinents pour la conception du référentiel, notamment par la réalisation de retours d'expérience autour des missions précédemment réalisées et d'une recherche documentaire ;
- Identifier les thématiques et les axes d'analyse du référentiel de maturité ;
- Formaliser et contextualiser les niveaux de maturité pour chacun des axes d'analyse ;
- Tester le référentiel sur la base des résultats de missions passées ;
- Contribuer à la définition d'une offre d'audit organisationnel des dispositifs DLP ;
- Valoriser les travaux réalisés dans le cadre d'un workshop et la rédaction d'un article de blog.

En complément de ces activités, le ou la stagiaire pourra réaliser un comparatif des solutions de traitement des alertes DLP de manière à faciliter ses différents travaux.

Etudiant.e ingénieur ou équivalent bac+5, tu te spécialise dans les métiers de la sécurité de l'information. Tes connaissances générales sur les infrastructures informatiques te permettent d'appréhender les problématiques liées à la sécurité de l'information. Bien que tu sois une personne curieuse, tu ne souhaites pas forcément mettre tes mains dans « le cœur du réacteur » et tu désires découvrir l'univers du conseil et de l'audit.

- Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).
- Tu es un bon communicant.
- Tu es désireux de travailler et échanger avec des clients et les équipes Almond.
- Tu es quelqu'un de créatif, organisé, autonome et passionné.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Move to Cloud – Move to CISO

Une étude menée conjointement par les cabinets Almond et Eurogroup Consulting en Novembre 2020, intitulée « Le Cloud : panacée de la transformation numérique ? », préconise pour les **RSSI/CISO** de devoir s'adapter rapidement à de nouveaux enjeux : ceux du **partage de la responsabilité de la sécurité avec le Cloud service provider**. La multiplication des risques Cloud et l'**industrialisation des attaques** requiert de **repenser** l'accompagnement des organisations dans leur stratégie de sécurité, en les aidant à se doter d'un RSSI/CISO **adapté, plus pertinent/efficace et mieux informé/armé contextuellement et conjoncturellement**.

Le stage aura donc pour principal objectif **de proposer un modèle stratégico-opérationnel de « Move to Cloud – move to CISO »** qui soit en adéquation avec les référentiels de bonnes pratiques, les exigences règlementaires, les contextes organisationnels en fonction de leur niveau de maturité en cybersécurité et les attentes exprimées par nos clients et leurs RSSI.

> Tes missions

Comprendre la problématique de la sécurité du Cloud et identifier les enjeux à traiter, dans un positionnement de RSSI (tu seras bien sûr aidé) avec les connaissances nécessaires, adaptées aux évolutions actuelles des cybermenaces :

- Paysage des cybermenaces, rapport de force entre attaquants et entreprises, scénarios de risques « sécurité Cloud »
- Référentiels NIST CSF, publications NIST SP 800-145 et CSA, ISO 17788 et exigences règlementaires AMF, CSSF, U.S...
- Niveaux de maturité, diagnostics cybersécurité, analyses de risque et scénarios Cloud
- Fonction RSSI à créer, ou nouvelles compétences de RSSI à renforcer en sécurité Cloud, parcours de formation/coaching

Identifier et analyser des outils de pilotage opérationnel en support des missions du RSSI, en recensant et comparant des solutions logicielles, pour aider à structurer/piloter une stratégie et des plans d'action pour le « Move to Cloud » :

- Tableaux de bord inspirés des grilles de question des régulateurs, des questionnaires Customer-Cloud provider, du registre STAR (Security, Trust and Assurance Registry) des matrices CCM (Cloud Controls Matrix du CSA)
- Analyses de risque, détection/monitoring d'incidents (gestion d'incidents dans le Cloud)
- Programmes de sensibilisation dédiés VIP et collaborateurs pour la « Sécurité dans le Cloud »

Consolider les deux premières composantes (A) et (B), pour proposer un modèle de « Move to Cloud – Move to CISO » :

- Sur la base d'un « Cost, Benefit and Maturity Report » s'inspirant du Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 et des outils (STAR registry, CCM matrix) de la CSA,
- Illustré de cas concrets et scénarios d'exercice pour mise en œuvre des connaissances lors de mises en situation client.
- Ce modèle opérationnel cherche à mieux sensibiliser les parties prenantes et décisionnaires, à étayer la décision d'un « Move to CISO » quand la fonction fait défaut et à épauler les clients en demande de conseil et renforcement des compétences de leurs RSSI en « Sécurité du Cloud ».

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Elève ingénieur (H/F) ou équivalent bac +5 avec une curiosité manifeste pour la cybersécurité et le Cloud car tu bénéficies de connaissances (formation école, séminaires, veille...) :

- Tu as la capacité à prendre du recul face à un problème donné (étude-conseil)
- Tu es un bon communicant
- Tu es désireux de travailler et échanger avec des RSSI/CISO et leurs équipes

Découverte et mise en œuvre des principaux référentiels d'exigence IT/OT

Les activités des équipes Gouvernance, Risques et Conformité d'**Almond** ont permis le développement des **outillages nécessaires** à la conduite d'évaluations ponctuelles comme continues des organisations clientes et de leurs partenaires (clients, fournisseurs, etc.) sur la base de **multiples référentiels** (lois, règlements, normes et standards).

Ces outils prennent diverses formes (Excel, Word, PowerPoint…) et permettent de **déterminer la conformité** et **la maturité des organisations** vis-à-vis des exigences pesant sur celles-ci. Utilisés quotidiennement par les consultants d'Almond, ces outils doivent être **documentés, entretenus et enrichis** pour s'ouvrir à l'industrialisation et à la valorisation des données collectées au gré des missions.

> Tes missions

Les **travaux à réaliser** par le stagiaire seront les suivants :

- Participer à l'entretien des kits et outils disponibles
- Participer à l'intégration de nouvelles fonctionnalités et nouveaux référentiels, notamment des référentiels destinés aux systèmes d'information industriels (Operational Technology, OT)
- Développer une méthode de consolidation et de valorisation des données issues des évaluations périodiques et/ou continues
- Participer à la rédaction des spécifications associées et contribuer au pilotage des activités de développement.
- Effectuer une veille réglementaire et une veille sur l'évolution du paysage de la menace sur les systèmes IT et OT

Elève ingénieur (H/F) ou équivalent bac+5 dans le domaine de la sécurité informatique ou des systèmes d'information. La Sécurité des Systèmes d'Information est un domaine qui t'attires et tu souhaites découvrir l'univers du Conseil et de l'Audit.

- Tu connais la suite Microsoft Office
- Les macros et le VBA sont des notions que tu connais au moins de nom
- Tes proches disent de toi que tu es quelqu'un de rigoureux, autonome, curieux et passionné

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Kit pour les orientations Cyber Bancassurances

Sous l'impulsion du **plan d'action FinTech** publié en 2018 par la Commission Européenne, l'**Agence Bancaire Européenne** (ABE) et l'**Autorité Européenne des Assurances et des Pensions Professionnelles** (AEAPP) ont établi des **orientations sur la gestion des risques, la gouvernance et la sécurité des Technologie de l'Information et de la Communication** (TIC) à destination des acteurs de la bancassurance. Ces orientations ont pour objectif de fournir des indications sur le niveau de cybersécurité attendu dans ce secteur afin de **réduire les risques** liés aux TIC dans un **système financier européen très dématérialisé et interconnecté.** L'**Autorité des Marchés Financiers** (AMF) a réalisé concomitamment entre 2017 et 2019 des contrôles de Supervision des Pratiques Opérationnelle et Thématique (SPOT) sur les dispositifs de cybersécurité des sociétés de gestion, signe de cette volonté de traduire à l'échelon national les ambitions européennes.

Le stage aura pour objet de **proposer un kit pour adresser les Orientations ABE et AEAPP auprès de nos prospects bancaires et assurances** en phase d'**avant-vente** puis **auprès de nos clients** en phase de **production**. Ce kit doit nous permettre de **gagner en maturité sur ce segment de marché** en **prouvant notre maîtrise des orientations** émanant des autorités européennes et en **démontrant notre capacité à accompagner** nos clients dans leurs chantiers de mise en conformité.

› Tes missions

- Comprendre et synthétiser les orientations de l'ABE et l'AEAPP pour les commerciaux et les consultants d'Almond.
- Faire émerger des orientations et de nos récentes réponses à appel d'offre les besoins potentiels des prospects sous forme de use cases.
- Sonder les équipes Almond afin de délimiter les services qu'Almond aurait la capacité de fournir sur ce type de missions.
- Préparer des supports d'avant-vente adaptés à l'étude des capacités d'Almond (capability study).
- Déterminer et formaliser les livrables nécessaires pour accélérer la production.
- Communiquer sur le kit de support des missions ABE/AEAPP crée.

Elève ingénieur (H/F) ou équivalent bac +5 avec une curiosité manifeste pour la cybersécurité dans ses aspects gouvernance, risques et conformité car tu bénéficies de connaissances (formation école, séminaires, veille...) :

- Tu as la capacité à prendre du recul face à un problème donné (étude-conseil)
- Tu es un bon communicant
- Tu es désireux de travailler et échanger avec des clients et les équipes Almond

Ce stage donne l'opportunité d'appréhender/analyser un corpus de documents de référence en Cybersécurité pour la bancassurance à l'échelon européen et d'examiner leur portée opérationnelle nationale.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Assistance à la sécurisation des services externalisés

Vous ferez partie intégrante de l'équipe IS Gouvernance & Conformité et participez au développement des services proposés par Almond à ses clients. Votre mission principale consistera à la réalisation d'outils pour l'accompagnement de nos clients qui souhaitent proposer des services d'externalisation sécurisée (IAAS, SAAS, PAAS) qui répondent aux attendus réglementaires, aux bonnes pratiques édictées par l'ANSSI (Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité, Cahier des clauses administratives générales 2021, Guide Externalisation de l'ANSSI, Cloud Security Alliance.).

Après une prise de connaissance des moyens déjà en place, la mission consistera :

- A référencer les règlements, guides et standards existants en établissant un comparatif de ces derniers.
- A établir les outils d'étude du niveau de maturité selon les guides, règlement et référentiels retenus.
- A établir/mettre à jour les outils de gestion d'externalisation (PAS, PAQ, PPR, Comitologie, Outil de recette).
- A accompagner des consultants séniors en mission pour éprouver les outils créés.

Tes missions

Lors de cette mission, vous serez amené à étudier les thématiques de sécurité suivantes :

- Modèles du Cloud computing (SAAS, IAAS, PAAS …) et Virtualisation
- Sécurité des contrôles d'accès et de l'exploitation des services Cloud
- Sécurité réseau (architecture réseau, firewall, DMZ…) et système (durcissement, antivirus, gestion des accès, logs…)
- Sécurité organisationnelle (gestion des incidents, veille sécurité, analyse de risques, rôles et responsabilités…)

Cette mission vous permettra de monter en compétence de manière ludique sur l'industrialisation de nos offres. Vos travaux seront réutilisables par nos consultants, qui adressent aussi bien ISO 27001 que d'autres référentiels, dans leurs interventions auprès de nos clients.

En parallèle, vous interviendrez avec nos consultants sur des missions secondaires en lien avec la sécurité de l'information et la gestion des risques SSI :

- Missions d'audit et/ou d'accompagnement à la mise en conformité, avec intervention en clientèle au côté d'un collaborateur expérimenté
- Élaboration de supports de formations et rédaction d'articles de sécurité pour publication dans la presse
- Vous pourrez intervenir sur différents référentiels de sécurité (PCI DSS, ISO 27k, HDS, RGPD…).

Étudiant(e) en école d'ingénieur, vous recherchez un stage de fin d'étude de 6 mois en prévision d'une embauche. Tu connais la suite Microsoft Office

- Vous aimez travailler en équipe et partager vos connaissances.
- Vous êtes dynamique, curieux(se), bon communiquant et faites preuve d'initiative.
- Vous êtes doté(e) d'un grand sens de l'organisation, êtes rigoureux(se), avez une forte capacitée d'analyse et de solides capacités rédactionnelles.
- Vous aimez travailler sur des sujets techniques liés à la sécurité des systèmes d'information.

Stage de 6 mois - basé à Nantes

1250€ / mois + Titre restaurant + Remboursement transport + Congés payés

STRATEGY, GOVERNANCE & TRANSFORMATION

Nous accompagnons nos clients lors des étapes importantes de l'évolution de leur Système d'Information. Notre objectif est de proposer à chaque client une approche, des outils et une feuille de route répondant spécifiquement à leur contexte.

Découvrez nos missions

1. Un stage au sein de l'équipe Digital & Technology, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.

2. Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

Cloud & FinOps

Tu seras rattaché(e) à la practice Digital & Technology qui accompagne ses clients Grands Comptes et Entreprise de Tailles Intermédiaires sur leurs enjeux, réflexions et problématiques autour du Cloud.

> Tes missions

Sous le pilotage d'un tuteur de stage et en s'appuyant sur tes collègues experts, tes missions seront :

Etudier l'état de l'art du marché du cloud

- Cartographie des acteurs français, européens, mondiaux.
- Evaluation des impacts de la crise Covid sur le marché, les tendances et les usages.
- Recensement des technologies Cloud actuelles et à venir.

Construire l'outillage permettant d'accompagner nos clients dans la réalisation de missions opérationnelles

- Elaboration d'un référentiel de diagnostic et de définition d'une trajectoire/roadmap Cloud.
- Consolidation des offres et expertises et animation des groupes de réflexions sur les problématiques Cloud, en interne.

Développer le segment FinOps de l'offre Cloud

- Benchmarking des solutions FinOps du marché.
- Etude des leviers/actions FinOps pour mesurer et maitriser l'empreinte carbone des entreprises (FinOps & GreenOps).

Sécuriser les environnements Cloud

- Etude des solutions de sécurité en environnement Cloud par brique de services.

Elève ingénieur (H/F) ou équivalent bac +5

- Tu bénéficies de connaissances générales sur les infrastructures IT et les nouvelles technologies digitales des entreprises.
- Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).
- Tu es un(e) bon(ne) communicant(e).
- Tu aimes travailler en équipe et partager tes connaissances.
- Tu disposes de fortes capacités rédactionnelles et de présentation.
- Tu as envie d'apprendre et de monter en compétences sur les technologies actuelles et à venir.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Consultant stratégie & transformation digitale

Almond se positionne comme un acteur français indépendant incontournable de l'audit et du conseil dans les domaines de la Cybersécurité, du Cloud et des Infrastructures :

- 200 collaborateurs
- 2/3 des sociétés du CAC 40 déjà clientes de Almond
- 5 implantations : Sèvres, Nantes, Strasbourg, Lyon et Genève

Tu es rattaché(e) à l'équipe Stratégie, Gouvernance et Transformation pour la réalisation opérationnelle de missions d'audit et de conseil auprès de clients grands comptes et entreprises de taille Intermédiaire.

> Tes missions

Au cours de ton stage tu pourras travailler sur :

- Diagnostic et audit IT, technique et organisationnel
- Schéma Directeur SI & définition de trajectoires Cloud et Data
- Accompagnement sur les projets DSI, Cloud, Data, RPA
- Organisation de la fonction SI et modèle opérationnel
- Pilotage de la performance, optimisation des coûts (FinOps)
- Aide au choix de partenaires et de solutions

En fonction de ta maturité sur les sujets traités, tu seras accompagné et soutenu par ton manager et tes collègues experts tout au long de tes missions.

- Tu aimes travailler en équipe et partager tes connaissances
- Tu disposes de fortes capacités rédactionnelles et de présentation
- Tu es un(e) bon(ne) communicant(e)
- Tu as envie d'apprendre et de monter en compétences sur les technologies actuelles et à venir
- Tu as la capacité à prendre du recul face à un problème donné

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

RPA & DATA : Automatisation des flux de données et des processus

Tu seras rattaché(e) à la practice Digital & Technology qui réalise des missions de Robotic Process Automation (RPA) et de Data Strategy auprès de clients Grands Comptes et Entreprise de Tailles Intermédiaires.

La RPA est une technologie permettant l'automatisation de règles et d'activités prédéfinies pour réaliser diverses tâches dans un écosystème applicatif afin de fournir un service de qualité, rapide et fiable. La RPA est un levier important pour accélérer et sécuriser la transformation numérique de nos clients.

La donnée est devenue un actif à part entière de l'entreprise, incontournable dans le processus de création de valeur et d'aide à la décision. Garantir sa qualité, sa durabilité, sa pertinence, sa sécurité et sa disponibilité sont des enjeux majeurs pour les entreprises, puisque facteurs de succès pour sa performance et son innovation. La RPA permet d'assurer aujourd'hui une meilleure exploitation des données avec l'imbrication de l'automatisation dans le processus de traitement de la data, de son extraction jusqu'à sa visualisation ce qui apporte plusieurs avantages non négligeables.

> Tes missions

Sous le pilotage d'un tuteur de stage et en s'appuyant sur tes collègues experts, tes missions seront :

- Conception et développement d'un projet interne de RPA et de gestion des données : comme par exemple mettre en place une solution d'automatisation des processus de back et front-office afin de les libérer des tâches longues et répétitives tout en proposant un reporting d'aide à la décision grâce à une solution de DATAVIZ.
- Cadrage du projet : étude du périmètre d'éligibilité, priorisation des process pertinents.
- Définition des principales fonctionnalités attendues : spécifications fonctionnelles et techniques, échanges avec les équipes de développement et cyber sécurité pour déployer des bonnes pratiques tout au long du cycle de vie du projet.
- Participation au développement de notre offre RPA & DATA : réalisation d'un comparatif poussé des fonctionnalités des différents acteurs y compris Microsoft, définition de la démarche type d'un projet allant du cadrage et des développements, jusqu'à la mise en production et la conduite du changement.
- Elaboration d'un Tool kit pour les consultants RPA et Data.

Elève ingénieur (H/F) ou équivalent bac +5, tu bénéficies de :

- D'une bonne connaissance de la Data (Data Strategy, data Management) et de son cycle de vie.
- D'une bonne connaissance de scripting VBA/Powershell pour l'automatisation et en Data Viz (Power Bi ou Tableau).
- D'une pratique de la programmation, de l'UML et de la conception de logiciels.
- D'une sensibilisation au développement web, en réseau et d'un fort sens de l'observation et d'analyse.

Ce stage est fait pour toi si :

- Tu aimes travailler en équipe et partager tes connaissances.
- Tu disposes de fortes capacités rédactionnelles et de présentation.
- Tu as la capacité à prendre du recul face à un problème donné et as un goût pour la mise en pratique technique.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

ARCHITECTURE & DIGITAL PLATFORM

Nos consultants experts en Cloud et en Infrastructure assistent nos clients dans la conception et l'intégration de leurs architectures ainsi que dans la mise en œuvre et le suivi des nouveaux modèles opérationnels.

Découvrez nos missions

1. Un stage au sein de l'équipe Architecture & Digital Platform, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.

2. Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

Homogénéisation et conformité des équipements Réseaux/Sécurité

Les systèmes informatiques jouent un rôle essentiel dans la performance des entreprises. Une infrastructure IT se doit de rester performante et résiliente afin d'offrir le meilleur service possible pour les équipes métiers et les clients finaux.

Le maintien en conditions opérationnelles et de sécurité du SI est à ce titre une activité primordiale de la DSI, et cette capacité repose largement sur la maîtrise des configurations des équipements exploités.

L'objectif de ce stage est de découvrir ensemble les différentes méthodes et outils (On Premise/Cloud) qui permettront, non seulement, de gérer les fichiers de configuration des équipements réseaux et de sécurité (sauvegarde des fichiers de configuration, Gestion des différentes versions, …) mais aussi de vérifier leurs conformités basées sur des exigences propre à chaque DSI.

> Tes missions

Durant ce stage vous devrez réaliser les tâches suivantes :

- Comprendre les enjeux et identifier les problématiques liées à la gestion des configurations
- Etudier l'état de l'art des solutions du marché
  - Comprendre la segmentation du marché et les différentes approches possibles
  - Identifier les principales solutions commerciales ou libres
  - Analyser leurs principes de fonctionnement (modules SNMP, SSH)
  - Comparer leurs principales fonctionnalités
- Proposer un scenario pour la réalisation d'une maquette
- Mettre en œuvre la maquette en testant, si possible, au moins 2 solutions retenues lors de l'étude

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité. Tu bénéficies de connaissances générales sur les infrastructures IT, le Cloud Computing et des langages de développement :

- Tu as la capacité à prendre du recul face à un problème donné (étude-conseil)
- Tu as un goût pour la mise en pratique technique.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Le marché et les enjeux autour du SASE

Dans le cadre de leurs transformations digitale, de plus en plus d'entreprises ont adopté la migration d'une partie de leurs applications vers le Cloud public. Le réseau WAN traditionnel basé principalement sur le MPLS ne semble pas répondre complétement aux nouvelles exigences dictées par le Cloud. Ce qui incite les entreprises à migrer vers le SD-WAN, qui promet de répondre à ces exigences.

Néanmoins, le SD-WAN amène de nouveaux défis, ainsi que de nouvelles problématiques liées au réseau WAN de l'entreprise, qui nécessite une adaptation des politiques de sécurités. Quelles sont ces nouveaux défis ? Est-ce que le SASE « Secure Access Secure Edge » représente la solution idéale ou c'est juste une mode passagère ? Quelles sont les promesses du SASE ?

Etant une technologie émergente, le SASE suscite beaucoup d'interrogations. Ce stage a pour objectif de répondre à ces dernières.

Pour atteindre cet objectif, il est impératif d'étudier le marché du SASE, et d'identifier ses différents acteurs et produits. Il faudra être en mesure de déterminer les enjeux autour du SASE, les gains attendus, et les risques associés de la mise en production de cette solution.

> Tes missions

A l'issue de cette étude, le stagiaire devra être capable d'analyser le marché du SASE et de ses enjeux.

> Etude de l'existant

- Analyser les architectures actuelles
- Identifier les problématiques liées aux solutions actuelles

> Etudier l'état de l'art de solutions SASE

- Analyser les enjeux du SASE
- Réaliser une étude comparative des solutions du marché SASE

> Maquetter et étudier une solution SASE

- Etude fonctionnelle et technique détaillée d'une solution SASE
- Expérimenter et évaluer les fonctionnalités de la solution SASE dans un environnement de maquette

> Livrables :

- Formaliser les résultats de l'étude sous la forme d'un document utilisable par tous les consultants

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation Réseaux, Systèmes ou Sécurité. Tu bénéficies de connaissances générales sur les infrastructures IT et le Cloud Computing :

> Tu as la capacité à prendre du recul face à un problème donné (étude-conseil).

> Tu as un goût pour la mise en pratique technique.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

board of cyber
security rating®

Board of Cyber est une startup française en hyper-croissance avec 1 mission : créer un écosystème de confiance en incitant les organisations à améliorer en continu leur performance cyber.

Découvrez nos missions

1. Un stage au sein de l'équipe SSP, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.

2. Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

Développeur junior

Almond se positionne comme un acteur français indépendant incontournable de l'audit et du conseil dans les domaines de la Cybersécurité, du Cloud et des Infrastructures.

Tu intègres l'équipe SSP (Security Service Platform) composée de 7 collaborateurs.

Ta mission principale consistera à aider l'équipe au développement du Security Rating et TPRM, qui est un outil d'évaluation de la maturité cyber des entreprises.

> Tes missions

Le stagiaire intègre l'équipe de développement des outils Security Rating et TPRM pour la durée de son stage sur un poste d'ingénieur d'étude et développement/développeur junior.

Dans ce cadre il intervient sur l'ensemble des composants des systèmes : front-ends (Angular) et back-ends (Java/Spring Boot, Python).

Il participe à la mise en œuvre du nouveau système de collecte des incidents de sécurité, à l'évolutions du système de gestion des vulnérabilités et plus généralement sur les évolutions des modules applicatifs : cartographies, sondes de mesures .../...

L'environnement technologique est le suivant : Angular, HTML / CSS, Typescript / Javascript / Java Spring Boot et projets associés, Python, Gitlab CI/CD, Docker, Kubernetes, Azure Cloud.

Elève ingénieur (H/F) ou équivalent bac +5 avec une spécialisation en Développement ou Ingénierie logicielle.

- Tu as une connaissance sur les technologies listées plus haut.
- Tu as déjà eu l'opportunité de développer au cours de tes études ou expériences
- Tu maitrises les fondamentaux des infrastructures réseau/système et de la sécurité applicative.
- Tu sais faire des points de situation clairs sous tension et rédiger des analyses et recommandations percutantes.

Stage de 6 mois - basé à Sèvres

1500€ / mois + Titre restaurant + Remboursement transport + Congés payés

Pour plus d'informations, contactez-nous !

almond

› Contact pour ce dossier

Anass ROUASS
Campus Manager
arouass@almond.consulting
+33 (0)1 46 48 26 49

https://almond.consulting