GET
READY
TO
JOIN
THE
G-TEAM

BOOK DE STAGES 2024

Almond

Almond

Almond est un acteur majeur français indépendant de l'audit, du conseil, de l'intégration et des services managés en Cybersécurité, Cloud et Infrastructures.

Découvrez nos offres de stages

01.
INFRASTRUCTURE SECURITY

02.
SOC / CERT CWATCH

03.
OFFENSIVE SECURITY

04.
GOVERNANCE, RISKS & COMPLIANCE

05.
DIGITAL TECHNOLOGY

06.
SECURE CLOUD & MANAGED SERVICES

GET READY TO JOIN THE -TEAM ?

UN STAGE CHEZ ALMOND

- Un stage au sein d'Almond, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années.
- Un accompagnement et un suivi de stage par des experts qui garantissent un véritable apprentissage du domaine.
- Un stage est vu comme une période de pré-embauche. Un poste de consultant en CDI pourrait donc être proposé à son issue.

LES AVANTAGES

01.

L'environnement

De grands locaux refaits à neuf avec des services dédiés : conciergerie, cours de sport, RIE... et surtout, les salles de pause équipées pour s'affronter sur la SWITCH

02.

La rémunération

- 1500€ à Paris
- 1350€ à Lyon
- 1250€ à Nantes

+ remboursement du titre de transport
+ titre restaurant

03.

Les events

Journée d'intégration, soirées à thème, escape game, soirée jeux de société, week-end ski annuel, events sportifs

INFRASTRUCTURE SECURITY

L’équipe est constituée de consultants 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).

Authentification SSO & MFA

Description

Les interconnexions croissantes des systèmes d'information 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'identité 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 MFA :

- Etude 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 le 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.

Stage de 6 mois basé à Sèvres

Voir l'offre

Sécurisation des E-mails

Description

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'information, 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 liées 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.

Stage de 6 mois basé à Sèvres

Voir l'offre

01. Tu es élève ingénieur ou équivalent BAC + 5 avec une spécialisation Réseaux, Systèmes ou Sécurité et tu bénéficies de connaissances générales sur les infrastructures IT ?

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

03. Tu es autonome tout en sachant communiquer et partager ?

ON N'ATTEND PLUS QUE TOI !

Nos offres Infrastructure Security

- Authentification SSO & MFA
- Sécurisation des E-mails

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.

Analyste SOC / CERT H/F

Description

Tu intègres l'équipe constituée de 40 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 périmètres 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 aux côtés 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 d'automatisation de remédiation, d'une procédure d'investigation.

Stage de 6 mois basé à Sèvres

Voir l'offre

01. Tu es élève ingénieur ou en Master 2, en recherche d'un stage de fin d'études de 6 mois en prévision d'une embauche ?

02. Tu maîtrises les aspects théoriques de la sécurité informatique (architecture, environnements cloud, protocoles, cryptographie, authentification, failles classiques et moins classiques, etc.) ?

03. Tu sais coder / scripter et refaire 5 fois une opération inintéressante t'exaspère ?

ON N'ATTEND PLUS QUE TOI !

Notre offre SOC / CERT CWATCH

→ Analyste SOC / CERT

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.)

Ethical Hacker / Pentester H/F

Description

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.

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.

L’équipe offre une grande liberté sur l’environnement de travail : outils, système d'exploitation, etc. Ce stage technique permet une forte montée en compétences : participation à des tests d’intrusion réels, sur de multiples environnements, toujours en collaboration avec des auditeurs expérimentés.

Tes missions

- Intervention sur des tests d’intrusion en conditions réelles en collaboration avec des pentesters expérimentés : tests d’intrusion web, sur des applications mobiles, des Clients lourds, mission Red Team, etc.;
- Recherche de vulnérabilités sur les périmètres audités et exploitation de celles-ci avec des outils au choix ou développés pour l’occasion;
- Réalisation de rapports et de supports de restitutions à destination des clients;
- 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.

Stage de 6 mois basé à Sèvres

Voir l’offre

01. Tu es élève ingénieur ou en Master 2, en recherche d'un stage de fin d'études de 6 mois en prévision d'une embauche ?

02. Tu as une première expérience en hacking : participation à des CTF, plateformes d'exercices (type « root-me », « Hack the Box », etc. ?

03. Tu connais 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.) ?

ON N'ATTEND PLUS QUE TOI !

Notre offre Offensive Security

→ Ethical Hacker / Pentester

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.

Elaboration d’une base de connaissance de solutions du marché pour répondre aux bonnes pratiques de sécurité

Description

Les normes et les référentiels en sécurité préconisent une liste de bonnes pratiques à mettre en place pour avoir un niveau minimal adéquat de sécurité du système d’information. La mise en place de certaines bonnes pratiques se traduit par l’adoption d’une solution technique qui existe sur le marché.

Le stage aura pour objet de faire un benchmark des solutions existantes sur le marché pour chaque bonne pratique. La réalisation de ce benchmark permettra les consultants GRC de partager avec les clients leurs recommandations dans le cadre de la sélection des solutions.

Tes missions

- Lecture des référentiels (ANSSI, NIST, ISO 27002) pour extraire les bonnes pratiques de base;
- Définir la liste des bonnes pratiques minimales et communes à mettre en place chez les entreprises;
- Réaliser une comparaison des solutions du marché en se basant sur des critères définis et propres à chaque type de solution;
- Les livrables attendus:
  - un document qui servira comme référentiel pour les consultants au sein de l’équipe pour qu’ils/elles puissent se renseigner sur les solutions leader du marché en cas de besoin;
  - une présentation de la démarche suivie et des résultats.

Stage de 6 mois basé à Sèvres

Voir l’offre

Sécurité des SI & IA

Description

Les outils d'IA ne sont pas nouveaux, mais l'engouement pour le ChatGPT les a définitivement ramenés à la une des journaux - les masses se précipitant pour mettre en œuvre "Comment utiliser le ChatGPT un client". Qu'il s'agisse d'écrire des poèmes ou de gagner du temps au travail, nous sommes-nous arrêtés pour réfléchir à la manière de former les employés à l'utilisation intelligente de ces outils tout en protégeant les données de l'entreprise ?

Il est important que la formation de sensibilisation à la sécurité inclue les dernières tendances afin d'aider vos employés à se tenir au courant des nouvelles menaces potentielles. Les cybercriminels sont constamment à l'affût de sujets populaires et en vogue dont ils peuvent tirer parti, comme c'est le cas avec le dernier outil d'IA qui fait la une des journaux.
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 liés à l'utilisation des outils IA.

Tes missions

- Comprendre les concepts, le fonctionnement et les enjeux de sécurité associés aux outils IA;
- Identifier les risques associés;
- Examiner les orientations de l'ANSSI;
- Etudier les principales solutions et architectures;
- Identifier les bonnes pratiques et mettre en œuvre ces dernières;
- Identifier les nouvelles tendances ou fonctionnalités émergentes prometteuses;
- Ces éléments devront se concrétiser dans un livrable qui pourra éventuellement être mis à la disposition de nos clients.

Stage de 6 mois basé à Sèvres

Voir l'offre

Coordination & optimisation des activités de R&D multi-référentielles GRC

Description

Almond / Hifield / Amossys investit chaque année beaucoup de temps en R&D, et chacun des collaborateurs de l'entreprise a du temps à y consacrer se doit de contribuer à cet effort collectif.

Au-dehors, le monde est foisonnant du côté de la production des standards, normes et réglementations applicables au domaine de la sécurité et du traitement du risque Cyber : DORA, NIS2, CRA, CMMC, nouvelles versions de l'ISO, EUCS, etc.

Nos clients ont besoin de s'y retrouver et d'optimiser leur engagement afin de ne pas se noyer tout en réussissant à respecter ce qui doit l'être. Nous nous faisons fort de les y aider et de les accompagner vers l'idéal du « test once – comply many ».

Pour ce faire, nos travaux de recherche sont coordonnés et visent à faciliter la vie de nos clients et de nos collaborateurs pour permettre de faire une sécu efficace ne nécessitant pas de production documentaire inutile.
Le contexte extérieur étant dense, il nous faut renforcer notre capacité en améliorant le pilotage actuel de notre R&D à l'aide d'un jeune et sémillant stagiaire : toi !

Tes missions

- De co-animer un programme de R&D et ses sous-projets;
- De participer à la coordination de la création de nos outils et de nos offres « support à l'audit et à la conformité » et « PNL (PASSI, PACS, NIS1/2, LPM 2016 / 2022, II901, 1300 & consorts);
- D'animer des réunions;
- De recetter les livrables produits par les autres forces vives de l'entreprise;
- De contribuer à la mise en place du conflict check, de la QA et de l'amélioration continue de nos offres.

Stage de 6 mois basé à Sèvres

Voir l'offre

Amélioration des outils et de la démarche d'audit technique

Description

L'ouverture croissante du Système d'Information et la mobilité des données et des utilisateurs requièrent de repenser les stratégies de sécurité et de les décentrer du périmètre classique du système d'information.
Dans le même temps, les attaquants sont de plus en plus inventifs pour essayer de contourner les mesures de sécurité. L'ensemble des équipes informatiques sont confrontées à ce phénomène. La complexité des systèmes d'information et la multiplication des outils compliquent leur travail dans la sécurisation des différents actifs.
Il devient difficile de s'assurer que les configurations apportées aux composants de leurs systèmes ou bien les choix d'architectures réalisés répondent bien aux enjeux de sécurité d'aujourd'hui.

Le stage aura pour objectif principal d'améliorer la démarche d'audit de technique réalisé, ainsi que les outils utilisés. Dans le but de proposer à nos clients une vue plus précise du niveau de sécurisation technique de leur système d'information.

Tes missions

Comprendre les enjeux & identifier les problématiques liées à la démarche actuelle :

- Comprendre la démarche d'audit et sa philosophie;
- Appréhender les outils actuels;
- Réaliser un état des lieux de la démarche et l'outillage.

Proposer des axes d'amélioration de la démarche :

- Proposer un plan d'action pour améliorer la démarche;
- Mettre en place ce plan d'action;
- Présenter et former les consultants sur cette nouvelle démarche.

Étudier et tester des outils de vérification technique :

- Identifier les contrôles à réaliser dans un SI;
- Définir des outils ou méthodes pour vérifier ces points de contrôles;
- Mettre en forme et présenter les résultats de contrôles;
- Documenter les vérifications pour être facilement exploitables par les consultants.

Stage de 6 mois basé à Nantes

Voir l'offre

Assistance à la sécurisation des services externalisés

Description

Vous ferez partie intégrante de l'équipe IS Gouvernance & Conformité et participerez au développement des services proposés par Almond à ses clients.

Tes missions

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, règlements et référentiels retenus;
- A établir/mettre à jour/adapter les outils de gestion des prestations d'externalisation (PAS, Convention de service, PAQ, PPR, Comitologie, Outil de recette);
- A accompagner des consultants séniors en mission pour éprouver les outils créés.

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

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

Stage de 6 mois basé à Nantes

Voir l'offre

Méthode d'audit de la sécurité des développements

Description

L'ouverture croissante du Système d'Information et la mobilité des données et des utilisateurs requièrent de repenser les stratégies de sécurité et de les décentrer du périmètre classique du système d'information.
Dans le même temps, les attaquants sont de plus en plus inventifs pour essayer de contourner les solutions de sécurité classiques avec des cinématiques d'attaques toujours en évolution. En particulier, les failles dans des applications exposées représentent un vecteur d'attaque de plus en plus important. Ce phénomène s'accroit avec l'utilisation de services Cloud, ou de méthodes privilégiant une mise en production rapide des projets (DevOps, …)

Le stage aura pour principaux objectifs de proposer une démarche d'audit des pratiques de sécurité des développements, en s'appuyant sur un état de l'art des référentiels existants, de construire un outillage d'audit et d'accompagnement en appui de cette démarche, et d'élaborer des offres d'audit et d'accompagnement à la sécurisation des développements s'insérant en complément des missions les plus recherchées par les clients de l'agence.

Tes missions

Comprendre les enjeux de sécurisation des développements et identifier les axes d'audit pertinents :

- Comprendre les principales sources de vulnérabilités dans les développements;
- Etudier les modèles et référentiels permettant de mesurer la maturité d'une entreprise pour la sécurité de ses développements, à commencer par le modèle SAMM de l'OWASP;
- En proposer une hiérarchisation en fonction du contexte technologique et de la maturité de l'entreprise ciblée.

Construire un outillage d'audit et d'accompagnement à la sécurisation des développements :

- Identifier les axes d'audit pertinents, les points de contrôle détaillés à vérifier, et proposer une notation équilibrée;
- Proposer des axes d'amélioration recommandés pour chaque axe d'audit identifié;
- Segmenter les points de contrôle selon deux grilles d'analyse : l'une détaillée, destinée à un accompagnement dans la durée de type ISO 27001 ; et l'autre synthétique, destinée à un audit flash;
- Outiller l'ensemble de manière à générer facilement un rapport d'audit et des recommandations.

Elaborer des offres d'audit et d'accompagnement à la sécurisation des développements :

- Participer à la réalisation d'un document marketing utilisable en avant-vente, incluant l'estimation des temps à prévoir;
- Présenter la démarche aux consultants Almond, et former ceux qui l'utiliseront;
- Initier les documents supports à l'accompagnement suite à l'audit : modèles de procédures applicables, référentiel d'outils du marché, etc.

Stage de 6 mois basé à Nantes

Voir l'offre

Sauvegardes et résilience des entreprises

Description

Les risques de sécurité du SI, notamment le risque de ransomware, augmentent et atteignent des niveaux records. Les entreprises doivent se préparer à subir une attaque. Le nombre d'attaquants et leurs moyens sont également de plus en plus importants.

Dans ce contexte, la mission d'Almond est d'aider les entreprises à se préparer le mieux possible et de manière pragmatique aux attaques et risques pesant sur le SI.

Ce stage aura pour objectif principal d'améliorer la résilience des entreprises en s'assurant qu'une des premières étapes de la sécurité est maîtrisée : les sauvegardes. Dans le but de proposer à nos clients une vue précise de leur capacité à réagir et restaurer leur système d'information.

Tes missions

Comprendre les enjeux :

- Comprendre la démarche d'audit et d'accompagnement d'organismes;
- Comprendre l'enjeux des sauvegardes et des tests de restauration, une mesure essentielle pour la résilience;
- Réaliser un état des lieux de la démarche et de notre outillage.

Outillage :

- Maitriser les best-practices du domaine, notamment l'identification des Recovery Point Objective (RPO) et Recovery Time Objective (RTO);
- Segmenter les points de contrôle selon une grille de contrôle;
- Définir différents indicateurs pouvant être utilisés par des sociétés de 100 personnes à plusieurs milliers de personnes.

Elaborer des offres :

- Participer à la réalisation d'un document marketing utilisable en avant-vente, incluant l'estimation des temps à prévoir;
- Présenter la démarche aux consultants Almond, et former ceux qui l'utiliseront;
- Présenter les outils à des clients.

Stage de 6 mois basé à Nantes

Voir l'offre

Maintien en condition de Cybersécurité

Description

Dans le cadre du développement de l'Agence lyonnaise, nous sommes à la recherche d'un stagiaire pour intervenir sur des sujets de GRC et plus particulièrement sur le domaine du contrôle permanent (SMSI, PCI, LPM, NIS, ISO 2700x, HDS, SWIFT, …).

Tu auras l'occasion de travailler sur notre offre de service « Maintien en condition de sécurité » et aborder également les sujets de l'automatisation. En parallèle de ce « fil rouge » tu seras amené à participer à des missions clients pour découvrir le métier du conseil.

Tes missions

La mission consistera plus précisément à définir l'expression de besoin pour un outil permettant de répondre à nos besoins.

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

- Les grands standards de sécurité (ISO 27xxx, PCI, LPM, NIS, SWIFT …) et leurs évolutions;
- Travailler sur les bonnes pratiques de sécurité et de maintien en condition de sécurité (ANSSI, SMSI, …);
- Acquérir & Approfondir tes connaissances en cybersécurité sur différentes technologies (Antivirus, Firewall, IDS/IPS, DNS, Active Directory, Proxy, NTP, Patching, Vulnérabilités, WAF, Bastion, Identification & Authentification, etc.);
- Participer à l'élaboration d'indicateurs pour nos clients.

En parallèle :

- Tu interviendras au côté d'un consultant expérimenté sur des missions de conseils en sécurité SI, d'audit et/ou d'accompagnement à la mise en conformité chez de vrais clients afin de t'imprégner à ton futur métier en lien avec la sécurité de l'information et la gestion des risques SSI;
- Tu participeras au développement de nos outils et méthodes de travail (élaboration de supports de formation, développement d'offre, etc.).

Stage de 6 mois basé à Lyon

Voir l'offre

01. Tu es élève ingénieur ou équivalent BAC + 5 dans le domaine de la sécurité informatique ?

02. Tu es un bon communicant et tu parles couramment anglais ?

03. Tu es désireux de travailler et échanger avec des clients et les équipes Almond ?

ON N'ATTEND PLUS QUE TOI !

Nos offres Governance, Risks & Compliance

- Elaboration d'une base de connaissance de solutions du marché pour répondre aux bonnes pratiques de sécurité
- Sécurité des SI & IA
- Coordination & optimisation des activités de R&D multi-référentielles GRC
- Amélioration des outils et de la démarche d'audit technique
- Assistance à la sécurisation des services externalisés
- Méthode d'audit de la sécurité des développements
- Sauvegardes et résilience des entreprises
- Maintien en condition de Cybersécurité

DIGITAL TECHNOLOGY

Notre équipe Digital & Technology accompagne nos clients dans la définition et la mise en œuvre de leur ambition digitale.

Consultant CIO Advisory H/F

Description

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 :

- 400 collaborateurs
- 350 clients actifs dont 2/3 des sociétés du CAC 40
- 8 implantations : Sèvres, Nantes, Rennes, Strasbourg, Lyon, Genève, Montréal, Seoul

Tu es rattaché(e) à l'équipe Digital Technology 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 les types de missions suivantes :

- 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 définition du 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.

Stage de 6 mois basé à Sèvres

Voir l'offre

IT Sustainability : comment concilier Green IT & Cybersécurité ?

Description

Almond vous offre la possibilité d'explorer la relation entre Cybersécurité et Green IT. Les enjeux climatiques actuels amènent à plus de sobriété numérique. Le Green IT en est un des leviers en visant à réduire l'impact environnemental des technologies de l'information, notamment en réduisant la consommation d'énergie et en favorisant l'utilisation de ressources durables.

A contrario, l'état de la menace Cyber impose aux organisations de faire appel à un écosystème de moyens et solutions de sécurité pouvant être très consommateurs.

Comment alors concilier ces deux impératifs de transformation et de sécurisation ?

Tes missions

- Mener une étude pour évaluer les pratiques actuelles en matière de cybersécurité au sein des organisations et matérialiser les écarts avec les principes de Green IT;
- Identifier les opportunités d'amélioration et de convergence entre la cybersécurité et le Green IT, en mettant l'accent sur les solutions technologiques éco-responsables;
- Proposer des recommandations pratiques pour aligner les pratiques de cybersécurité avec les objectifs de durabilité des organisations.

Stage de 6 mois basé à Sèvres

Voir l'offre

Stratégie de gestion des flottes de terminaux mobiles

Description

Le nomadisme et la mobilité sont parties intégrantes des systèmes d'information des entreprises. Sécuriser les flottes de terminaux mobiles est donc un enjeu majeur afin de répondre aux usages digitaux tout en garantissant une maitrise des end-points du SI.

Tes missions

Réaliser une étude sur les stratégies de gestion des terminaux mobiles dans le cadre d'architectures nomades :

- Définir une stratégie de déploiement des end-points;
- Définir une politique de maintien en conditions opérationnelles / maintien en condition de sécurité des terminaux mobiles.

Approfondir l'étude en traitant le sujet particulier des flottes de terminaux mobiles chiffrés

Réaliser un benchmark des solutions SaaS disponibles pour la gestion des terminaux mobiles :

- Gestion des flottes de terminaux mobiles (MDM);
- Gestion des stratégies mobiles de l'organisation (EMM);
- Gestion des terminaux unifiés (UEM).

Stage de 6 mois basé à Sèvres

Voir l'offre

M&A IT/Cyber : Accompagnement pré-deal et post-deal

Description

Almond accompagne ses clients sur les composantes IT & Cyber de leurs activités transactionnelles (fusion, acquisition, cession). Du pré-deal au post-deal, Almond intervient sur l'ensemble des étapes du cycle de vie des opérations Mergers & Acquisitions, auprès de clients privés, institutionnels, fonds de Private Equity, sur des missions à forts enjeux.

En rejoignant l'équipe IT M&A d'Almond vous serez amené à intervenir sur des missions de Buy-Side Due Diligence, Vendor Due Diligence pour le compte d'acquéreurs ou de cédants ainsi que sur des projets de mise en œuvre type Carve-in / Carve-out.

Tes missions

- Participer au développement et packaging des offres Almond sur l'ensemble du cycle de vie des opérations M&A : Buy-Side et Vendor Due Diligence, Accompagnement Carve-in / Carve-out;
- Enrichir les référentiels d'évaluation IT & Cyber sur les opérations de Buy-Side et Vendor Due Diligence;
- Formaliser les enjeux d'intégration et de séparation IT et leurs implications sur le métier;
- Documenter les axes de réflexion stratégiques sur des opérations carve-in/carve-out et le toolkit de plan de mise en œuvre;
- Participation à la veille sectorielle, à la capitalisation des connaissances et à la rédaction d'article sur cette thématique.

Stage de 6 mois basé à Sèvres

Voir l'offre

Résilience : renforcer la capacité de nos clients à faire face à des incidents majeurs

Description

L’évolution de la menace cyber impose à nos clients de renforcer en permanence leur résilience opérationnelle.

Almond, de par sa forte expertise Cyber et Infrastructure et sa connaissance du cadre réglementaire, accompagne depuis de nombreuses années les PME, ETI et Grands Comptes dans la mise en place de leurs dispositifs de continuité d’activité, dans le but de s'assurer de leur capacité à limiter l'impact d’un incident majeur sur les activités.

Tes missions

- Réalisation d’une étude/benchmark des solutions du marché de Disaster Recovery as a Service (DRaaS) et de backup cloud;
- Développement d’une matrice d’évaluation de la maturité DRP;
- Contribution active au développement de l’offre avec l’équipe DRP Almond, en lien avec nos équipes Cyber Tech & Transformation, GRC et CERT;
- Participation à la veille sectorielle, à la capitalisation des connaissances et à la rédaction d’article sur cette thématique.

Stage de 6 mois basé à Sèvres

Voir l’offre

01. Tu es élève ingénieur ou équivalent BAC + 5 une spécialisation en management des systèmes d'information ou transformation digitale ?

02. Tu es un bon communicant et tu parles couramment anglais ?

03. Tu as envie d'apprendre et de monter en compétences sur les technologies actuelles et à venir ?

ON N'ATTEND PLUS QUE TOI !

Nos offres Digital & Technology

- → Consultant CIO Advisory
- → IT Sustainability : comment concilier Green IT & Cybersécurité ?
- → Stratégie de gestion des flottes de terminaux mobiles
- → M&A IT/Cyber : Accompagnement pré-deal et post-deal
- → Résilience : renforcer la capacité de nos clients à faire face à des incidents majeurs

SECURE CLOUD & MANAGED SERVICES

L’équipe SCMS accompagne nos clients dans la construction d’infrastructures cloud s’appuyant sur un large spectre de technologies : devops, cloud, sécurité, infrastructure, réseau, web…

Ingénieur Réseaux & Systèmes H/F

Description

Tu intègres l'équipe de production MSP, en charge de la gestion de plateformes techniques complexes (sites web, applications métiers web, SI et applications internes) pour une centaine de clients.

L'équipe est composée de 60 passionnés par les technologies des infrastructures capables d'accomplir des prouesses techniques pour l'ensemble de nos clients.
Dans le cadre de nos activités d'infogérance système et réseau, nous gérons des plateformes techniques complexes pour le compte de nos clients Middle Market. Ces équipements sont pour partie situés sur les sites de nos clients, hébergés directement sur les plateformes ou encore sur du cloud Public (Azure ou AWS).

Dans le cadre de la croissance de notre équipe de production, nous cherchons un(e) alternant(e) en tant qu'administrateur système et réseau, qui intégrera l'équipe d'ingénieurs de production.

Tes missions

Tu seras encadré par un ingénieur expérimenté mais toute l'équipe sera là pour t'aider à monter en compétence sur les taches suivantes :

- Résoudre des incidents de production;
- Mettre en place les changements et évolutions sur les systèmes, y compris parfois sous forme de projets (ex: installation et configuration de nouveaux firewall);
- Aider au bon fonctionnement des plateformes de nos clients;
- Rédiger la documentation technique;
- Participer à l'optimisation de nos systèmes de production.

Ton environnement :

Désolé pour cette (longue) liste, mais nous n'avons pas trouvé mieux pour te montrer l'étendue du scope technique sur lequel tu travailleras !

- Cloud : AWS, Microsoft Azure, Office 365;
- Réseau : LAN (Cisco Nexus et Catalyst, Meraki, HP,etc.), Firewalls (Fortinet, Checkpoint);
- Environnements Linux : Debian, NGINX, Apache, Proftpd, …;
- Environnement Windows : OS Windows Serveur (2012/2016/2019), Active Directory, PKI Microsoft;
- Virtualisation / Infrastructure : VMware, SAN Dell EMC;
- Supervision : Centreon (Nagios);
- BDD : MySQL, MS SQL server, ElasticSearch, PostgreSQL ou MongoDB;
- Scripting : Puppet, Ansible, Shell, Powershell, Python;
- Déploiement continu : GitLab-ci.

Stage de 6 mois basé à Sèvres

Voir l'offre

Service Delivery Manager H/F

Description

Tu intègres l'équipe de production MSP, en charge de la gestion de plateformes techniques complexes (sites web, applications métiers web, SI et applications internes) pour une centaine de clients.
L'équipe est composée de 60 passionnés par les technologies des infrastructures capables d'accomplir des prouesses techniques pour l'ensemble de nos clients.

Tes missions

Désormais Service Delivery Manager, tu seras l'interlocuteur privilégié auprès de plusieurs de nos clients Almond pour :

- Être garant de la bonne gestion des infrastructures des clients;
- Fluidifier les échanges entre l'équipe de production et les clients;
- Intervenir sur les incidents d'exploitation;
- Suivre l'avancement des projets initiés par les clients avec nos équipes projets
- Initier et accompagner les clients dans l'optimisation de leurs architectures, en travaillant en binôme avec un expert technique selon ton expérience et tes appétences;
- Participer à la rédaction des propositions commerciales pour faire évoluer les périmètres sous notre responsabilité et suivre la rentabilité des clients, en travaillant avec l'ingénieur d'affaires responsable de ce compte.

Tes objectifs :

- Apporter tes compétences relationnelles et ton expertise;
- Être présent pour notre équipe et les interlocuteurs client afin de les aider à trouver les solutions adaptées aux situations rencontrées;
- Savoir adapter son discours en fonction des interlocuteurs (métiers, sécurité, infra, etc.);
- Poursuivre la construction d'une relation de proximité avec les clients de ton portefeuille;
- Participer à la pérennisation de ces clients.

Stage de 6 mois basé à Sèvres

Voir l'offre

IA – Exploration des LLM pour l'optimisation de nos outils

Description

Au sein de notre équipe dédiée aux outils, l'accent est mis sur deux piliers fondamentaux :

- Développement sur mesure : Création d'outils en PHP/JS conçus pour simplifier les processus internes et introduire de nouveaux services à l'attention de nos clients.
- Intégration et Maintenance : Assurer l'intégration et la maintenance de différentes solutions du marché (monitoring, gestion des tickets, CMDB, SSO, etc.), en veillant à leur interopérabilité pour une synergie optimale.

Tes missions

L'objectif principal de ce stage est d'explorer et de tester des applications pratiques de l'Intelligence Artificielle (IA), notamment les Modèles de Langage à Grande Échelle (LLM) tels que GPT-4, Claude 2, et Llama 2, au sein de notre environnement MSP. En tant que partenaire Azure, l'exploitation des services liés à Azure OpenAI et autres offres IA de ce fournisseur cloud sera privilégiée.

Voici comment se déroulera ton immersion (à priori… Nous sommes ouverts aux propositions !)

Phase de découverte :

- Acquérir une compréhension des opérations et du fonctionnement de notre équipe MSP;
- Initiation aux technologies et outils que nous employons.

Étude de marché :

- Effectuer une revue des modèles LLM actuels et émergents;
- Identifier les potentialités et limitations en rapport avec nos usages.

Identification des cas d'usage :

- Imaginer et sélectionner des cas d'usage prometteurs pour l'IA et les LLM dans l'amélioration de nos outils et services (par exemple analyse de ticket automatique, aide au débug sur Linux,…).

Réalisation de Preuves de Concept (PoC) :

- Elaborer des PoC rapides, en utilisant par exemple le framework Langchain en Python ou d'autres langages appropriés selon tes compétences et préférences.

Évaluation et analyse :

- Analyser les retours sur les PoC, évaluer leur pertinence et la faisabilité (par exemple le cout) de leur mise en production;
- Proposer des stratégies pour l'intégration en production des solutions retenues, en évaluant les efforts requis.

Stage de 6 mois basé à Sèvres

Voir l'offre

01. Tu es élève ingénieur ou équivalent BAC + 5 avec une spécialisation dans le Réseau, Système ou Cloud computing ?

02. Tu es un bon communicant et tu parles couramment anglais ?

03. Tu as un bon relationnel, tu es dynamique et motivé ?

ON N'ATTEND PLUS QUE TOI !

Nos offres Secure Cloud & Managed Services

- Ingénieur réseaux & systèmes H/F
- Service Delivery Manager
- IA – Exploration des LLM pour l'optimisation de nos outils

GET
READY
TO
JOIN
THE

-TEAM

Almond

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

Contact pour ce dossier

Almond Campus
campus@almond.eu
+33 (0)1 46 48 26 49