GET
READY
TO
JOIN
THE
G-TEAM

BOOK DE STAGES 2025

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.
SOC / CERT CWATCH

02.
OFFENSIVE SECURITY

03.
GOVERNANCE, RISKS & COMPLIANCE

04.
CYBER TECHNOLOGY & TRANSFORMATION

05.
SECURE MANAGED SERVICES & INTEGRATION

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

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

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

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.

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

Authentification par mot de passe

Description

L'authentification par mot de passe est un pilier fondamental de la sécurité informatique.

L'objection du stage sera dans un premier temps de fournir une vue d'ensemble sur l'utilisation des mots de passe dans les systèmes d'information, en explorant les différentes méthodes d'authentification, les pratiques courantes et les recommandations des principaux acteurs du domaine. Par la suite, l'étude portera sur les principales solutions et architectures mises en œuvre en entreprise pour utiliser les mots de passe et les interfacer aux autres solutions de SSO et d'authentification forte.

Tes missions

Comprendre les concepts, le fonctionnement et les enjeux de sécurité associés à l'usage de mots de passe :

- Analyse des tendances actuelles et des évolutions historiques en matière de sécurité des mots de passe.
- Identifier les risques associés à la gestion des mots de passe ;
- Étude des différents types d'authentification utilisant des mots de passe et leur pertinence dans divers contextes et cas d'usages.
- Comprendre le fonctionnement du MFA, ses atouts et ses impacts techniques et opérationnels en entreprise.
- Etudier l'impact psychologique et comportemental des utilisateurs face aux politiques de mots de passe, et l'impact des violations de mots de passe sur les entreprises.
- Élaboration de recommandations pour améliorer la sécurité des mots de passe dans un système d'information.
- Mettre en place une méthodologie d'audit de la qualité des mots de passe dans un SI.
- Proposer un outillage (dictionnaires, etc.) permettant de s'assurer de la qualité des mots de passe dans un SI.

Etudier les principales solutions de gestionnaires de mots de passe :

- Examen des fonctionnalités et de l'impact des gestionnaires de mots de passe sur la sécurité.
- Réaliser un état de l'art et le comparatif des solutions de gestionnaires de mots de passe du marché ;
- Identifier les tendances et ouvertures vers les nouvelles solutions d'authentification sans mots de passe.

Identifier les bonnes pratiques d'usage des mots de passe et les tendances futures :

- Proposer un ensemble de recommandations et de bonnes pratiques concernant l'usage des mots de passe en fonction de cas d'usages.
- Proposer une nouvelle approche de sensibilisation et de formation pédagogique des utilisateurs aux usages des mots de passe.
- Implémenter deux solutions d'authentification par mots de passe dans un environnement de maquette, afin d'évaluer les fonctionnalités, les avantages, les contraintes techniques et opérationnelles, et les comparer.
- Etudier les innovations en matière d'authentification sans mot de passe et leur futur potentiel.

Stage de 6 mois basé à Nantes

Méthode d’audit de la sécurité des développements

Description

Au cours des dix dernières années, les technologies de virtualisation ont considérablement évolué, transformant les infrastructures IT des entreprises. Initialement dominées par les hyperviseurs comme VMware vSphere et Microsoft Hyper-V, la virtualisation a permis de consolider les serveurs physiques, réduisant ainsi les coûts matériels et énergétiques.

La montée en puissance des conteneurs, notamment avec Docker et Kubernetes, a révolutionné la gestion des applications, offrant une portabilité et une efficacité accrues. Parallèlement, le concept de virtualisation de réseau (SDN) et de stockage (SDS) a émergé, permettant une flexibilité et un dimensionnement sans précédent. Les entreprises ont progressivement adopté des solutions de cloud hybride et multi-cloud, combinant ressources sur site et dans le cloud pour une agilité optimale. En outre, l'intégration de technologies comme l'IA et l'automatisation a amélioré la gestion et l'orchestration des environnements virtualisés. Cependant, ces avancées ont aussi posé des défis en matière de sécurité et de gestion de la complexité croissante des infrastructures IT.

Le stage aura pour principaux objectifs de proposer une démarche d’audit des pratiques de sécurisation des environnements virtualisés, 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 infrastructures de virtualisation s’insérant en complément des missions les plus recherchées par les clients de l’agence.

Tes missions

Comprendre les enjeux de sécurisation des infrastructures de virtualisation

- Réaliser un état des lieux des principales solutions de virtualisations utilisées en entreprise
- Comprendre les principales sources de vulnérabilités dans la mise en œuvre de ces solutions
- Définir des recommandations opérationnelles d’implémentation
- 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 infrastructures de virtualisation

- 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 infrastructures de virtualisation

- 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 à la suite de l’audit : modèles de procédures applicables, référentiel d’outils du marché, etc.

Stage de 6 mois basé à Nantes

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

- Assistance à la sécurisation des services externalisés
- Authentification par mot de passe
- Méthode d'audit de la sécurité des développements

CYBER TECHNOLOGY & TRANSFORMATION

Notre équipe Cyber Technology & Transformation 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 Cyber Technology & 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 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

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 !

Notre offre Cyber Technology & Transformation

→ Consultant CIO Advisory

SECURE MANAGED SERVICES & INTEGRATION

L’équipe SMSI 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 MS&C, 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

Service Delivery Manager H/F

Description

Tu intègres l'équipe de production MS&C, 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

IA - Exploration des possibilités des LLM pour l'optimisation des outils MS&C (H/F)

Description

Almond est un acteur français indépendant reconnu dans l'Audit, le Conseil, l'Intégration, et les Services Managés spécifiquement dans les domaines de la Cybersécurité, du Cloud et des Infrastructures.
En intégrant notre équipe MS&C, composée de 60 professionnels passionnés, tu contribueras activement à la concrétisation de services managés diversifiés pour nos clients. Ces services englobent des domaines tels que le Cloud (Azure), l'hébergement sur site, la sécurité, la gestion de réseau et bien d'autres. Notre cœur de métier repose sur de l'administration système et réseau, l'hébergement de sites web, la mise à disposition d'infrastructures hautement disponibles, ...

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

- Développement sur mesure : Création d'outils en Python, 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-4o, Claude 3 et Llama 3, au sein de notre environnement MSC. En tant que partenaire Azure, l'exploitation des services liés à Azure OpenAI et autres offres IA de ce fournisseur cloud sera privilégiée. En 2024, une plateforme avec des premières fonctionnalités a été développée en Python / Flask / ChromaDB en utilisant GPT-4. L'objectif est d'enrichir cette plateforme avec des nouveaux cas d'usage.

Voici comment se déroulera ton immersion :

Phase de découverte du métier / équipe

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

Phase de découverte de l'outils développé en 2024

- S'approprier le projet existant
- Configurer son environnement de développement

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,…)

Évaluation, analyse et mise en place

- Analyser les retours sur des PoC (Proof of Concept), évaluer leur pertinence et la faisabilité (par exemple le coût versus l'apport) 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

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 Managed Services & Integration

- 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