Almond

BOOK DE STAGES 2026

GET READY TO JOIN THE G-TEAM

Almond

Est un groupe français indépendant spécialisé en cybersécurité. Avec 450 experts en France, en Suisse et des centres de services à l'international permettant d'assurer ses opérations en 24/7, Almond anticipe les menaces futures et propose une offre de bout-en-bout pour répondre à toutes les problématiques de ses clients en matière de cyberdéfense : anticipation, protection, détection, réaction, restauration et gouvernance.

DÉCOUVREZ NOS OFFRES DE STAGE 2026

SOC | CERT | CTI CWATCH

OFFENSIVE SECURITY

GOVERNANCE, RISKS & COMPLIANCE

CYBER TECHNOLOGY & TRANSFORMATION

MS&C

INTEGRATION

INNOVATION

LABORATOIRE CESTI

AUDIT & ADVISORY

UN STAGE CHEZ ALMOND

- 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 ou au baby foot !

02.

La rémunération

1500€ à Paris et à Rennes - 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 , events sportifs et plus encore !

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

Vous intégrez 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, vous êtes 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).

Vos missions

- Vous intervenez 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…;
- Vous opérez dans un environnement technique riche : SIEM, EDR, SOAR…;
- Vous êtes impliqué toujours en doublon avec des experts, sur des engagements du CERT en réponse sur incident, recherche de compromission, forensic ou gestion de crise;
- Vous portez 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 et à Lyon

Voir l'offre

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

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

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

ON N'ATTEND PLUS QUE VOUS !

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.

Vos 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 (y compris l'outillage offensif IA).

Stage de 6 mois basé à Sèvres

Voir l'offre

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

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

03. Vous connaissez 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 VOUS !

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.

Etablir un référentiel de traitement des risques Cyber

Description

Nous menons auprès de nos clients des analyses de risques Cyber selon des méthodes maison ou EBIOS Risk Manager et compatibles avec la norme ISO 27005, maîtresse en matière de gestion des risques en sécurité de l'information. En tant que Cabinet de conseil, nous avons le devoir de proposer à la fin de l'exercice d'analyse de risques les meilleures recommandations de sécurité à nos clients pour réduire leurs risques de cybersécurité.
Ces recommandations organisationnelles ou techniques peuvent se matérialiser en jours-hommes internes/externes ou par l'acquisition de solutions du marché.
Nous devons être en mesure de définir des métriques de charge et des coûts moyens d'acquisition et de maintien des produits du marché le plus efficacement possible pour les soumettre à nos clients. Cela éviterait à nos consultants de répéter le travail de collecte de métriques à chaque nouveau client.

L'objectif du stage sera de faire le pont entre Risque, Mesure et Contrôle en proposant une base de connaissance actionnable de:

- Risques Cyber
- Mesures de traitement de ces risques: projets, produits et services sur lesquels Almond a des convictions
- Indicateurs de performance de ces mesures sur les risques et la conformité

Vos missions

Identifier les Risques Cyber :

- A partir du registre des risques Almond et de notre historique d'analyses, sélectionner les risques les plus couramment énoncés dans les analyses de risques

Identifier les Mesures de traitement de risques :

- Proposer un éventail des mesures organisationnelles et techniques suffisamment larges pour adresser toutes les dimensions d'entreprise et tous les budgets
- Faire émerger nos convictions en termes de projets, produits et services en sondant les équipes Almond & se focaliser sur ces convictions
- Spécifier les apports, limites et coûts moyens des mesures proposées
- Proposer des benchmarks le cas échéant
- Identifier les interlocuteurs Almond ou partenaires qui pourraient accompagner nos clients sur la mise en œuvre des recommandations

Identifier des Indicateurs de performance des mesures sur les risques :

- Jauger le niveau d'efficacité de chaque mesure sur le risque auprès des experts et surtout argumenter et prouver ce niveau d'efficacité
- Associer à chaque mesure de sécurité un indicateur de performance sur la conformité à partir d'un socle de référentiels courants (ISO27001, NIS2, DORA, LPM…)

Stage de 6 mois basé à Sèvres

Voir l'offre

IA pour la continuité d'activité : accélérer le BIA et la préparation PCA/PRA

Description

Les équipes Almond ont développé sur les 10 dernières années une très belle bibliothèque d'outils et de pratiques permettant la délivrance des missions d'audit organisationnelles et physiques et de conseil connexes. Ces matériels nous assurent efficacité et efficience sur de nombreux standards (+50 à date), des plus communs (ISO27001, NIST CSF, NIS2, DORA, RGPD, II901…) aux plus rares (NR659, HKMA, AESCSF…), et permettent d'adresser de nombreuses questions de risques (Cyber, sécurité de l'information, sûreté physique) et de conformité (dura lex, sed lex).

Ces derniers mois ont vu l'entrée en vigueur de nombreux textes (acte d'exécution NIS2, RTS et ITS DORA, IA ACT, Data Act) et d'autres sont encore à venir. Cette inflation conjoncturelle concomitant de la montée en maturité des outillages logiciels GRC et de l'IA générative, ainsi que de l'arrivée du CRA (Cyber Resilience Act) nous amènent à investir dans un nouveau cycle d'entretien et d'amélioration continue de nos armes du quotidien.

Votre mission lors de ce stage, sera de définir les fonctionnalités d'un outil visant à automatiser la mise en place et complétude de Business Impact Analysis (BIA) grâce à l'intelligence artificielle existante, puis de le tester sur un environnement restreint. Pour nos équipes, comme pour nos clients, l'objectif sera de gagner du temps de complétude des BIA, faciliter leur analyse et l'identification de moyens palliatifs ou solutions de contournement pour le déploiement du Plan de Continuité d'Activité.

Vos missions

Analyser l'existant

- A partir du registre des risques Almond et de notre historique d'analyses,
- Textes de références : ISO 22301, ISO 27001/02, ISO 42001
- Comprendre les enjeux des PCA / PRA et explorer les apports potentiels de l'IA pour faciliter la mise en place des campagnes de BIA et leur application. L'étude devra s'intéresser dans une moindre mesure au PRA également
- Faire une analyse risque/bénéfice de l'intégration de l'IA dans les programmes de continuité d'activité et plus spécifiquement dans la mise en place de BIA
- Benchmark simplifié : identifier et comparer les solutions PCA/PRA et BIA existantes sur le marché

Concevoir un outil sur la base d'un modèle IA existant

- Identifier les prérequis et le périmètre d'applicabilité de l'outil
- Développer le modèle d'IA qui simplifiera le BIA sur la base d'un modèle IA existant (exemple : dashboard, assistant etc.)

Tester l'outil

- Tester l'outil sur un périmètre restreint interne
- Identifier des capacités d'améliorations, voire d'application étendue au PRA

Stage de 6 mois basé à Sèvres

Voir l'offre

Entretenir & révolutionner l'outillage des équipes audit & conformité

Description

Les équipes Almond ont développé sur les 10 dernières années une très belle bibliothèque d'outils et de pratiques permettant la délivrance des missions d'audit organisationnelles et physiques et de conseil connexes. Ces matériels nous assurent efficacité et efficience sur de nombreux standards (+50 à date), des plus communs (ISO27001, NIST CSF, NIS2, DORA, RGPD, II901…) aux pus rares (NR659, HKMA, AESCSF…), et permettent d'adresser de nombreuses questions de risques (Cyber, sécurité de l'information, sûreté physique) et de conformité (dura lex, sed lex).

Ces derniers mois ont vu l'entrée en vigueur de nombreux textes (acte d'exécution NIS2, RTS et ITS DORA, IA ACT, Data Act) et d'autres sont encore à venir. Cette inflation conjoncturelle et l'interplay en rodage (coexistence et superposition de pratiques), concomitant de la montée en maturité des outillages logiciels GRC et de l'IA générative, ainsi que de l'arrivée du CRA (Cyber Resilience Act) nous amènent à investir dans un nouveau cycle d'entretien et d'amélioration continue de nos armes du quotidien.

Mais cette année, ce n'est pas seulement une évolution qui est attendue, mais une révolution. Réduire au maximum les temps d'intégration de nouveaux standards par l'automatisation, développer simplement des matrices complexes multi référentielles, alléger la charge bureautique de nos consultants, permettre de donner encore plus de valeur et de sens à nos clients sont les enjeux du stage que notre groupe de travail permanent « Support aux conformités » propose.

Vos missions

Comprendre les concepts, le fonctionnement et les enjeux de l'outillage GRC :

- Compréhension du paysage de normes et standards
- Compréhension des mécaniques d'audit et de conseil
- Compréhension du socle d'outillages Almond disponible
- Compréhension des besoins du métier (avec participation à des missions)

Identifier les voies permettant la rénovation / actualisation rapide de l'existant :

- Utiliser les services d'IA génératives internes et externes
- Comprendre leurs limites
- Définir le projet
- Déployer !

Définir la révolution :

- Capitaliser sur l'étape précédente pour définir une méthode de production rapide de nouveaux kits
- L'utiliser sur différents textes (CRA, RTS/ITS DORA, ISO21434, ISO62443, ANSSI INDUS 2025, etc.)
- Accompagner le métier sur la production de toolkits multi référentiels avec la méthodologie définie précédemment

Stage de 6 mois basé à Sèvres

Voir l'offre

Développement d'une boite à outil pour la réalisation d'homologation de sécurité

Description

L'usage d'un système d'information peut entraîner des risques ayant des impacts graves pour une activité. L'homologation d'un système d'information permet, à travers un acte formel, d'attester, à un niveau adéquat de l'organisation, la connaissance des risques pesant sur ce dit système. L'homologation est recommandée depuis de nombreuses années par l'ANSSI et rendue obligatoire par un grand nombre de textes officiels (arrêtés sectoriels de la loi de programmation militaire, par exemple).

Almond accompagne de nombreux clients dans l'homologation de leurs systèmes d'information. Une boite à outil a été développée au fil des années et permet aujourd'hui d'alléger certaines de nos activités.

La parution d'une nouvelle version du guide de l'ANSSI nous amène à devoir transformer certains éléments de cet outillage.

L'objectif de ce stage est de réaliser une mise à niveau de l'outillage existant, en prenant appui sur l'expérience acquise auprès de consultants. Le stagiaire sera impliqué sur des missions liées à cette activité et pourra avoir une première vision du métier de consultant en Gouvernance, Risques et Conformité.

Vos missions

S'approprier le processus d'homologation et l'outillage existant :

- Analyser les écarts entre le nouveau et l'ancien guide d'homologation de l'ANSSI
- Réaliser un panorama des textes et des exigences relatifs à l'homologation de sécurité
- Synthétiser les évolutions liées à l'homologation de sécurité au regard des changements réglementaires et doctrinaux

Identifier les évolutions à réaliser et les mettre en œuvre :

- Analyser la boite à outils existante et identifier les évolutions à réaliser
- Intégrer les évolutions identifiées dans les modèles de documents
- Adapter le générateur de documents, le cas échéant

Identifier les outils existants sur le marché pour faciliter le suivi des homologations :

- Identifier les cas d'usage pouvant nécessité l'usage d'une solution applicative
- Identifier et prioriser les fonctionnalités attendues pour de telles solutions
- Identifier les solutions existantes sur le marché
- Synthétiser les résultats des travaux menés dans un comparatif de solutions

Stage de 6 mois basé à Sèvres

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, PCIDSS, DORA, NIS2, ISO 2700x, HDS, SWIFT, …).

Vous aurez l'occasion de travailler sur notre offre de service « Maintien en condition de sécurité » et aborder également les sujets de l'automatisation notamment les « power » tools (Power Automate, Power BI, Power Excel). En parallèle de ce « fil rouge » vous serez amené à participer à des missions clients pour découvrir le métier du conseil.

Vos missions

La mission consistera plus précisément à mettre en place du contrôle permanent pour notre propre conformité, mais également à construire un framework de contrôles, capable de satisfaire plusieurs normes / lois / standards de sécurité.

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

- Les grands standards de sécurité (ISO 27xxx, PCIDSS, DORA, NIS2, 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 :

- Vous interviendrez 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 vous imprégner à ton futur métier en lien avec la sécurité de l'information et la gestion des risques SSI;
- Vous participerez 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

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.

Vos 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

Sécurisation des infrastructures de virtualisation

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.

Vos 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

Voir l'offre

Etude des mécanismes d'authentification

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.

Vos 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

Voir l'offre

01.

Elève ingénieur ou équivalent BAC + 5, vous bénéficiez de connaissances générales sur les infrastructures IT.

02.

Vous avez la capacité à prendre du recul face à un problème donné (étude-conseil), vous êtes un bon communicant et vous parlez couramment anglais ?

03.

Vous avez un goût pour la cybersécurité et vous êtes désireux de travailler avec des clients et les équipes Almond ?

ON N'ATTEND PLUS QUE VOUS !

Nos offres Governance, Risks & Compliance

- → Etablir un référentiel de traitement des risques Cyber
- → Intelligence artificielle pour la continuité d'activité
- → Entretenir & révolutionner l'outillage des équipes audit & conformité
- → Développement d'une boite à outil pour la réalisation d'homologation de sécurité
- → Maintien en condition de cybersécurité
- → Assistance à la sécurisation des services externalisés
- → Sécurisation des infrastructures de virtualisation
- → Etude des mécanismes d'authentification

CYBER TECHNOLOGY & TRANSFORMATION

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

État de l'art et benchmark des outils de gestion des vulnérabilités / Vulnerability Operations Center

Description

Dans un contexte de digitalisation croissante et de multiplication des cyberattaques, l'analyse des vulnérabilités est devenue une brique fondamentale de toute stratégie cybersécurité.
Aujourd'hui, les menaces cyber évoluent rapidement, avec des campagnes de ransomware de plus en plus ciblées, des groupes APT sophistiqués et une pression réglementaire qui ne cesse de s'accroître.
L'analyse des vulnérabilités est devenue une pratique clé en cybersécurité, permettant d'identifier de manière proactive les faiblesses techniques exploitables par des attaquants. Cette démarche consiste à évaluer en continu les systèmes, applications et réseaux du SI pour détecter les vulnérabilités, les classer par criticité et proposer des mesures correctives.
Ce stage permettra d'explorer en profondeur cette pratique, ses outils, ses méthodologies, ainsi que ses enjeux pour les entreprises, tant sur le plan technique que stratégique.

Les objectifs de ce stage sont :
- Explorer l'état de l'art de l'analyse des vulnérabilités (outils, méthodologies, contexte réglementaire).
- Définir une stratégie opérationnelle pour piloter cette activité dans un SI d'entreprise.
- Établir une grille comparative entre les outils d'analyse des vulnérabilités.

Vos missions

1. Étude du contexte actuel et des enjeux :

- → Analyse des tendances récentes : groupes cybercriminels actifs, techniques d'exploitation utilisées…
- → Étude des principales réglementations et standards (NIS2, DORA, ISO 27001, PCI-DSS) et exigences de conformité en matière de gestion des vulnérabilités ;
- → Rôle de l'analyse des vulnérabilités dans une démarche de cybersécurité globale ;

2. État de l'art des outils d'analyse de vulnérabilités :

- → Benchmark des principaux outils du marché (Scanner en Standalone, plateforme centralisée de gestion des vulnérabilités) ;
- → Classification par typologie (réseau, web, code, base de données…) ;
- → Élaboration d'une grille d'évaluation technique et fonctionnelle pour comparaison structurée ;

3. Définition d'une stratégie opérationnelle de gestion des vulnérabilités (Vulnerability Operations Center – VOC) :

- → Délimitation et cartographie des périmètres à surveiller : identification des composants du SI à inclure dans la stratégie VOC incluant : SI interne (serveurs, postes utilisateurs, AD), applications web, infrastructures cloud… ;
- → Définition de la méthodologie de gestion des vulnérabilités :
  - Découverte des actifs via une CMDB ou par scans ;
  - Planification des campagnes de scans : fréquence, typologie ;
  - Déploiement et positionnement des sondes : scanners locaux, agents sur endpoints, scanners cloud pour les environnements hybrides;
- → Développement d'un modèle de reporting décisionnel :
  - Construction de tableaux de bord exploitables par les équipes métiers et sécurité présentant des KPIs pertinents ;
  - Définition d'une logique de priorisation des alertes ;
  - Organisation du cycle de remédiation : détection, escalade et suivi des actions ;
- → Mise en place d'une veille proactive :
  - Sélection de sources fiables et mise en place d'outils de surveillance (flux RSS, alerting, agrégateurs de vulnérabilités) ;
  - Intégration des flux de veille dans les processus d'analyse et de priorisation ;

4. Analyse des limites et recommandations d'implémentation :

- → Identification des freins à la mise en œuvre : Coûts (Capex vs Opex), complexité technique (découverte des assets, intégration dans les workflows existants), qualité des résultats… ;
- → Propositions de scénarios de déploiement adaptés aux différents contextes (PME, grand compte, cloud- native...)

Stage de 6 mois basé à Sèvres

Voir l'offre

Infrastructures SI et Cryptographie Post Quantique (PQC)

Description

La cryptographie post-quantique (PQC) n'est plus une perspective lointaine : les algorithmes sont désormais standardisés et intégrés dans certaines solutions, avec pour objectif de résister aux futures capacités de calcul quantique. L'un des principaux risques actuels est celui des attaques Store Now, Decrypt Later (SNDL), où des données interceptées aujourd'hui pourraient être déchiffrées demain. Pourtant, la majorité des organisations restent peu sensibilisées à ce sujet, et ne disposent pas toujours d'une cartographie claire de leurs mécanismes cryptographiques actuels.

Migrer vers la PQC aura un impact majeur sur l'ensemble du SI : réseaux, systèmes, virtualisation, accès distants, navigation Internet, API, authentification, signature, chiffrement des données at rest, in motion et in use.
Ce stage propose d'explorer les enjeux de la PQC, d'expérimenter ses implémentations concrètes et de définir une trame de migration pour accompagner les organisations dans cette transition.

Vos missions

1. Comprendre et analyser

- → Assimiler les concepts fondamentaux de la PQC et des mécanismes cryptographiques dans un SI.
- → Identifier les fonctions, flux, protocoles et usages de la cryptographie (at rest, in motion, in use).
- → Étudier les travaux en cours (cadre théorique, algorithmes NIST, implémentations dans les protocoles).
- → Proposer une vision d'un SI « PQC-ready ».

2. Expérimentation technique

- → Définir un cahier de tests pour documenter l'intégration et les impacts de la PQC.
- → Concevoir une maquette représentative d'un SI pour tester différents cas d'usage.
- → Expérimenter l'implémentation de la PQC dans les protocoles et mécanismes du SI.
- → Évaluer la maturité technique et opérationnelle des solutions actuelles.

3. Recommandations et plan de migration

- → Rédiger un plan de migration PQC standard adaptable aux organisations.
- → Formuler des recommandations et bonnes pratiques spécifiques (SSO, MFA, gestion des certificats, etc.).Implémenter et comparer deux solutions SSO/MFA du marché dans un environnement de test (fonctionnalités, avantages, contraintes).

Stage de 6 mois basé à Sèvres

Voir l'offre

Etat de l'art des solutions Enterprise Browser

Description

L'usage des accès aux SI des organisations **évolue** fortement pour une bonne partie des cas d'usage. Ce sont principalement les accès à **privilèges** qui se voient modifiés, autant pour des populations d'utilisateurs internes (les administrateurs), que pour des utilisateurs externes à l'organisation (des prestataires ponctuels ou récurrents). Ces usages à distance sont par ailleurs devenus courant suite à la situation Covid qui a pris fin en 2022, et la **mobilité induite**.

Enfin, l'évolution des technologies et surtout des standards de sécurité se fait rapidement : les solutions ZTNA, en cours de remplacement des solutions VPN classiques, convergent vers un mode de déploiement **simplifié sans agent**, uniquement depuis le navigateur ; la navigation à travers Internet évolue aussi vers le déploiement de **TLS 1.3** et potentiellement d'une norme qui pourrait réduire l'efficacité de certains outils d'inspection des flux (ECH).
Et enfin, nous constatons le déclin des solutions classiques de virtualisation des accès au travers de machines virtuelles complètes (VDI), trop lourdes à mettre en place et maintenir.

Avec ces éléments de contexte, une technologie émerge depuis quelques années : les solutions de **virtualisation applicative d'un simple navigateur**, le RBI, et à présent ce qu'on nomme les solutions **d'Enterprise Browser** (ou nextgen-RBI).

Almond, société de conseil, experte en sécurité des systèmes d'information, souhaite étudier ce sujet **nouveau**, les solutions actuelles proposant ces fonctionnalités, les enjeux auxquels ces techniques répondent, et comment elles s'implémentent réellement au sein d'un SI.

Vos missions

1. Etat de l'art des solutions d'Enterprise Browser

- → Etudier les enjeux et les problématiques associés aux cas d'usage de ces solutions de sécurité,
- → Etudier les offres commerciales des éditeurs du marché,
- → Comparer les fonctionnalités techniques et les approches des solutions proposées,
- → Identifier les nouvelles tendances ou fonctionnalités émergentes prometteuses.

2. Etude fonctionnelle et technique de 3 solutions d'Enterprise Browser

- → Choisir et comparer fonctionnellement 3 solutions du marché,
- → Proposer une démarche d'étude technique pour ces 3 solutions qui soit la plus complète possible,
- → Construire un cahier de tests permettant d'évaluer l'ensemble des fonctionnalités des solutions,
- → Mettre en œuvre les solutions dans un environnement de maquette, et comparer les résultats.

Stage de 6 mois basé à Sèvres

Voir l'offre

Assurer le succès du déploiement d'une roadmap cyber

Description

Au sein de l'équipe Cyber Technology & Transformation d'Almond, un de nos défis quotidien consiste à assurer le succès du déploiement des roadmap Cyber de nos clients. Cette étape clé nécessite une planification et une exécution rigoureuses pour garantir la tenue des objectifs et renforcer notamment la résilience de nos clients.

L'objectif est de leur fournir une méthodologie éprouvée pour améliorer la sécurité de leurs systèmes et protéger leurs données sensibles. Cette approche personnalisée leur permettra de renforcer leur posture de sécurité, d'identifier et de gérer les risques, et de mettre en place des mesures de sécurité efficaces.

Ce stage vise à compléter et renforcer nos pratiques et outillage à destination de, nos clients, afin qu'ils puissent bénéficier d'une approche structurée.

Vos missions

Au cours de ton stage vous pourrez travailler sur les types de missions suivantes :

- → Capitaliser sur les missions emblématiques de l'équipe pour prendre en main le sujet, identifier les points forts et les difficultés rencontrées.
- → Réaliser une étude de marché sur les solutions de gestion de projet, mettre en évidence les meilleures pratiques et identifier les outils les plus pertinents.
- → Proposer une matrice d'aide au choix sur les méthodologies à mettre en place pour chaque type de projet, adaptée aux besoins et objectifs.
- → Élaborer des mécanismes de révision et de mise à jour pour garantir la pertinence et l'efficacité de la roadmap Cyber et des budgets associés.
- → Participer à la veille sectorielle et à la capitalisation des connaissances, permettant ainsi de rester à la pointe des dernières tendances et technologies.
- → Créer du contenu pertinent, tel qu'un article ou une présentation, pour partager vos conclusions et votre expertise avec l'équipe.
- → Bénéficier d'un accompagnement personnalisé et d'un soutien continu de la part de votre manager et des collègues experts, adapté à votre niveau de maturité et à vos besoins.

Ce stage offre une occasion unique de développer vos compétences, d'acquérir de nouvelles connaissances et d'apporter une contribution significative à l'équipe.

Stage de 6 mois basé à Sèvres

Voir l'offre

01. Elève ingénieur (H/F) ou équivalent Bac+5 avec une spécialisation réseaux, systèmes ou sécurité, vous bénéficiez de connaissances générales sur les infrastructures IT et la sécurité.

02. Vous avez la capacité à prendre du recul face à un problème donné (étude-conseil) Vous êtes un bon communicant et vous parle couramment anglais ?

03. Vous avez un bon relationnel, êtes dynamique, motivé(e) et avez un goût pour la mise en pratique technique ?

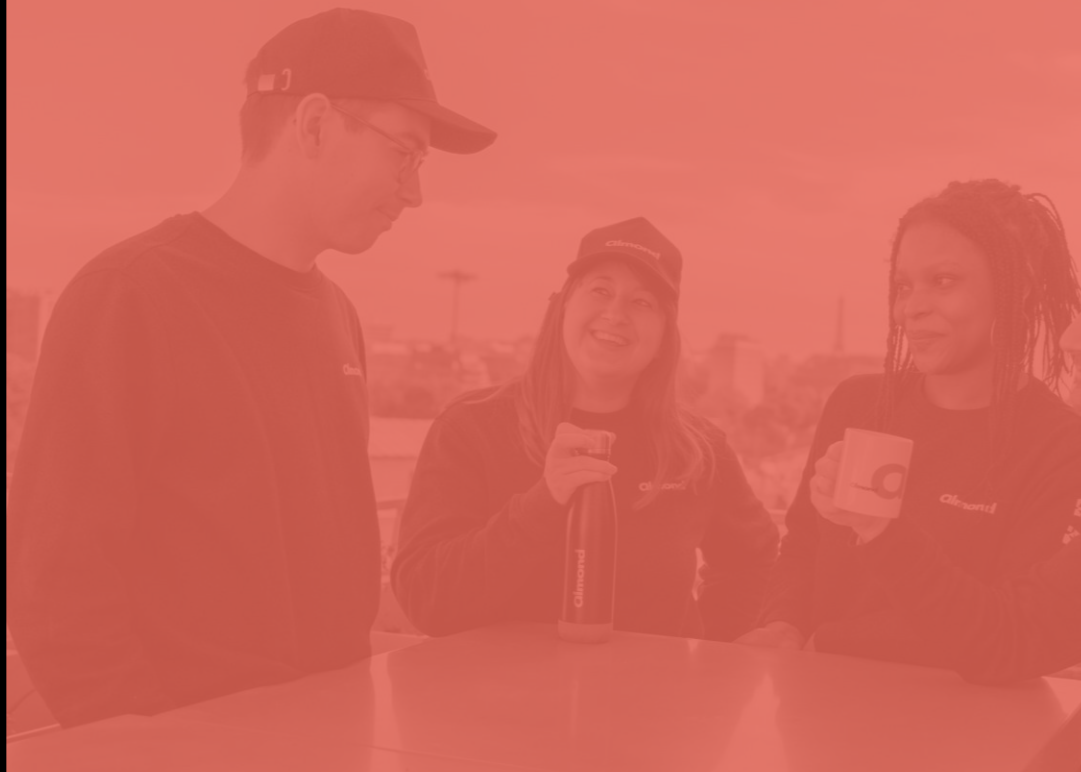
ON N'ATTEND PLUS QUE VOUS!

Notre offres Cyber Technology & Transformation

- → Etat de l'art et benchmark des outils de gestion des vulnérabilités / VOC
- → Infrastructures SI et Cryptographie Post Quantique
- → Etat de l'art des solutions Entreprises Browser
- → Assurer le succès du déploiement d'une roadmap cyber

MANAGED SERVICES & CLOUD

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



Chef de Projet 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.
Vous contribuerez à la réalisation de projets diversifiés dans les domaines de la sécurité, de la gestion de réseau, des infrastructures, du Cloud et de l'hébergement sur site.

Vos missions

Le Chef de Projets est responsable de la planification, du pilotage et du suivi de projets depuis la phase de cadrage jusqu'à la livraison finale, en garantissant le respect des délais, du budget et de la qualité.
Il s'assure de la qualité, du respect des délais et de la satisfaction client, tout en identifiant les opportunités de développement commercial pour faire grandir la relation et le business.

L'objectif principal de ce stage sera de suivre des projets structurants pour la société en adaptant la méthodologie adaptée au projet.
Voici comment se déroulera votre immersion :

Assurer la réussite des projets confiés

- Respecter les délais, les budgets et les périmètres définis.
- Atteindre les objectifs de performance fixés par l'entreprise et/ou le client.
- Mettre en place et suivre les processus de gestion de projets (méthodologies agiles, ITIL, etc.)
- Animer les comités de pilotage 'Projet'

Piloter la coordination et la communication

- Assurer une communication claire et régulière auprès des intervenants projet (reporting, comités de pilotage, documentation).

Optimiser l'utilisation des ressources

- Gérer & suivre les budgets et la rentabilité des projets
- Booker les profils techniques mis à disposition par les équipes opérationnelles.

Contribuer à la satisfaction du client et des utilisateurs

- Maintenir un haut niveau de satisfaction et de confiance avec les parties prenantes
- Être garant(e) de l'expérience finale des clients Almond.
- Assurer les reporting réguliers et les envoyer aux clients Almond

Participer à l'amélioration continue de la gestion de projets

- Capitaliser sur les retours d'expérience (REX).
- Contribuer à l'évolution des méthodes et outils de gestion de projet au sein de l'entreprise.
- Valider que les coûts estimés en AVV sont cohérents avec ceux nécessaires dans le cadre du projet

Stage de 6 mois basé à Sèvres

Voir l'offre

Service Delivery Manager H/F

Description

Vous intégrerez 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.

Vos missions

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

- Être garant(e) 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 vos expériences et 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.

Vos objectifs :

- Apporter vos compétences relationnelles et votre expertise ;
- Être présent(e) 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

01.

Vous êtes élève Ingénieur ou équivalent Bac +5 avec une spécialisation dans le réseau, système ou cloud computing ?

02.

Vous avez de bonnes capacités de communication et parlez couramment anglais ?

03.

Vous disposez de bonnes capacités relationnelles, être dynamique et motivé(e) ?

ON N'ATTEND PLUS QUE VOUS !

Nos offres Secure Managed Services & Integration

- Chef de projet
- Service Delivery Manager

INTEGRATION

L’équipe Intégration joue un rôle clé dans la mise en œuvre des solutions réseau et sécurité au sein des infrastructures clients. Elle se distingue par sa capacité à vendre et conduire des projets complexes alliant performance et fiabilité, tout en veillant à la satisfaction des besoins spécifiques de chaque client.

Ses missions principales consistent à intégrer des briques de sécurité - pare-feux, systèmes de détection d’intrusion, solutions VPN, etc. - dans des environnements variés et parfois critiques.

En parallèle, l’équipe s’attache à concevoir et construire des infrastructures réseau et sécurité.

Étude des solutions de sécurisation IA

Description

L’adoption rapide des LLM et services d’IA (SaaS, API, plugins) transforme les usages métiers, tout en exposant les organisations à des risques spécifiques: exfiltration de données via prompts, fuites de secrets, shadow AI, hallucinations/toxicité, dérives de modèles, et non conformités réglementaires.

Les plateformes SSE/SASE, CASB/DLP et API Security introduisent des capacités de protection dédiées: visibilité des usages IA, contrôle d’accès contextuel, DLP sémantique, guardrails/filtrage de prompts, masquage/rédaction dynamique, etc. Les politiques deviennent granulaires (par application IA, utilisateur, type de données) et s’étendent au navigateur et aux API.

Nos partenaires technologiques (Check Point, Palo Alto Networks, Zscaler, etc.) enrichissent leurs offres pour sécuriser les interactions avec l’IA : découverte des usages, prévention de fuite, sécurisation des prompts/réponses, conformité, et protection des connecteurs.
Almond, souhaite étudier ce sujet pour évaluer la maturité des solutions, mesurer leur couverture de risques IA et définir des trajectoires d’intégration opérationnelles dans les SI clients.

Vos missions

1. Analyse du marché
- Qualifier les offres partenaires (Check Point, Palo Alto Networks, Zscaler…) et d’acteurs pure player.
- Comparer les approches techniques (agent/proxy/navigateur/API),
- Identifier les tendances: guardrails LLM, content safety avancée, politiques adaptatives, audit.

2. Étude technique et évaluation
- Sélectionner un ensemble de solutions partenaires et définir des scénarios de risques.
- Construire un cahier de tests: critères
- Déployer en maquette les solutions
- Exécuter les tests et produire un rapport comparatif: couverture des risques, efficacité, impacts UX/perf, effort d’intégration, TCO, conformité.

En complément de l’étude de solutions, vous participerez à des missions d’intégration avec un ingénieur senior.
Livrables: cartographie risques/contrôles par solution; cahier de tests ; lab reproductible; rapport comparatif (scoring, recommandations d’intégration); supports de restitution et guide d’intégration pour Almond.

Stage de 6 mois basé à Sèvres

Voir l’offre

01. Vous êtes élève Ingénieur ou équivalent Bac +5 avec une spécialisation dans le réseau, système ou cloud computing ?

02. Vous avez de bonnes capacités de communication et parlez couramment anglais ?

03. Vous disposez de bonnes capacités relationnelles, être dynamique et motivé(e) ?

ON N'ATTEND PLUS QUE VOUS !

Notre offre INTEGRATION

Étude des solutions de sécurisation IA

INNOVATION

L'équipe Innovation conçoit, développe et déploie des solutions sur mesure pour soutenir les équipes internes d'Almond.

Elle se distingue par son approche innovante, tant dans les méthodes adoptées que dans les technologies utilisées au cœur de ses solutions, comme les LLM, les bases vectorielles et les plateformes d'automatisation.

Ingénieur(e) en automatisation & intelligence artificielle

Description

Au sein de notre équipe Innovation, tu travailleras au croisement des métiers techniques (SOC, CERT, CTI, infogérance, intégration, conseils...) et des enjeux stratégiques.

Ton objectif : concevoir et expérimenter des solutions concrètes à base d'automatisation, d'intelligence artificielle ou de traitement de données pour booster notre performance et la qualité des services rendus.

Tu auras à disposition une palette d'outils moderne (orchestrateur, plateforme multimodale, CI/CD, agents IA, plateformes no-code/low-code, etc.) et un terrain de jeu varié : automatisation de use-cases SOC, chatbot et assistants internes, génération de rapports automatiques, création de règles de détection, dashboards IA…

Vos missions

- Identifier, concevoir et développer des *workflows d'automatisation* à fort ROI pour les équipes internes (SOC, CERT, CTI, audit, infogérance, compliance…)

- Créer et tester des *agents IA* (GPT, Dust, etc.) pour automatiser l'analyse, la rédaction ou l'assistance technique.

- Industrialiser des *prototypes no-code/low-code* jusqu'à leur passage en production

- Contribuer à la *veille technologique* sur les usages IA / automation dans le secteur cyber

- Collaborer avec des experts métier pour cadrer les besoins, tester des idées, et mesurer l'impact des solutions proposées

Stage de 6 mois basé à Sèvres et à Lyon

Voir l'offre

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

02. Vous avez l'envie de créer et développer de nouveaux concepts utiles à l'écosystème cyber et vous avez des compétences pour le faire !

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

ON N'ATTEND PLUS QUE VOUS !

Notre offre INNOVATION

Ingénieur(e) en automatisation & intelligence artificielle

SECURITY EVALUATION & ANALYSIS LAB (CESTI)

Les membres du SEAL *(Security Evaluation & Analysis Lab)* évaluent le niveau de sécurité de produits logiciels au travers d'une approche offensive, dans le cadre des activités d'analyse logicielle ou des activités du laboratoire CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) d'AMOSSYS.

Ces analyses peuvent porter sur des composants de l'informatique standard (solution EDR, pare-feu, système de messagerie sécurisée, bibliothèque cryptographique, etc.) comme des produits plus spécialisés (système de contrôle d'accès, équipement industriel, etc.).

Exploitation des mécanismes IPC Windows

Description

Au travers des activités de son CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information, agréé par l'ANSSI), AMOSSYS est amené à évaluer et analyser la sécurité de nombreux produits logiciels, notamment sur plateforme Windows. Le principal axe d'analyse consiste à rechercher d'éventuelles vulnérabilités pouvant toucher ces produits.

Pour orienter leurs recherches de vulnérabilités, les Analystes et Évaluateurs procèdent au préalable à une étude de la surface d'attaque du produit, à la cartographie des briques logicielles ainsi qu'à l'identification fine des communications entre ces processus. Ces *Inter-Process Communications* peuvent être de plusieurs types et servir à partager des informations ou faire exécuter des actions par d'autres processus, devenant ainsi des cibles privilégiées pour la recherche de vulnérabilités.
Afin de faciliter et accélérer les analyses de ce type de mécanismes, tout en maximisant la qualité de la recherche de vulnérabilités, AMOSSYS a mis en place plusieurs bases de connaissances et méthodologies internes sur le sujet.

Le stage proposé permettra de poursuivre le développement de ces connaissances tout en les enrichissant d'outils et scripts visant à automatiser l'analyse et l'identification de vulnérabilités sur ces mécanismes d'IPC.

Vos missions

Le stage s'organisera de la manière suivante :

- Phase 1 : état de l'art des mécanismes IPC Windows et de leur sécurité ;
- Phase 2 : mise à jour des méthodologies et connaissances internes ;
- Phase 3 : développement d'outils dédiés à l'analyse de sécurité et de robustesse de ces mécanismes, recette sur des situations de test représentatives, documentation du fonctionnement et de l'utilisation.

A noter que vous serez amené(e) à partager l'avancée de vos travaux avec l'équipe en participant à des ateliers de présentation et en produisant des contenus et/ou livrables écrits.

Les vulnérabilités identifiées au cours du stage sur des produits open-source ou publics pourront être remontées aux éditeurs concernés pour participer à leur correction.

Stage de 6 mois basé à Rennes

Voir l'offre

Vulnérabilités des mécanismes de virtualisation

Description

Au travers des activités de son CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information, agréé par l'ANSSI), AMOSSYS est amené à évaluer et analyser la sécurité de nombreux produits logiciels. Le principal axe d'analyse consiste à rechercher d'éventuelles vulnérabilités pouvant toucher ces produits.

De plus en plus les produits logiciels se basent sur de la containerisation pour améliorer leur niveau de sécurité, ou basent leur sécurité sur une intégration en profondeur de mécanismes de virtualisation ou d'hyperviseurs. Pour faciliter l'analyse de la sécurité de ces produits et de ces mécanismes, AMOSSYS a mis en place plusieurs bases de connaissances et méthodologies internes sur le sujet.

Le stage proposé permettra de poursuivre le développement de ces connaissances tout en les enrichissant d'outils et scripts visant à automatiser l'analyse et l'identification de vulnérabilités sur les hyperviseurs et mécanismes de virtualisation. Sans s'attacher à la sécurité de la configuration des solutions de containerisation (type Docker et Kubernetes), le stage se concentrera sur les mécanismes de sécurité intrinsèques des hyperviseurs ainsi que les moyens de les contourner.

Vos missions

Le stage s'organisera de la manière suivante :

- Phase 1 : état de l'art des mécanismes IPC Windows et de leur sécurité ;
- Phase 2 : mise à jour des méthodologies et connaissances internes ;
- Phase 3 : développement d'outils dédiés à l'analyse de sécurité et de robustesse de ces mécanismes, recette sur des situations de test représentatives, documentation du fonctionnement et de l'utilisation.

A noter que vous serez amené(e) à partager l'avancée de vos travaux avec l'équipe en participant à des ateliers de présentation et en produisant des contenus et/ou livrables écrits.

Les vulnérabilités identifiées au cours du stage sur des produits open-source ou publics pourront être remontées aux éditeurs concernés pour participer à leur correction.

Stage de 6 mois basé à Rennes

Voir l'offre

01. Vous êtes élève Ingénieur ou équivalent Bac +5 dans le domaine de la sécurité informatique

02. Vous détenez des compétences en sécurité et mécanismes internes des systèmes Windows et/ou Linux ainsi qu'en développement d'outils logiciels et de scripts

03. Vous aimez travailler en équipe ? Vous êtes rigoureux(se) et possédez de bonnes capacités de synthèse ?

ON N'ATTEND PLUS QUE VOUS !

Notre offre SEAL

Exploitation des mécanismes IPC Windows

Vulnérabilités des mécanismes de virtualisation

AUDIT & ADVISORY

Les collaborateurs du pôle Audit & Advisory interviennent sur des missions variées aussi bien sur des aspects organisationnels que techniques. Ses missions d'audit consistent notamment à identifier des vulnérabilités au sein d'applications ou de systèmes d'information afin de proposer des recommandations de sécurité adaptées à chaque contexte.

Contournement d'EDR

Description

Les collaborateurs du Pôle Audit et Conseil de Rennes interviennent sur des missions variées aussi bien sur des aspects organisationnels que techniques.

Ces missions d'audit consistent notamment à identifier des vulnérabilités au sein d'applications ou de systèmes d'information afin de proposer des recommandations de sécurité adaptées à chaque contexte.

Vos missions

Le stage s'organisera de la manière suivante :

- Recherche et développement sur le contournement (bypass) d'EDR :
- Faire un état de l'art des techniques de contournement existantes ;
- Tester certaines techniques (POC) ;
- Développer un outil implémentant plusieurs techniques de contournement d'EDR et pouvant être utilisé lors de tests d'intrusion ou Red Team sur différents systèmes d'information ;
- Rechercher de nouvelles techniques de contournement d'EDR ;
- Présenter ses travaux au reste de l'équipe d'audit ;
- Alimenter la détection du SOC Almond en échangeant sur les techniques étudiées.

- Découvrir le métier d'Auditeur en assistant à quelques missions d'audit.

Stage de 6 mois basé à Rennes

Voir l'offre

Rédaction de rapport d'audit assistée par IA

Description

Les membres du Pôle Audit & Advisory de Rennes interviennent sur des missions variées aussi bien sur des aspects organisationnels que techniques. Ces missions d'audit consistent notamment à identifier des vulnérabilités au sein d'applications ou de systèmes d'information afin de proposer des recommandations de sécurité adaptées à chaque contexte.

Actuellement, le pôle audit dispose d'une base de connaissances comprenant des blocs de vulnérabilités et de recommandations prérédigées. Celle-ci pourrait être améliorée en utilisant l'intelligence artificielle (rédaction de nouveaux blocs, traduction, harmonisation des styles, détection des fautes d'orthographe, etc.).

Vos missions

Le stage s'organisera de la manière suivante :

- Recherche et développement sur la rédaction de rapport d'audit assistée par IA :
- Faire un état de l'art de l'existant, pointer les forces et les faiblesses ;
- Tester certains modèles avec la base documentaire (POC) ;
- Explorer les possibilités d'intégration dans l'outillage existant ;
- Développer des agents permettant de manipuler la base de connaissances du pôle audit ;
- Présenter ses travaux au reste de l'équipe d'audit.

- Découvrir le métier d'Auditeur en assistant à des missions d'audit, principalement des tests d'intrusion Web.

Stage de 6 mois basé à Rennes

Voir l'offre

01. Vous êtes élève Ingénieur ou équivalent Bac +5 dans le domaine de la sécurité informatique

02. Vous détenez des compétences dans les domaines suivants : systèmes et réseaux ; programmation et scripting ; sécurité informatique.

03. Vous aimez travailler en équipe et détenez de bonnes capacités de communication. Rigoureux(se), vous êtes force de proposition.

ON N'ATTEND PLUS QUE VOUS !

Notre offre Audit & Advisory

Contournement d'EDR

Rédaction de rapport d'audit assistée par IA

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