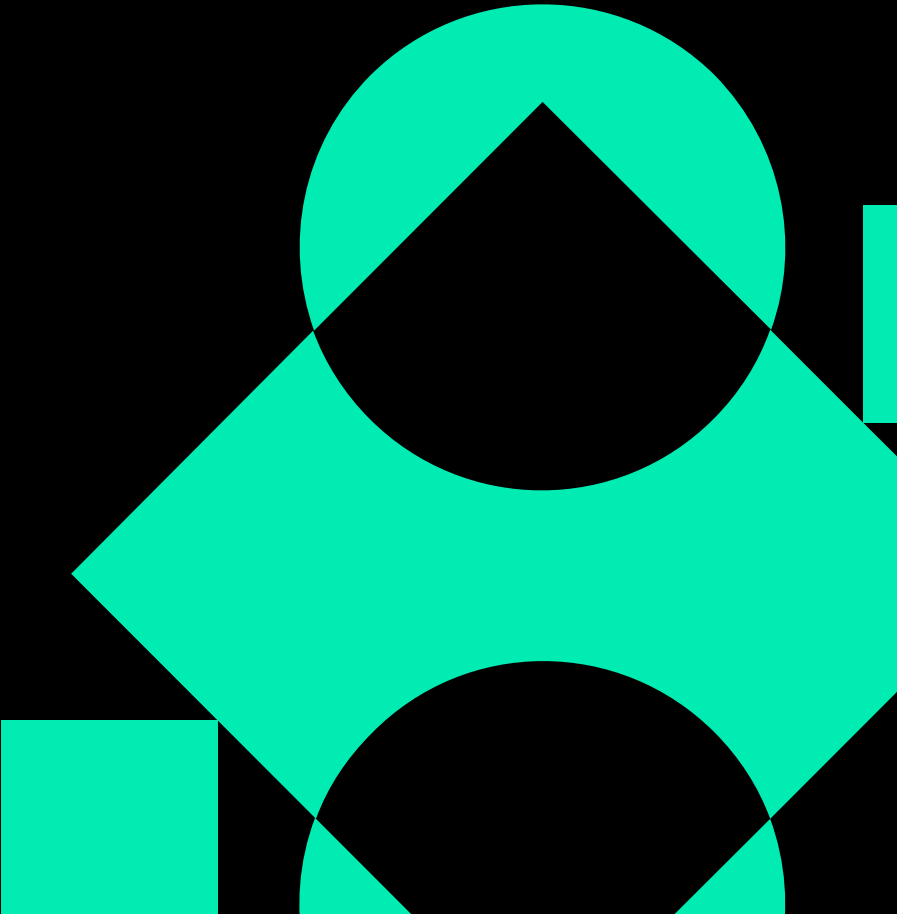


BOOK DE STAGES 2027

Almond

RESILIENCE OPERATIONS CENTER



Analyste CERT H/F

Stage de 6 mois basé à Sèvres

Description

Nous sommes à la recherche d'un stagiaire de fin d'étude pour faire partie de notre équipe CERT. Intégrer nos équipes, c'est rejoindre un collectif passionné, bénéficier d'un environnement stimulant proposant des opportunités de formation et d'évolution au sein du groupe.

Vos missions

- Répondez aux incidents et aidez aux phases de confinement et d'éradication de la menace.
- Effectuez des acquisitions et des analyses Forensics sur de nombreux systèmes d'exploitation (Windows/Linux/Mac/Mobile), des équipements réseaux et sur des applications (sécurité/web/ métier/...).
- Préservez, collectez, analysez les données et preuves dans le respect des normes d'expertise numérique (menaces internes, de fraude et de litiges).
- Etablissez une vue d'ensemble de la compromission et donnez les éléments factuels de l'incident sous forme de chronologie fiable dans un rapport.
- Identifiez un plan d'actions pertinentes et élaborer les stratégies de confinement et d'éradication.
- Accompagnez le client dans la gestion de la crise de bout-en-bout et communiquez avec lui au fil de l'eau.
- Assurez la liaison et la coordination avec d'autres équipes opérationnelles/enquêtrices/techniques pour aider et fournir et/ou recueillir des informations.
- Évaluez et résolvez une variété de problèmes techniques dans un cadre où les personnes peuvent avoir des intentions potentiellement malveillantes ou criminelles présumées.
- Maintenez à jour le Laboratoire Forensics et testez de nouveaux outils.
- Développez et contribuez aux nouvelles initiatives qui améliorent nos capacités de réponse, enrichissent notre boîte à outils et accélèrent nos délais de remédiation.
- Intervenez en support lorsque le SOC escalade un incident.
- Echangez avec les membres de la communauté et vous partagez vos informations de veille, vos IOC quand c'est possible (TLP) et vos sources.
- Respectez la réglementation en matière de respect de la vie privée.

Analyste SOC | CERT H/F

Stage de 6 mois basé à Sèvres

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 impliqués 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.

Ingénieur Réseaux & Systèmes H/F

Stage de 6 mois basé à Sèvres

Description

Vous intégrez l'équipe de production IT Operations, 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 sécurité, 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 notre plateforme cloud privé ou encore sur du cloud Public (Azure ou AWS). Dans le cadre de la croissance de notre équipe de production, ce stage de 6 mois est pensé comme une première étape au sein de l'équipe de production. Si la collaboration fonctionne bien des deux côtés, nous souhaitons vous proposer de poursuivre l'aventure en CDI à l'issue du stage. La suite envisagée : deux années en VIE à Séoul, avant de revenir dans l'équipe en France. C'est donc une opportunité de construire un parcours sur la durée, entre expertise technique, environnements de production exigeants et expérience multiculturelle !

Vos missions

Vous serez encadré par un ingénieur expérimenté et toute l'équipe sera là pour vous aider à monter en compétences sur les tâches 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 firewalls);
- Aider au bon fonctionnement des plateformes de nos clients;
- Rédiger la documentation technique;
- Participer à l'optimisation de nos systèmes de production.

Votre environnement : Désolé pour cette (longue) liste, mais nous n'avons pas trouvé mieux pour vous montrer l'étendue du scope technique sur lequel vous travaillerez !

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

Chef de Projet H/F

Stage de 6 mois basé à Sèvres

Description

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)
- 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

Service Delivery Manager H/F

Stage de 6 mois basé à Sèvres

Description

Vous intégrez l'équipe de production ITOps, 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

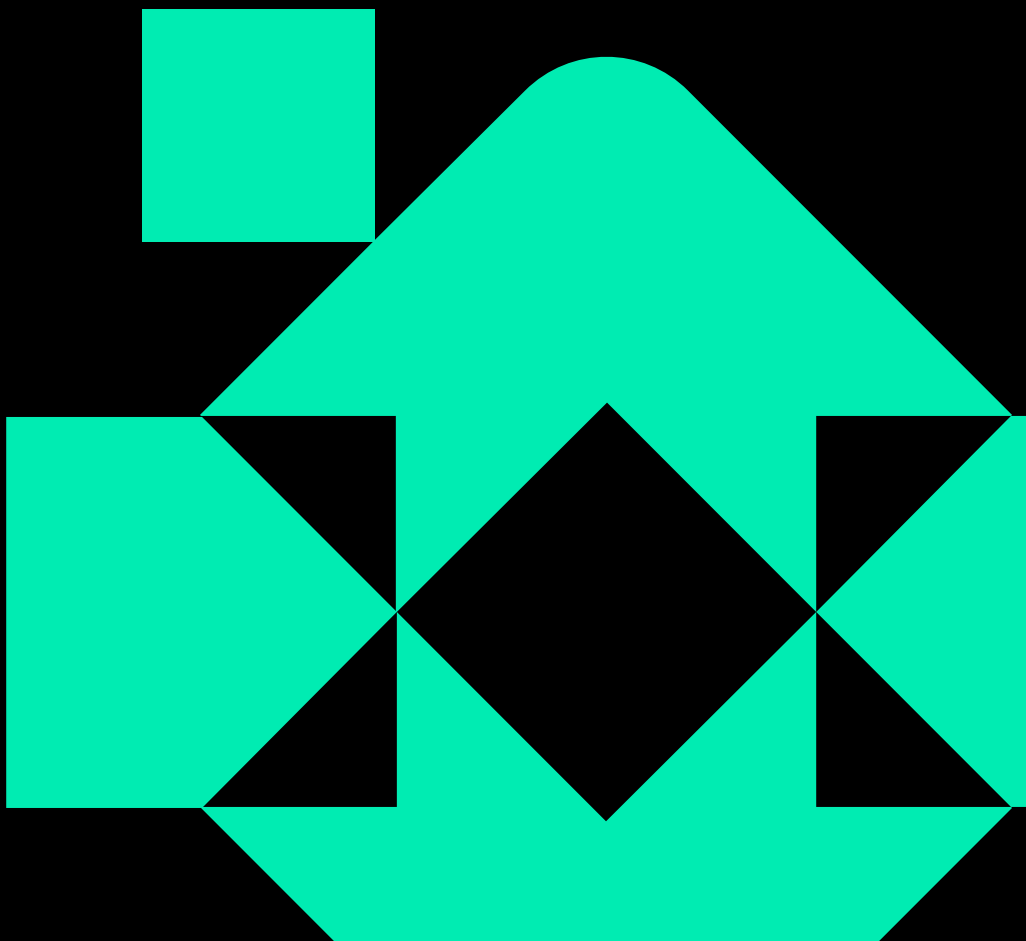
Désormais Service Delivery Manager, vous serez l'interlocuteur privilégié auprès de plusieurs de nos clients Almond pour :

- 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

PLATFORM & AUTOMATION



Ingénieur(e) en automatisation & intelligence artificielle H/F

Stage de 6 mois basé à Sèvres et à Lyon

Description

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

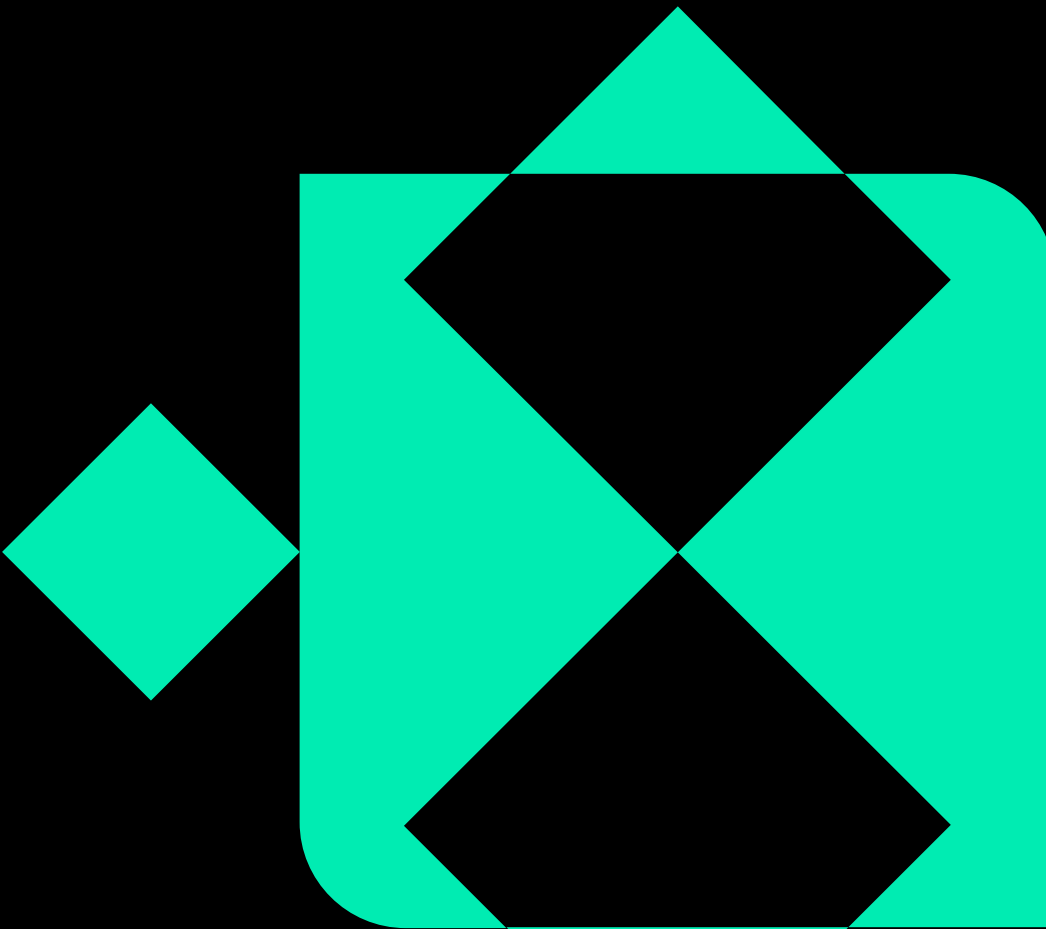
Votre objectif : concevoir et expérimenter des solutions concrètes à base d'automatisation, d'intelligence artificielle ou de traitement de données pour booster notre performance et la qualité des services rendus.

Vous aurez 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.

GOVERNANCE, RISKS & COMPLIANCE



Maintien en condition de Cybersécurité H/F

Stage de 6 mois basé à Lyon

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 t'imprégner de votre 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.).

Gouvernance de la sécurité de l'IA : intégrer l'IA dans les boîtes à outils GRC

Stage de 6 mois basé à Sèvres

Description

Les systèmes d'IA déplacent les repères de la sécurité de l'information. Aux critères classiques de disponibilité, intégrité, confidentialité et traçabilité s'ajoutent des préoccupations propres aux modèles : biais, robustesse, intelligibilité, dérive et encadrement humain. Ce n'est pas une rupture mais une accélération : la réglementation évolue lentement, l'environnement technique très vite, et c'est l'écart entre les deux que la gouvernance du client doit refermer pour ne pas s'exposer à une trop grande surface de risques.

Almond a construit une offre « Gouvernance de la sécurité des systèmes d'IA » structurée en trois temps, cadre, évaluation et accompagnement, adossée à un référentiel unifié couvrant sept référentiels. Les premières missions menées fin 2026 ont validé l'approche et fourni un matériau important à capitaliser. L'objectif de ce stage est de faire descendre cette offre dans l'outillage quotidien des équipes GRC : traiter le syncrétisme entre ISO 27001 et ISO 42001, formaliser le mariage des deux grilles de lecture, enrichir les boîtes à outils existantes et matérialiser un toolkit « roadmap gouvernance de la sécurité de l'IA » utilisable dès le cadrage d'une mission.

Vos missions

S'approprier les nouveaux paradigmes de la sécurité de l'information :

- Analyser le syncrétisme ISO 27001 / ISO 42001 : exigences communes, points de divergence, réutilisation d'un SMSI existant pour porter un système de management de l'IA;
- Formaliser le mariage des critères DICT et des critères propres à l'IA (biais, robustesse, intelligibilité, dérive, encadrement humain);
- Étudier l'articulation entre la contrainte technique qui entoure un agent et ce que la gouvernance exige et mesure;
- Suivre l'actualité normative et réglementaire (AI Act, ISO 42001, NIST AI RMF) et en tirer des notes d'impact courtes.

Intégrer l'IA dans les boîtes à outils GRC existantes :

- Capitaliser sur les missions menées au dernier trimestre 2026 : retours terrain, écarts observés, questions récurrentes des clients;
- Enrichir le référentiel unifié et les grilles d'analyse d'écart multi-référentiels;
- Adapter les trames GRC courantes — analyse de risques, politique de sécurité, contrôle permanent, homologation — aux systèmes d'IA.

Matérialiser le toolkit « roadmap gouvernance de la sécurité de l'IA » :

- Construire un modèle de trajectoire par niveaux de maturité, avec chantiers types, jalons et effort indicatif;
- Définir un modèle opérationnel évolutif et les indicateurs de pilotage associés;
- Produire les supports de formation interne et contribuer au développement de l'offre et à l'avant-vente.

Renforcement de l'outillage GRC pour la conformité au CRA

Stage de 6 mois basé à Sèvres

Description

Le règlement (UE) 2024/2847, dit Cyber Resilience Act (CRA), impose aux fabricants, éditeurs, intégrateurs et distributeurs de produits comportant des éléments numériques un socle d'exigences de sécurité : security by design, gestion des vulnérabilités sur toute la durée de support, documentation technique et évaluation de conformité. Les obligations de notification via la plateforme européenne de reporting de l'ENISA sont déjà en approche et l'applicabilité complète du texte interviendra fin 2027.

Les équipes GRC d'Almond ont formalisé un catalogue de services CRA couvrant la préparation (cadrage, cartographie produits, analyse de risques, politiques et processus), l'assessment (analyse d'écart, roadmap opérationnelle) et le suivi (pilotage, gestion à chaud des vulnérabilités et incidents, accompagnement continu). Délivrer ces services à l'échelle suppose un outillage industrialisé, cohérent d'une mission à l'autre et articulé avec les capacités techniques du groupe : laboratoire CESTI, services PSIRT et VOC.

L'objectif de ce stage est de renforcer cette boîte à outils : établir les liens de l'univers GRC avec le CESTI et son offre PSIRT, outiller les processus de gestion des vulnérabilités et des incidents produits, formaliser un kit « analyse de risques produits » et construire les trames d'auto-évaluation et d'évaluation accompagnée par un organisme notifié.

Vos missions

S'approprier le cadre CRA et l'outillage GRC existant :

- Construire un panorama du CRA et de ses textes d'application (actes délégués et d'exécution, normes harmonisées, guidelines ENISA et Commission);
- Analyser le catalogue de services CRA des équipes GRC et identifier, service par service, les manques d'outillage et les tâches à industrialiser;
- Cartographier les interfaces avec le CESTI et les services de PSIRT et de VOC : points d'entrée, données échangées, responsabilités respectives.

Outiller les processus produits et l'analyse de risques :

- Formaliser les processus de gestion des vulnérabilités et des incidents produits (détection, triage, correctif, notification, communication) avec RACI et délais;
- Produire les modèles associés : avis de sécurité, notifications aux autorités et aux clients, registre de suivi, matrice de support et de fin de vie;
- Formaliser un kit « analyse de risques produits » : méthode, échelles, scénarios types, registre et vue portefeuille, en cohérence avec EBIOS RM et l'IEC 62443.

Préparer les évaluations de conformité :

- Construire les grilles d'auto-évaluation par exigence, exploitables par les équipes produit des clients;
- Outiller la constitution du dossier d'évaluation accompagnée par un organisme notifié et son articulation avec les schémas de certification européens;
- Éprouver l'outillage sur une mission réelle, puis le présenter et le transmettre aux consultants GRC.

Sécurité des projets d'intelligence artificielle et des systèmes associés

Stage de 6 mois basé à Sèvres

Description

Almond fournit à ses clients des services de sécurité dans les projets, historiquement centrés sur les développements applicatifs et les infrastructures. Ces services sont délivrés de deux manières : réalisés par nos consultants projet par projet, ou implantés chez le client sous la forme d'un processus d'intégration de la sécurité dans les projets structuré et outillé.

Les projets d'intelligence artificielle mettent ces trames en difficulté. Les données d'entraînement et d'alimentation, les modèles et leurs fournisseurs, les chaînes de recherche augmentée, les agents et leurs garde-fous introduisent des questions que les questionnaires de sécurité projet actuels ne posent pas, et des mesures de sécurité que les catalogues existants ne couvrent qu'en partie.

L'objectif de ce stage est de développer un kit « Sécurité des projets d'intelligence artificielle et de systèmes associés » : des trames faisant la synthèse entre les critères DICP et les critères propres à l'IA, pour conduire, étape par étape, à la définition et à la mise en œuvre des bonnes mesures de sécurité.

Vos missions

S'approprier la démarche sécurité dans les projets :

- Analyser le processus et l'outillage existants : expression des besoins de sécurité, analyse de risques projet, plan d'assurance sécurité, recette et homologation;
- Identifier les points de contrôle par phase projet et la manière dont le processus s'implante chez un client;
- Confronter ces trames à des projets d'IA réels et documenter leurs limites.

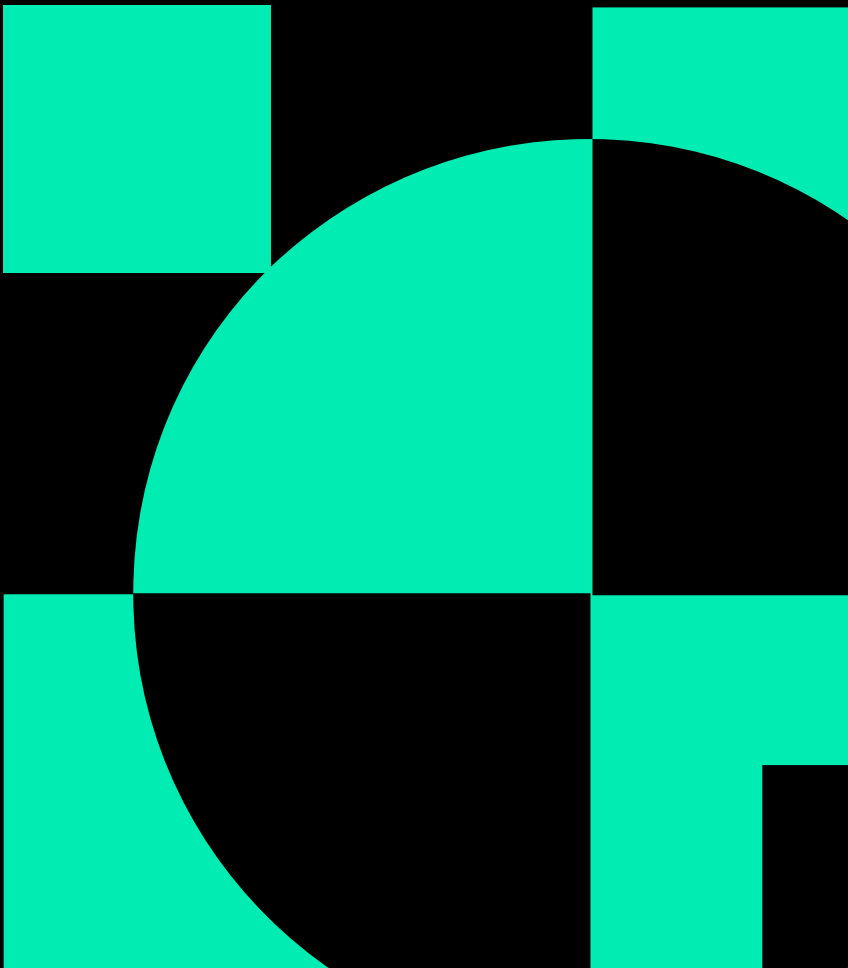
Construire le kit « sécurité des projets d'IA » :

- Concevoir une grille de qualification du projet : cas d'usage, données, modèle interne ou fournisseur, degré d'autonomie, exposition;
- Produire une trame d'expression des besoins de sécurité faisant la synthèse des critères DICP et des critères propres à l'IA;
- Construire le catalogue de mesures associé : protection des données et des modèles, filtrage des entrées et des sorties, garde-fous des agents, journalisation, supervision humaine, réversibilité;
- Définir les critères d'acceptation et les tests de recette sécurité correspondants.

Éprouver et industrialiser :

- Tester le kit sur un projet interne ou une mission client et l'ajuster;
- Articuler le kit avec les travaux de gouvernance de la sécurité de l'IA et avec l'homologation;
- Préparer les supports d'implantation du processus chez le client et former les consultants

CYBER TECHNOLOGY & TRANSFORMATION



Cyber résilience – Définir la Minimum Viable Company et concevoir son socle numérique minimal de confiance H/F

Stage de 6 mois basé à Sèvres

Description

Face à une cyberattaque majeure, les entreprises doivent identifier les activités indispensables à maintenir ou à reprendre et les moyens nécessaires à leur fonctionnement. Cette réflexion implique de définir un niveau minimal d'activité acceptable, puis de le traduire en besoins organisationnels et techniques. L'approche Minimum Viable Company (MVC) vise à déterminer ce périmètre métier essentiel : activités, niveaux de service, personnes et partenaires indispensables. La Minimum Viable Infrastructure (MVI) constitue le socle technique nécessaire pour le soutenir, en tenant compte des applications, des données et des dépendances du système d'information. L'objectif de ce stage sera de construire une méthodologie permettant de définir la MVC, de concevoir la MVI associée et d'établir une trajectoire de transformation réaliste. Vous contribuerez à articuler les besoins métier et les choix d'architecture, puis à prioriser les évolutions selon les risques, les coûts et les contraintes de mise en œuvre. La démarche sera appliquée à un périmètre pilote.

Vos missions

Définir la Minimum Viable Company :

- Étudier les analyses d'impact métier et les dispositifs de continuité existants ;
- Définir les scénarios de crise et les durées de fonctionnement dégradé à considérer ;
- Identifier les activités indispensables, leurs niveaux de service minimaux et les délais de reprise attendus ; Déterminer les ressources humaines, les partenaires et les modes opératoires nécessaires, y compris les alternatives manuelles ;
- Formaliser le périmètre MVC et les arbitrages à faire valider par les directions métier.

Définir la Minimum Viable Infrastructure associée :

- Traduire les besoins de la MVC en applications, données et services techniques indispensables ; Cartographier leurs dépendances : identités, réseau, hébergement, stockage, postes de travail et services externes ;
- Concevoir une architecture minimale de confiance adaptée aux scénarios retenus, intégrant les protections nécessaires ; Identifier les moyens d'administration, de sauvegarde et de restauration permettant de rétablir ce socle en cas de compromission ; Vérifier la cohérence de la cible avec les niveaux de service et les objectifs de reprise de la MVC.

Construire la trajectoire de transformation :

- Évaluer les écarts entre le système d'information existant et la MVI cible ;
- Comparer les options d'évolution selon leur faisabilité, leur coût et leur contribution à la résilience ; Prioriser les actions et définir des paliers de transformation tenant compte des dépendances et des ressources disponibles ;
- Construire une feuille de route précisant les responsabilités, les charges estimatives et les critères de validation ; Formaliser un plan d'exercices et de tests permettant de vérifier progressivement la capacité à soutenir la MVC.

Data Protection – Industrialiser un Data Protection Operation Center associant DLP, DSPM et assistance IA H/F

Stage de 6 mois basé à Sèvres

Description

La dispersion des données entre environnements internes, cloud et applications SaaS complexifie leur protection. Les entreprises doivent identifier leurs données sensibles, comprendre leur exposition et maîtriser leurs usages. Les solutions de Data Loss Prevention (DLP) et de Data Security Posture Management (DSPM) apportent des capacités complémentaires pour répondre à ces enjeux.

Leur exploitation nécessite une organisation capable de qualifier les alertes, de contextualiser les risques et de coordonner les actions de remédiation avec les équipes techniques et les métiers. L'assistance IA ouvre également des possibilités d'enrichissement et d'accélération des analyses, dont la fiabilité et les limites doivent être évaluées.

L'objectif de ce stage sera de contribuer à l'industrialisation d'un Data Protection Operation Center (DPOC), en capitalisant sur une première expérimentation associant des solutions pure player du marché. Vous participerez à la définition d'un service reproductible, depuis le traitement des alertes jusqu'à la réduction durable de l'exposition des données.

Vos missions

Comprendre les enjeux de protection des données et la complémentarité DLP/DSPM :

- Étudier les fonctionnalités, les périmètres de couverture et les limites des solutions DLP et DSPM ; Identifier les principaux scénarios de risque : partage excessif, transfert non autorisé, exposition de données sensibles et usages de l'IA ;
- Analyser les informations disponibles dans les deux solutions et les possibilités de rapprochement ; Définir un langage commun de classification des données et de qualification des risques.

Structurer le fonctionnement du Data Protection Operation Center :

- Analyser le retour d'expérience du premier déploiement et identifier les difficultés opérationnelles ;
- Formaliser les processus de qualification, de priorisation, d'escalade et de suivi des remédiations ;
- Préciser les responsabilités des équipes sécurité, IT et des propriétaires métier des données ; Construire les indicateurs de performance du service et de réduction de l'exposition.

Expérimenter l'assistance IA et préparer l'industrialisation du service :

- Prototyper l'enrichissement des alertes et l'assistance à leur qualification, selon les interfaces et données accessibles ;
- Comparer les résultats avec une analyse humaine, en évaluant la pertinence, les erreurs et les gains de temps ;
- Définir les conditions de validation humaine et de protection des informations traitées ; Produire un kit de déploiement réutilisable : prérequis, procédures, modèle de charge et supports de pilotage.

Protection des infrastructures IA – Concevoir et valider les mesures de sécurité d'une plateforme IA

Stage de 6 mois basé à Sèvres

Description

Les plateformes d'intelligence artificielle associent des modèles, des données, des infrastructures, des identités et des connexions au système d'information. L'intégration d'agents et de connecteurs étend leurs capacités d'action et nécessite une maîtrise précise des droits, des échanges et des traitements réalisés. Leur sécurisation doit couvrir les risques d'infrastructure et les menaces propres aux usages de l'IA : injection de prompt, exposition d'informations sensibles, altération des sources documentaires ou actions non autorisées. Elle suppose d'identifier les protections adaptées à chaque composant et d'évaluer leur efficacité sur une chaîne complète. L'objectif de ce stage sera de construire un état de la menace et de le traduire en mesures de protection techniques. Vous concevrez une architecture de référence et participerez à la validation de ses contrôles sur une plateforme de démonstration représentative, intégrant un modèle, un corpus documentaire et des connecteurs.

Vos missions

Comprendre les architectures IA et leurs risques de sécurité :

- Étudier les composants d'une plateforme IA : modèles, prompts, agents, bases documentaires, API et connecteurs ;
- Identifier les flux de données, les identités utilisées et les frontières de confiance ;
- Construire un état de la menace à partir de publications de référence ;
- Élaborer un modèle de menace sur une architecture pilote et hiérarchiser les scénarios à traiter.

Définir une architecture et des mesures de protection adaptées :

- Étudier la sécurisation des accès, des comptes techniques, des secrets et des droits accordés aux agents ;
- Définir les protections des données et des échanges, de l'ingestion documentaire jusqu'aux réponses et actions produites ;
- Identifier les mesures d'isolation, de durcissement, de journalisation et de maîtrise des flux sortants ;
- Comparer les contrôles disponibles dans l'environnement existant et les capacités des solutions spécialisées.

Mettre en œuvre et évaluer les protections sur une maquette :

- Déployer une chaîne IA représentative sur un périmètre technique maîtrisé ;
- Configurer les mesures de protection et construire des scénarios de validation en laboratoire ;
- Évaluer leur efficacité, leurs limites et leurs effets sur les usages légitimes et les performances ;
- Produire une architecture de référence, un catalogue de contrôles et un guide de sécurisation réutilisables.

Vulnerability Management / CTEM – Concevoir une priorisation explicable et reproductible des expositions, orientée remédiation H/F

Stage de 6 mois basé à Sèvres

Description

La gestion des vulnérabilités nécessite de rapprocher les constats techniques de leur contexte d'exploitation et des enjeux métier. La sévérité d'une vulnérabilité doit être complétée par l'analyse de l'accessibilité des actifs, des possibilités d'exploitation, des protections existantes et des conséquences potentielles pour l'entreprise. La démarche Continuous Threat Exposure Management (CTEM) vise à organiser l'identification, la priorisation, la validation et le traitement des expositions. Dans ce contexte, les capacités de découverte de vulnérabilités associées à l'IA, notamment autour de Mythos, soulèvent des questions sur l'évolution des besoins de priorisation et des capacités de remédiation. L'objectif de ce stage sera de concevoir et d'éprouver une méthode permettant de sélectionner les actions de réduction d'exposition les plus pertinentes sur un périmètre pilote. Vous évaluerez l'apport de l'IA à cette démarche, en recherchant des recommandations explicables, reproductibles et utilisables par les équipes opérationnelles.

Vos missions

Comprendre la démarche CTEM et les évolutions liées à l'IA :

- Étudier les étapes du CTEM et leur articulation avec la gestion des vulnérabilités ;
- Analyser les facteurs de priorisation : criticité métier, exposition, exploitabilité et mesures compensatoires ; Étudier les capacités et limites documentées des approches de découverte assistées par IA, notamment Mythos ;
- Identifier leurs implications possibles sur les volumes à traiter et l'organisation de la remédiation.

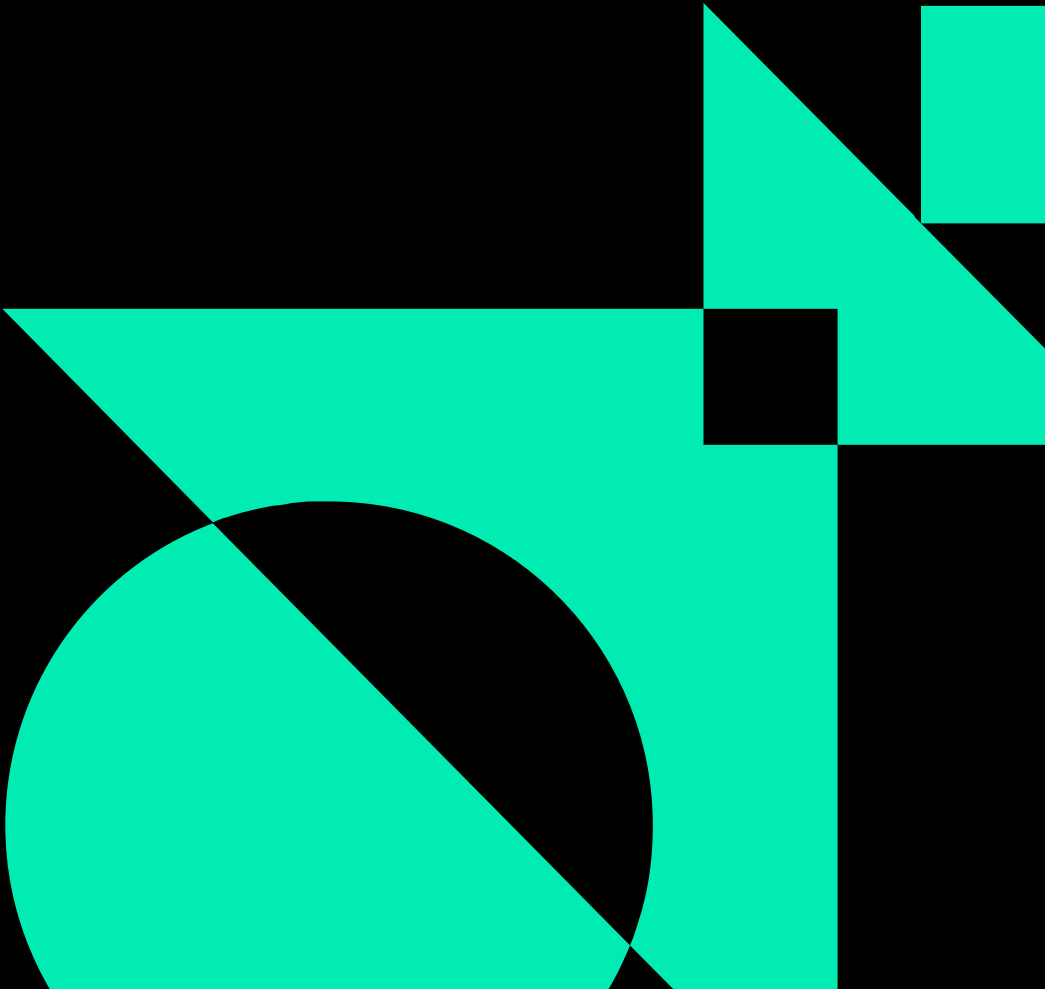
Construire une méthode de priorisation contextualisée :

- Définir un périmètre pilote et recueillir les informations nécessaires sur ses actifs et ses dépendances ; Formaliser des critères de décision traçables, en tenant compte de la qualité des données disponibles ;
- Comparer une priorisation par sévérité, une approche fondée sur des règles contextuelles et une approche assistée par IA ;
- Intégrer les contraintes de traitement : responsabilités, effort, fenêtres de changement et dépendances techniques.

Expérimenter la méthode jusqu'à la réduction de l'exposition :

- Étudier les architectures techniques permettant une ingestion massive de données d'exposition (APIs, agents, scanners) et leur corrélation ;
- Identifier les tendances vers l'automatisation décisionnelle (Risk-Based Prioritization) et les nouvelles méthodes de scoring dynamique.
- Développer un démonstrateur produisant des recommandations justifiées et soumises à validation ; Proposer des traitements adaptés : correctif, durcissement, restriction d'accès ou mesure compensatoire ;
- Vérifier, sur des cas sélectionnés, l'efficacité des actions réalisées ;
- Formaliser un kit méthodologique comprenant arbres de décision, indicateurs, limites et conditions de réutilisation.

OFFENSIVE SECURITY



Ethical Hacker / Pentester

Stage de 6 mois basé à Sèvres

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.

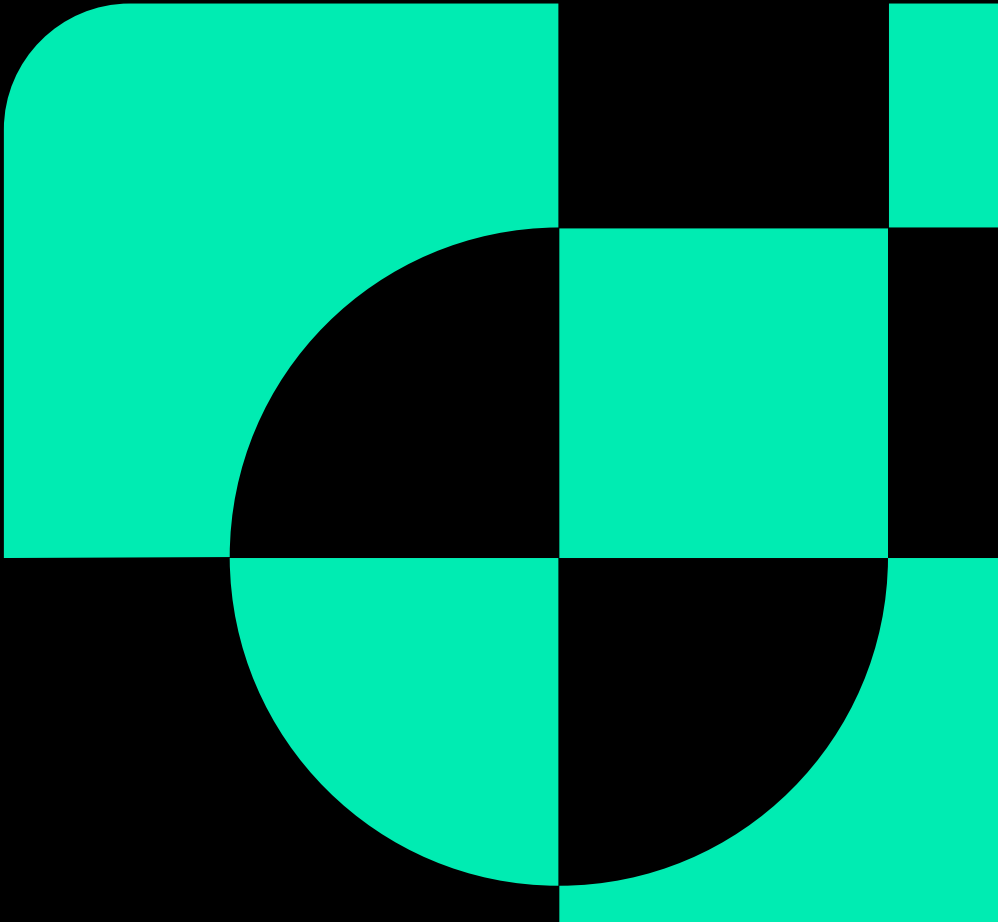
Un stage au sein de l'équipe Offensive Security, c'est l'opportunité de travailler avec des personnes spécialisées dans le domaine et fortes d'une expérience de plusieurs années, ayant rédigé plusieurs articles techniques sur des sujets divers de la sécurité offensive.

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).

AVANT - VENTE



Ingénieur Transformation Digitale Avant-Vente Cyber

Stage de 6 mois basé à Sèvres

Description

Au sein de l'équipe Avant-Vente Cyber, vous contribuerez à la transformation digitale de nos activités en développant des outils, en structurant nos offres de cybersécurité et en intégrant les usages de l'Intelligence Artificielle.

Vous interviendrez sur des projets concrets ayant un impact direct sur la performance commerciale et l'efficacité des équipes.

Vos missions

30 % | Développement Power Platform & Data

- Développer des applications avec Power Apps.
- Automatiser des processus avec Power Automate.
- Concevoir des tableaux de bord Power BI.
- Exploiter les données issues de Microsoft 365, SharePoint ou Dataverse.
- Améliorer les outils de pilotage de l'activité.

40 % | Avant-Vente & Offres Cyber

- Participer à la création et à l'évolution des offres de cybersécurité.
- Structurer des modèles d'offres, de livrables et de chiffrage.
- Produire des supports de présentation synthétiques.
- Contribuer au suivi de l'activité commerciale et à l'amélioration du Win Rate.
- Participer à l'amélioration continue des méthodes et des outils de l'équipe.

30 % | IA & Innovation

- Identifier de nouveaux usages de l'IA générative.
- Développer des assistants et outils d'aide à l'avant-vente.
- Exploiter l'IA pour améliorer les développements et les processus.
- Réaliser une veille technologique et proposer des innovations.

SECURITY EVALUATION & ANALYSIS LAB (CESTI)



Évaluation de sécurité matérielle H/F

Stage de 6 mois basé à Rennes

Description

Au travers des activités de son CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information, agréé par l'ANSSI), Almond évalue et analyse actuellement la sécurité de nombreux produits logiciels, avec une expertise reconnue sur la recherche de vulnérabilités touchant ces produits. Dans la continuité de cette expertise, Almond souhaite étendre ses capacités d'évaluation de la sécurité matérielle des produits. Une chaîne de sécurité ne s'arrête pas au logiciel : elle repose aussi sur le matériel qui l'héberge, et c'est précisément là que se cachent certaines des vulnérabilités les plus critiques.

Le stage proposé s'inscrit dans cette démarche de recherche de vulnérabilités. Il consistera à développer des méthodologies et techniques d'analyse basées sur des techniques offensives à part entière : rétro-ingénierie de PCB ou de firmware, exploitation d'interfaces de debug (JTAG, UART, SWD), extraction et analyse de mémoires flash, contournement de mécanismes anti-tamper, etc. Ces attaques matérielles permettent de faire tomber des protections que l'analyse logicielle seule ne peut jamais atteindre — un terrain de jeu exigeant, à la croisée de l'électronique, du bas niveau (bare metal, temps réel) et de la sécurité offensive.

Vos missions

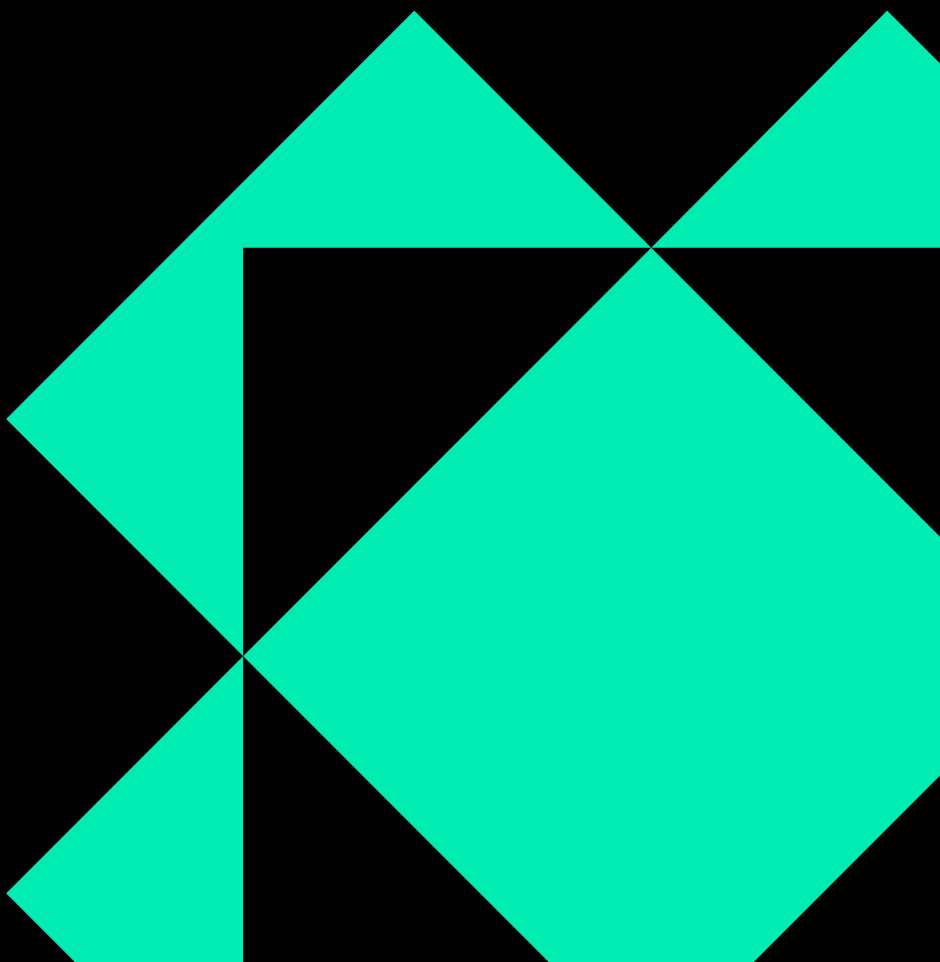
Le stage s'organisera de la manière suivante :

- Phase 1 : Montée en compétence sur la sécurité matérielle,
 - Identification des composants d'un PCB
 - Soudure/décapage
 - Protocoles de communications (JTAG, UART, SPI, ...)
 - Extraction de mémoire flash
- Phase 2 : mise à jour des méthodologies et connaissances internes
- Phase 3 : développement d'outils dédiés

Compétences recherchées

- Programmation bas niveau (C, et idéalement notions de VHDL/Verilog) et systèmes Linux
- Curiosité pour le hardware hacking et la rétro-ingénierie
- Rigueur et autonomie dans la conduite d'analyses techniques

PÔLE OUEST



Cybersouveraineté des infrastructures H/F

Stage de 6 mois basé à Nantes ou Rennes

Description

De nombreuses organisations se trouvent actuellement dans un phénomène de multi-dépendances vis-à-vis de ses fournisseurs de solutions de sécurité du SI : géopolitique avec un risque d'espionnage ou de rupture de service, hégémonique avec un risque d'augmentation non maîtrisée des prix, ou encore technique avec un risque de perte de maîtrise des fonctions (accentué par la SaaSification des services). Dans ce contexte, ces organisations pensent de plus en plus à renforcer le critère de « souveraineté » pour augmenter la maîtrise de leur SI, mais sont confrontées à des limites de connaissances et de compétences sur le marché cyber EU ou FR pour faire les bons choix.

L'objectif du stage sera dans un premier temps de comprendre les principaux concepts des architectures technique des organisations et des dépendances. Par la suite, l'étude portera sur les principales solutions de sécurité et architectures alternatives qui existent et peuvent être considérées plus souveraines, des offres privées EU jusqu'à l'open-source. 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. Un focus particulier serait à faire sur l'ensemble des fonctions de la plateforme Microsoft 365 pour construire des schémas alternatifs, et étudier les méthodologies possibles de transition.

Vos missions

Comprendre les concepts, les solutions, les architectures, et les recommandations liées à la « souveraineté » :

- Qu'est-ce la souveraineté, et dans quels contextes est-elle importante ? ;
- Identifier les sources de risques liées au défaut de souveraineté dans un SI, et en évaluer le poids pour prioriser les chantiers d'infrastructure du SI ;
- Comprendre l'articulation des composants et solutions de sécurité dans un SI

Etudier les alternatives aux solutions de sécurité hégémoniques :

- Proposer des scénarios d'études approfondies pour étudier les alternatives, M365 était un axe prioritaire à développer ;
- Sur ces scénarios, étudier le marché des solutions, des fonctions, des architectures, des prix qui permettent des alternatives ;
- Identifier les méthodes et moyens permettant les transitions pour chaque scénario (projet et technique).

Mettre en place un PoC :

- Mettre en place un tenant M365 et le peupler de manière standard ;
- Choisir 1 à 2 scénarios alternatifs, implémenter les solutions cibles, et tester la bascule de modèle.

Etude des recommandations liées à l'authentification

Stage de 6 mois basé à Nantes ou Rennes

Description

L'authentification par mot de passe est un pilier fondamental de la sécurité informatique. L'objectif 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 (pour des identités humaines), 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 des mots de passe :

- Analyse des tendances actuelles et des évolutions historiques en matière de sécurité 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.
- 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.
- Proposer un ensemble de recommandations et de bonnes pratiques concernant l'usage des mots de passe en fonction de cas d'usages.
- 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.

Méthodologie d'audit des applications LLM/RAG

Stage de 6 mois basé à Nantes ou Rennes

Description

L'adoption des assistants conversationnels et applications reposant sur des modèles de langage (LLM) s'est généralisée dans les organisations. Ces applications sont majoritairement construites selon une architecture RAG (Retrieval-Augmented Generation), qui connecte un modèle de langage au patrimoine documentaire de l'entreprise afin de produire des réponses contextualisées. Cette architecture introduit une classe de risques que les méthodologies de test d'intrusion traditionnelles ne couvrent pas. Certains référentiels (OWASP Top 10 for LLM Applications, MITRE, etc.) commencent à structurer ces risques, mais restent au niveau du catalogue et n'offrent pas de mode opératoire de test outillé et reproductible.

L'objectif du stage sera, dans un premier temps, de comprendre le fonctionnement technique des architectures LLM/RAG et de cartographier leur surface d'attaque réelle. L'étude portera ensuite sur la construction d'une méthodologie d'audit structurée, reproductible et outillée, couvrant l'ensemble de la chaîne, de l'ingestion documentaire à la restitution à l'utilisateur. Cette méthodologie devra être confrontée au terrain à travers un environnement de maquette permettant d'éprouver les tests et servir de support de montée en compétences pour l'équipe. L'ensemble a vocation à alimenter directement l'offre d'audit et à être mobilisable en mission.

Vos missions

Comprendre les architectures LLM/RAG et leurs enjeux de sécurité :

- Assimiler les concepts fondamentaux liés aux LLM et environnements RAG ;
- Décrire les architectures de déploiement rencontrées en entreprise ;
- Cartographier la surface d'attaque de bout en bout : sources documentaires, pipeline d'indexation, modèle, interface utilisateur ;
- Réaliser un état de l'art des référentiels existants, en identifier les points communs & les angles morts.

Construire un outillage permettant d'assister les auditeurs pendant les audits :

- Étudier les outils d'audit de LLM disponibles, évaluer leur apport réel par rapport aux tests manuels, et développer un outillage complémentaire si pertinent ;
- Concevoir et développer une application RAG vulnérable en environnement interne, reproduisant un cas d'usage réaliste.

Formaliser une méthodologie et un référentiel de tests :

- Formaliser un référentiel de cas de test par catégorie de risque : injection de prompt, exfiltration de données, contournement des garde-fous
- Définir le mode opératoire d'une mission type : cadrage, informations et accès à demander au client, périmètre technique, points de contrôle en revue d'architecture
- Proposer un ensemble de recommandations et bonnes pratiques liées aux infrastructures LLM/RAG.

Recherche et développement sur la sécurité des applications mobiles (Android & IOS) H/F

Stage de 6 mois basé à Rennes

Description

Les équipes d'audit de Rennes et Nantes 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

- Faire un état de l'art des techniques de test d'intrusion sur les plateformes Android et iOS (OWASP MASVS / MASTG)
- Approfondir l'analyse statique : rechercher, tester et évaluer des méthodologies et outils d'analyse statique automatisée et manuelle (reverse engineering, décompilation, inspection de code, détection de secrets, etc.)
- Développer des preuves de concept (POC) : tester différentes techniques d'attaque dynamique et d'analyse statique sur des applications réelles ou d'entraînement ;
- Développer un outillage interne permettant de structurer et d'automatiser une partie des audits mobiles.
- Enrichir la base de connaissances interne : rédiger de la documentation technique et des guides méthodologiques à destination de l'équipe
- Présenter ses travaux et animer une session de partage de connaissances
- Découvrir le métier d'Auditeur en assistant à quelques missions d'audit (tests d'intrusion, audit de code, audit de configuration, etc.).

Profil recherché

- Vous êtes élève Ingénieur ou équivalent Bac +5 dans le domaine de la sécurité informatique/
- Vous détenez des compétences dans les domaines suivants : systèmes et réseaux, programmation et scripting, sécurité informatique.
- Vous possédez une appétence particulière et une curiosité pour les environnements mobiles Android et IOS.
- Vous aimez travailler en équipe et détenez de bonnes capacités de communication. Rigoureux(se), vous êtes force de proposition.

Amélioration de l'outillage pour l'audit de code H/F

Stage de 6 mois basé à Rennes

Description

Les audits de code sont des missions qui consistent à auditer la sécurité d'applications sur la base de leur code source. L'objectif est d'y identifier des vulnérabilités afin de proposer des recommandations de sécurité adaptées à chaque contexte.

La plupart du temps, pour des raisons de confidentialité ces audits sont réalisés sur des postes déconnectés d'internet, ce qui limite les outils utilisables. Actuellement, l'équipe dispose d'une méthodologie d'analyse manuelle et d'outils rudimentaires. Pour renforcer la qualité de ces audits, l'outillage à disposition des auditeurs pourrait être amélioré et étendu.

Vos missions

Le stage s'organisera de la manière suivante :

- Prise en main de la méthodologie d'audit et des outils existants.
- Amélioration d'outils existants, notamment pour la vérification de vulnérabilités publiques dans les dépendances logicielles.
- Création de règles Semgrep approfondies.
- Réalisation d'un état de l'art d'outils de création de CFG (control-flow graph) du code, puis adaptation d'un de ces outils aux besoins d'audit.
- Amélioration de la détection de fonctions dangereuses, notamment en Java et PHP.
- Consolidation de la méthodologie d'analyse par la rédaction de certains blocs.
- Automatisation de certaines tâches de base.
- Présentation de ses travaux au reste de l'équipe d'audit.
- Découverte du métier d'auditeur en assistant à des missions d'audit, en particulier des audits de code.

Attaques & Audit en environnement Azure et Hybride H/F

Stage de 6 mois basé à Rennes

Description

Les entreprises migrent massivement leurs systèmes d'information vers le Cloud et adoptent des architectures hybrides mêlant infrastructures on-premise et services hébergés.

Cette transformation redéfinit en profondeur la surface d'attaque et pose de nouveaux défis en matière de cybersécurité. En effet, l'interconnexion entre un annuaire Active Directory local et un tenant Azure/Entra ID, la multiplication des identités synchronisées ainsi que la diversité des services managés exposés augmentent significativement les risques de compromission. Les chemins d'attaque ne se limitent plus au périmètre traditionnel : un accès obtenu sur un poste on-premise peut, par rebond, conduire à la prise de contrôle d'un environnement Cloud complet, et inversement.

C'est pourquoi la maîtrise des vecteurs d'attaque propres à ces environnements est aujourd'hui indispensable pour évaluer et renforcer le niveau de sécurité des organisations.

L'objectif du stage sera dans un premier temps de réaliser un état de l'art des différentes architectures Azure et hybrides rencontrées en entreprise, ainsi que des mécanismes de sécurité et des vecteurs d'attaque associés.

Par la suite, il s'agira de concevoir et déployer un laboratoire de test représentatif de ces environnements, servant de support à la réalisation d'attaques couvrant les différentes phases d'un test d'intrusion. Enfin, l'ensemble de ces travaux devra aboutir à la formalisation d'un plan de tests structuré et réutilisable, destiné à outiller les missions d'audit réalisées pour nos clients.

Attaques & Audit en environnement Azure et Hybride H/F

Stage de 6 mois basé à Rennes

Vos missions

Réaliser un état de l'art des environnements Azure et hybrides et de leurs enjeux de sécurité :

- Étudier les différentes architectures Azure et Entra ID rencontrées en entreprise, ainsi que les mécanismes de gestion des identités et des accès (RBAC, rôles, principaux de service, identités managées) ;
- Comprendre le fonctionnement des architectures hybrides et des briques de synchronisation entre Active Directory on-premise et le Cloud (Entra Connect, PHS, PTA, ADFS) ;
- Identifier les risques et les vecteurs d'attaque spécifiques à ces environnements, ainsi que les chemins de compromission entre le monde on-premise et le Cloud ;
- Cartographier la surface d'attaque en s'appuyant sur des référentiels reconnus (MITRE ATT&CK, matrices de menaces Cloud).

Concevoir un laboratoire de test et réaliser des attaques :

- Définir les cas d'usage et les configurations représentatives des environnements d'entreprise à reproduire ;
- Déployer un lab intégrant un tenant Azure/Entra ID, un Active Directory local et les briques de synchronisation hybride, avec des configurations réalistes et volontairement vulnérables ;
- Étudier et éprouver les principaux outils offensifs de l'écosystème (ROADtools, AzureHound, MicroBurst, GraphRunner, etc.).

Formaliser un plan de tests pour les audits clients :

- Documenter chaque technique d'attaque, ses prérequis, ses moyens de détection et les mesures de remédiation associées ;
- Proposer un ensemble de recommandations et de bonnes pratiques de durcissement des environnements Azure et hybrides ;
- Capitaliser l'ensemble des travaux sous la forme d'un plan de tests structuré, réutilisable et directement exploitable lors des missions d'audit en contexte client

Ingénieur R&D Sécurité Offensive Émulation d'Attaques Avancées (Red Team) H/F

Stage de 6 mois basé à Rennes

Description

La plateforme M&NTIS, développée par Almond, est une solution de Cyber Range et d'émulation d'adversaires. Elle permet de générer des infrastructures d'entreprises réalistes et d'y dérouler des scénarios d'attaque pour entraîner des équipes de défense (Blue Team) et évaluer des solutions de sécurité (EDR, SIEM, sondes, agents IA, ...).

Pour maintenir la pertinence de son catalogue d'attaques face à l'évolution des menaces courantes (groupes APT, ransomwares), l'équipe R&D doit régulièrement concevoir de nouveaux scénarios. L'objectif de ce stage est de concevoir, développer et automatiser un enchaînement d'actions offensives calqué sur un mode opératoire récent documenté par la communauté cyber.

Vos missions

Encadré par un ingénieur de l'équipe M&NTIS, les activités du stage se structureront autour des étapes suivantes :

Cyber Threat Intelligence (CTI) & Modélisation

- Étudier des rapports techniques de sources de référence (CERTs, éditeurs de sécurité) pour identifier un mode opératoire d'attaque d'actualité.
- Cartographier logiquement l'ensemble des actions (Kill Chain) en s'appuyant sur le référentiel général MITRE ATT&CK®.

R&D Offensive

- Concevoir et développer les scripts ou programmes matérialisant chaque action offensive (ex: accès initial, contournement d'EDR, élévation de privilèges, mouvements latéraux, persistance).
- Exploiter les outils de test d'intrusion reconnus ou concevoir des charges utiles sur mesure.

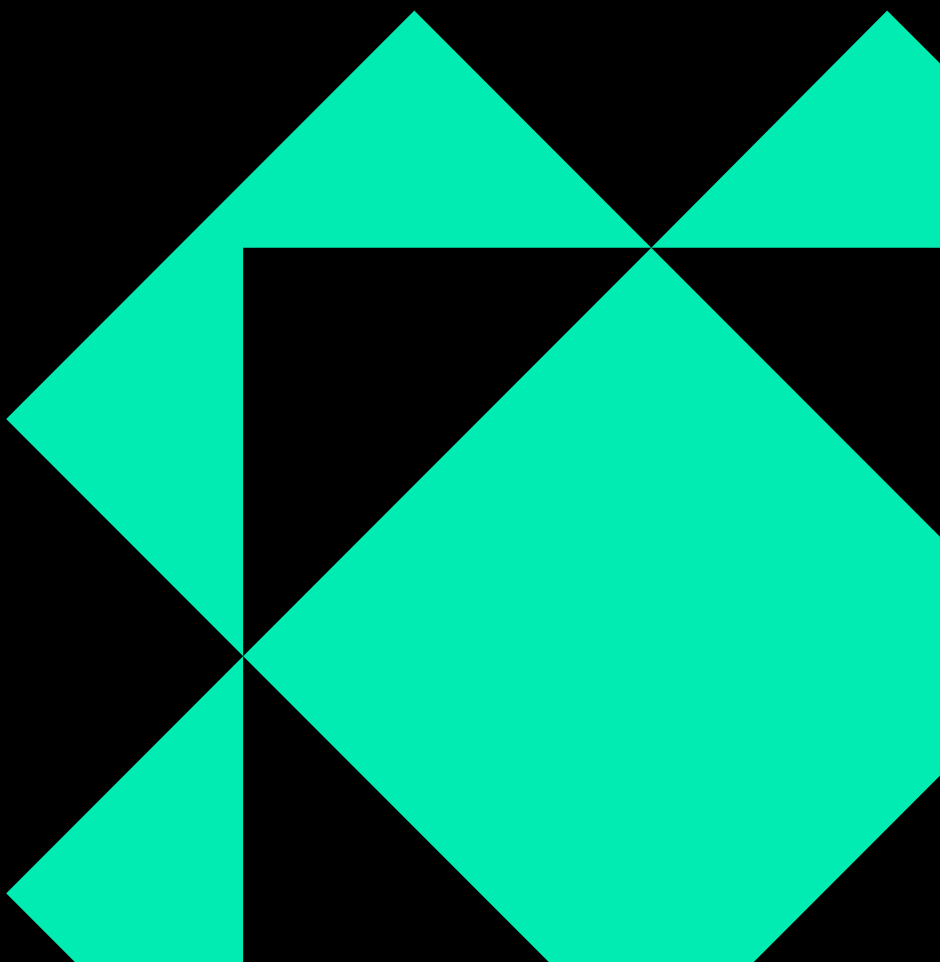
Orchestration et Scénarisation (Cyber Kill Chain)

- Assembler ces attaques unitaires au sein du moteur d'émulation de M&NTIS pour former un scénario complet et cohérent (ex: le résultat de l'étape A sert d'outil ou d'accès pour l'étape B).
- Prendre en compte les contraintes d'évasion pour rendre le comportement de l'injecteur d'attaque réaliste face aux solutions de sécurité (EDR, SIEM, sondes réseau) connectées à la plateforme.

Qualification & Analyse des Données

- Exécuter le scénario complet dans les environnements virtuels de test.
- Analyser et documenter les traces générées (fichiers PCAP, logs système au format ECS) afin de garantir la pertinence des métadonnées produites par la plateforme pour les équipes défensives (SOC / CERT).

BOARD OF CYBER



Chef de projet clients cybersécurité H/F

Stage de 6 mois basé à Sèvres

Description

Board of Cyber est une startup française, qui développe et commercialise des solutions SaaS Cyber. Son produit phare est le «Security Rating®» qui délivre une notation de la performance et de la maturité cyber des entreprises sur leur empreinte Internet à partir de données publiques. Cette notation est non intrusive, en continu, 100% automatisée et propose des recommandations pour améliorer la performance cyber.

Vos missions

En tant que Customer Success Manager, vous accompagnez et fidélisez les clients dans l'utilisation du Security Rating® pour qu'ils en tirent le maximum de valeur.

- Participer au suivi du portefeuille client et être l'interlocuteur de référence.
- Accompagner les clients dans l'usage du Security Rating® : conseiller, former et répondre au mieux à leurs besoins et à leurs attentes.
- Apporter un premier niveau de réponse aux demandes entrantes de nos clients
- Fidéliser la clientèle et suivre la satisfaction client.
- Renseigner les suivis clients dans notre outil de gestion de projet interne (Hubspot)
- Participer à automatisation de la relation clients et la structuration du département.

Profil recherché

- Vous êtes étudiant(e) en BAC + 4/5, en école d'ingénieur, université/école de management ou formation avec une dimension commerciale.
- Vous avez un bon degré d'autonomie et est toujours partant(e) pour t'emparer des sujets qui te sont confiés.
- Vous avez une personnalité positive, enthousiaste et sociable
- Vous avez déjà une première expérience commerciale
- Vous avez curieux(se)/intéressé(e) par le domaine de l'informatique et plus spécifiquement de la Cybersécurité

DIRECTION DES OPERATIONS



Chief of Staff Operations H/F

Stage de 6 mois basé à Sèvres

Description

Board of Cyber est une startup française, qui développe et commercialise des solutions SaaS Cyber. Son produit phare est le «Security Rating®» qui délivre une notation de la performance et de la maturité cyber des entreprises sur leur empreinte Internet à partir de données publiques. Cette notation est non intrusive, en continu, 100% automatisée et propose des recommandations pour améliorer la performance cyber.

Vos missions

En tant que Customer Success Manager, vous accompagnez et fidélisez les clients dans l'utilisation du Security Rating® pour qu'ils en tirent le maximum de valeur.

- Participer au suivi du portefeuille client et être l'interlocuteur de référence.
- Accompagner les clients dans l'usage du Security Rating® : conseiller, former et répondre au mieux à leurs besoins et à leurs attentes.
- Apporter un premier niveau de réponse aux demandes entrantes de nos clients
- Fidéliser la clientèle et suivre la satisfaction client.
- Renseigner les suivis clients dans notre outil de gestion de projet interne (Hubspot)
- Participer à automatisation de la relation clients et la structuration du département.

Profil recherché

- Vous êtes étudiant(e) en BAC + 4/5, en école d'ingénieur, université/école de management ou formation avec une dimension commerciale.
- Vous avez un bon degré d'autonomie et est toujours partant(e) pour t'emparer des sujets qui te sont confiés.
- Vous avez une personnalité positive, enthousiaste et sociable
- Vous avez déjà une première expérience commerciale
- Vous avez curieux(se)/intéressé(e) par le domaine de l'informatique et plus spécifiquement de la Cybersécurité