APPEL À MANIFESTATION D'INTÉRÊT

Offreurs de solutions & services de sécurisation de l'IA à destination des TPE, PME, acteurs de l'ESS & collectivités territoriales

Contrat de subvention DIGITAL n°101083769
Date de début du projet : 1 janvier 2023
Durée du projet : 42 mois
Auteur : Cyril Nicolotto
Date : 08/07/2025

Ce projet est cofinancé par l'Union européenne dans le cadre du programme DIGITAL.
Ce document est destiné à une diffusion publique (PU).

SOMMAIRE

1. CONTEXTE DE L'AMI 2
2. OBJECTIF DE L'AMI 3
3. CRITÈRES DE RÉFÉRENCEMENT DES OFFREURS 5
4. DURÉE DE RÉFÉRENCEMENT DES OFFRES 6
5. MODALITÉ DE RÉPONSE À L'AMI 6
6. RADIATION 7
7. À PROPOS DE CYBIAH 7

1. CONTEXTE DE L'AMI

Le Campus Cyber porte le projet CYBIAH, European Digital Innovation Hub, sous forme d'un parcours d'accompagnement, visant à consolider la résilience aux cyberattaques des TPE, PME, acteurs de l'ESS et collectivités d'Ile de France.

Le parcours proposé aux TPE, PME, acteurs de l'ESS et collectivités d'Ile de France comprend plusieurs phases :

- **Embarquement**
- **Diagnostic**
- **Services et solutions**
- **Ingénierie financière**

La première phase du parcours d'accompagnement dite « **embarquement** » consiste à rencontrer les dirigeants de la société et d'évaluer le niveau de risque cyber auquel elle doit faire face, tout en comprenant les enjeux métiers et stratégique de la structure.

La seconde phase du dispositif, « **diagnostic** », vise à s'inscrire dans l'accompagnement bout-en-bout par un acteur bienveillant et de confiance. Cette seconde phase a pour objectif la réalisation de **diagnostics techniques et organisationnels** qui vont permettre d'établir un «plan de remédiation », qui va inclure des recommandations sur l'organisation interne, sur un plan de formation, sur les solutions techniques, et d'expérimenter également ces solutions techniques dans le contexte des TPE, PME, acteurs de l'ESS et collectivités.

La troisième phase « services & solutions », objet du présent AMI, vise à proposer aux TPE, PME, acteurs de l'ESS et collectivités, qui ont fait l'objet d'un diagnostic cyber, un ensemble de solutions de cybersécurité pour la sécurisation de l'IA qui répondent aux recommandations du plan de sécurisation, afin d'en produire un plan d'actions opérationnel. Chaque besoin nécessitant du matériel, des logiciels, des services ou prestations de cybersécurité fera l'objet d'une recommandation d'un offreur afin d'orienter la structure diagnostiquée vers un professionnel de la cybersécurité « de confiance » qui aura été sélectionné au sein de cet AMI.

Chacune des solutions de cybersécurité pour la sécurisation de l'IA retenues dans cet AMI pourra être recommandée, selon les résultats des diagnostics, à de nombreuses TPE, PME, acteurs de l'ESS et collectivités de la région Ile-de-France. **CYBIAH a pour objectif d'accompagner 150 TPE, PME, acteurs de l'ESS et 30 collectivités à horizon mi-2026**.

Cofinancé par l'Union européenne
CAMPUS CYBER
Région îledeFrance

2. OBJECTIF DE L'AMI

Le présent AMI vise à recenser des offreurs de solutions de cybersécurité pour la sécurisation de l'IA selon plusieurs « segments ». Les solutions recherchées dans cet AMI sont :

Solutions recherchées
1. Gouvernance et conformité IA
Audit, conformité et gouvernance
Solutions permettant l'analyse de risques, la conformité réglementaire (NIS2, RGPD, AI Act, etc.), la cartographie des modèles et des flux de données, l'audit de code et de pipeline IA, solution de journalisation de la télémétrie de l'IA
Robustesse et validation
Test d'attaques, vérification de robustesse, évaluation de la résilience des modèles (adversarial testing, red teaming IA)
Gestion Risques
Solutions pour l'accompagnement sur l'analyse des risques spécifiques à l'IA, la création d'une matrice de criticité, l'établissement d'une cartographie des vulnérabilités du système d'IA, la création d'une nomenclature des matériaux de l'IA (AI Bill Of Material)
2. Protection des données et des flux d'IA
Chiffrement et anonymisation avancés
Solutions de cryptographie et anonymisation appliquées à l'apprentissage fédéré, au stockage, à la transmission des données (chiffrement homomorphe, differential privacy)
Protection contre l'empoisonnement de données et l'exfiltration
Contrôle de la confidentialité et l'intégrité des entrées et des sorties, solutions de détection d'anomalies dans les jeux de données, détection de prompt injection, monitoring des accès
3. Sécurité applicative et infrastructurelle pour l'IA
Sécurisation des API, endpoints et intégrations IA
Solutions de découverte, de contrôle d'accès et de protection des API exposant des modèles d'IA (API Security, API Gateway avec détection d'anomalies IA), protection CI/CD IA, solutions

Cofinancé par l'Union européenne
CAMPUS CYBER
Région îledeFrance

Solutions recherchées
d'évaluation du niveau de confiance des bibliothèques et des modules externes utilisés dans les systèmes d'IA
Protection des environnements IA (cloud, edge, on-premise)
Plateformes de sécurisation des charges de travail IA (apprentissage, validation, inférence, déploiement, orchestration sécurisée, segmentation réseau)
Sécurité collaborative
Solutions de chiffrement de paramètres fédérés, de détection de participants malveillants et d'audits des environnements multiparties
4. Détection, réponse et remédiation spécifique IA
SIEM (Security Information and Event Management) / UEBA (User and Entity Behavior Analytics) / SOAR (Security Orchestration, Automation and Response) adaptés à l'IA
Outils de supervision, de détection d'incidents et d'analyse comportementale intégrant des scénarios d'attaque IA (prompt injection, model stealing, etc.).
SOC (Security Operations Center) et MDR (Managed Detection & Response) spécialisés IA
Services externalisés de détection et de réponse aux incidents sur les systèmes d'IA, incluant threat hunting IA et forensic IA
5. Solutions de protection « spécifiques IA » (modèles, LLM, RAG, Agents, etc...)
Défense contre l'empoisonnement, l'évasion et le vol de modèle
Durcissement du modèle (entraînement adversarial ou distillation de réseau), défense contre le model extraction et le model inversion, solutions de formats sécurisés pour le stockage et la distribution des modèles d'IA, solutions de filtrage de sécurité pour détecter les instructions malveillantes, les entrées adverses ou les requêtes atypiques
Protection contre la Shadow AI et usages non autorisés
Outils de découverte et de blocage des usages non validés de l'IA dans l'organisation (Shadow IT appliqué à l'IA)
Sécurisation de la chaîne RAG et de l'ingestion de données
Contrôle d'accès et chiffrement des flux entre sources de données et modèles, vérification d'intégrité des données injectées dans les workflows RAG

Cofinancé par l'Union européenne
CAMPUS CYBER
Région îledeFrance

Solutions recherchées
Systèmes agentiques
Solutions de filtrage de prompt injection, surveillance agents autonomes, protection bases de connaissances, protection des communications avec d'autres agents ou systèmes (A2A, MCP)
6. Protection des systèmes spécifiques
Protection des environnements IoT / OT embarquant de l'IA
Solutions dédiées à la sécurisation des IA déployées sur objets connectés, automates industriels, etc.
Solutions de sécurité de l'IA spécifiques aux domaines sectoriels
Solutions verticalisées adressant les contraintes réglementaires et techniques de secteurs spécifiques (conformité HDS en santé, DORA en finance, etc…)

3. CRITÈRES DE RÉFÉRENCEMENT DES OFFREURS

Les offreurs de solutions et de services en cybersécurité retenus dans le cadre du référencement devront respecter les critères suivants :

- Être une entreprise avec un établissement implanté dans l'Union Européenne et en capacité de déployer ses prestations en matière de cybersécurité sur une zone géographique au minimum départementale en France ;
- Disposer d'une bonne connaissance de la sécurisation des systèmes d'informations des petites et moyennes entreprises, acteurs de l'ESS et des petites collectivités.

Les critères d'évaluation des propositions seront les suivants :

- Capacité à adresser le marché des TPE, PME, acteurs de l'ESS et collectivités
- Prix de l'offre cohérent
- Pricing & mode de distribution adapté
- Robustesse / certifications de sécurité éventuelles (audits de sécurité de la solution, certifications/qualifications type ANSSI, labellisations cyber)
- Modalités d'intégration
- Modalité d'administration & maintenabilité

Cofinancé par l'Union européenne
CAMPUS CYBER
Région îledeFrance

Une commission sera réunie pour noter les réponses sur la base de ces critères et **retenir de 1 à 3 offreurs sur le segment/type de produit/service recherché** selon le nombre de réponses reçues. Il sera demandé aux offreurs de consentir à une remise tarifaire dans le cadre de leur candidature au présent AMI, et ce, afin de faire bénéficier aux 150 potentielles TPE, PME, acteurs de l'ESS franciliennes et 30 collectivités, d'un tarif attractif permettant d'acquérir la solution au meilleur prix.

4. DURÉE DE RÉFÉRENCEMENT DES OFFRES

Les offres qui auront été sélectionnées dans le présent AMI seront retenues au sein du catalogue CYBIAH pour une durée allant jusqu'au mois de juin 2026. Un nouvel AMI pourra être communiqué à l'issue de cette période.

À l'issue de la sélection et jusqu'à la fin de cette période de référencement, les offreurs retenus seront sollicités de manière semestrielle afin de confirmer ou mettre à jour les informations de candidatures transmises initialement. Si ces informations étaient de nature à remettre en cause la sélection initialement réalisée, un offreur pourrait voir sa solution retirée du catalogue en lieu et place de l'offreur immédiatement en dessous dans la grille de notation.

5. MODALITÉ DE RÉPONSE À L'AMI

Les candidatures doivent être envoyées via le formulaire suivant :

https://cybiah.eu/fr/actualites/ami-ia/

Le calendrier pour l'appel d'offres est le suivant :

- Date limite de réception des propositions : **15/09/ 2025**
- Sélection du prestataire retenu et communication des résultats : **à partir du 20/10/2025**

Veuillez noter que toutes les communications (questions et réponses à l'AMI) relatives à cet appel à manifestation d'intérêt doivent être dirigées vers l'adresse électronique suivante : **contact@cybiah.eu**

Si de nouvelles briques technologiques n'ont pas été identifiées dans le présent AMI et qu'elles s'avèrent nécessaires par la suite, un nouvel appel spécifique sur ce segment pourrait être passé

Cofinancé par l'Union européenne
CAMPUS CYBER
Région îledeFrance

selon les mêmes modalités. Le segment technologique en question fera l'objet du même processus de sélection que décrit dans le présent AMI.

S'il s'avère qu'aucune société n'a candidaté sur un segment spécifique, un nouvel AMI pourra être publié dans les mêmes conditions.

6. RADIATION

Toute entreprise pourra être radiée de la liste de référencement lors des évaluations périodiques, notamment pour les raisons suivantes :

- Si elle se trouve prise en défaut vis-à-vis des déclarations relatives à la réponse formulée au présent appel à manifestation d'intérêt ;
- Si elle se retrouve dans l'incapacité de mener à bien les prestations sur la base desquelles elle a été référencée.
- Si les conditions d'exécutions de la prestation mentionnée dans la réponse de l'entreprise ne sont pas ou plus applicables
- CYBIAH se réserve la possibilité de radier une société référencée à sa discrétion.

7. À PROPOS DE CYBIAH

CYBIAH (Cyber et IA Hub) est un programme coordonné par le Campus Cyber qui aide les TPE, PME, acteurs de l'Économie Sociale et Solidaire et collectivités d'Île-de-France à renforcer leur sécurité numérique.

CYBIAH propose un **accompagnement cybersécurité complet** : évaluation des besoins, diagnostic personnalisé, recommandations concrètes et solutions adaptées. Ce dispositif est **intégralement pris en charge** grâce au cofinancement de l'Union européenne, en partenariat avec la Région Île-de-France pour les TPE, PME et acteurs de l'ESS, et avec la Métropole du Grand Paris pour les communes métropolitaines.

Dans ses missions, CYBIAH s'appuie sur un consortium de 11 partenaires publics et privés, parmi lesquels : **Campus Cyber, la CCI Paris Île-de-France, POLD, Inria, Sekoia.io, EPITA, Erium, F.initiatives, Hub France IA, la Métropole du Grand Paris, et Allonia**. CYBIAH est reconnu comme pôle de référence en cybersécurité **(EDIH – European Digital Innovation Hub)** par la Commission Européenne.