



CYBIAH
EUROPEAN DIGITAL
INNOVATION HUB
ILE-DE-FRANCE



Cofinancé par
l'Union européenne



Région
Île-de-France



Appel à manifestation d'intérêt relatif à l'achat de prestations dites de « Diagnostics de maturité cyber des PME d'Ile-de-France »

Contrat de subvention DIGITAL n° 101083769

Date de début du projet : 01/01/2023

Durée du projet : 42 mois

Auteur : Hubert Loiseau

Ce projet est co-financé par l'Union Européenne via le programme DIGITAL		
Niveau de diffusion		
PU	Public	x
SEN	Limité dans les conditions prévues par le contrat de subvention	
RE	Restreint à un groupe spécifié par le consortium qui inclut les services de la Commission Européenne et de la Région Île-de-France	
CO	Confidentiel, diffusé seulement aux membres du consortium, services de la Commission Européenne et de la Région Île-de-France inclus.	



Achat de prestations de « Diagnostics de maturité cyber des PME d'Ile-de-France »

Le présent AMI vise à solliciter des sociétés de conseil & audit en cybersécurité à même de réaliser des prestations d'audit cyber au profit de PME accompagnées dans le cadre du programme CYBIAH. Cet AMI vise à retenir les deux sociétés les plus pertinentes afin de réaliser ces prestations de diagnostic.

Le Campus Cyber porte le projet CYBIAH, European Digital Innovation Hub, sous forme d'un parcours d'accompagnement, visant à renforcer le niveau de cybersécurité des PME et Collectivités de l'Ile de France.

Le parcours proposé aux PME et Collectivités de l'Ile de France comprend plusieurs phases :

- Embarquement
- Diagnostic
- Services et solutions
- Ingénierie financière

La seconde phase du dispositif, « **diagnostic** », **objet du présent AMI**, 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 sécurisation », 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 de la PME ou de la collectivité.

Cet AMI vise à appuyer les équipes CYBIAH d'un dispositif humain capable de réaliser un grand nombre de diagnostics/audit cyber au sein de nombreuses PME de la région Ile-de-France. **CYBIAH a pour objectif d'accompagner 150 PME à horizon mi-2026.**

Les diagnostics de maturité seront réalisés, sur la durée de la consultation de septembre 2024 à juin 2026, sur la base d'un **volume estimatif** de :

- 50 unités de niveau argent
- 40 unités de niveau or



1. Prestations attendues

1.1 Réalisation d'un diagnostic de maturité cyber - PME/TPE niveau « argent » - (UO-DIAG-ARGENT)

Cette prestation consiste en la réalisation d'un diagnostic de maturité cyber d'une PME (bénéficiaire) nécessitant la présence du titulaire sur site en région Ile-de-France.

1.1.1 Périmètre

Cette prestation vise des PME et collectivités territoriales **ne disposant pas de tous les premiers réflexes d'hygiène de sécurité numérique** et qui nécessitent d'approfondir l'évaluation de leur maturité sur une vision dite « 360° » dans un contexte de **structure de taille intermédiaire**.

Le niveau retenu sera défini par l'équipe CYBIAH après la réunion d'embarquement. Les critères retenus pour identifier si une structure relève d'un diagnostic argent ou or sont :

- Note issue de l'évaluation de la surface externe de l'entreprise ;
- Besoins de sécurité de l'entreprise ;
- Complexité du système d'informations.

1.1.2 Description de la prestation attendue

Il est attendu de la part du sous-traitant la réalisation des actions suivantes :

1. Rencontres avec les parties prenantes au cours d'une réunion d'embarquement **(1/ 2 jour)** :
 - Rencontre du gérant de la structure (1 à 2 heures)
 - Rencontre du responsable informatique (s'il existe) et du prestataire en charge de la gestion du parc informatique (s'il existe)
 - Rencontre du responsable cyber (s'il existe)
 - Objectif :
 - Compréhension du périmètre métier de la structure, des risques auxquels elle fait face, des besoins de sécurité et de la stratégie d'entreprise (développement, marchés à conquérir, concurrents, partenaires stratégiques).
 - Identification des « macro » actifs informatiques de la structure (cartographie DSI)
2. Déroulé du questionnaire de maturité **(1 jour)** sur la base d'un référentiel de maturité inspiré du guide d'hygiène numérique de l'ANSSI¹ (environ 70 questions).
3. Déroulé du questionnaire « DMA » (digital maturity assesment) sur la base du référentiel européen fourni en annexe 3 (1 heure).
4. Rédaction d'un rapport dit « plan de sécurisation » accompagné d'un support de présentation proposant des mesures couvrantes, le cas échéant, les aspects suivants **(2 jours)** :
 - Techniques

¹ <https://cyber.gouv.fr/publications/guide-dhygiene-informatique>



- Organisationnels
 - Formations
5. Débriefing du rapport de sécurisation à l'attention du dirigeant de la structure accompagnée (1/2 jour)

1.1.3 Délais de réalisation

Un diagnostic argent est réalisé par le titulaire sur un planning de deux semaines au maximum, en fonction de la disponibilité de la structure diagnostiquée.

Le titulaire propose un planning de réalisation selon son estimation et valide ce planning avec CYBIAH.

Le délai de réalisation court à partir de la date de réalisation de la réunion d'embarquement.

1.1.4 Réalisation

La prestation est forfaitaire mais les heures de présence des consultants doivent être également consignées par émargement afin de s'assurer du bon respect des contraintes de sécurité du site.

En fonction de la durée des travaux, un suivi régulier devra être mené avec le responsable de projet CYBIAH afin :

- De valider le bon avancement de la prestation
- D'identifier les risques ou les difficultés pouvant survenir en phase de diagnostic
- De mettre en œuvre les actions correctives pour garantir d'une part, la bonne délivrance des livrables, et d'autre part, la qualité et l'adéquation de la prestation avec le besoin initial.

1.1.5 Synthèse diagnostic argent

Intitulé
{UO-DIAG-ARGENT} - Réalisation d'un diagnostic de maturité cyber – PME niveau « argent »
Livrables attendus
Questionnaire de maturité cyber complété Questionnaire « DMA » complété Rapport « plan de sécurisation » Support de présentation de la réunion de restitution CR de la réunion de restitution Cartographie DSI
Charge estimée
4 jours / homme
Délai de réalisation



2 semaines

1.2 Réalisation d'un diagnostic de maturité cyber – PME niveau « or » - (UO-DIAG-OR)

Cette prestation consiste en la réalisation d'un diagnostic de maturité cyber d'une PME, TPE (bénéficiaire) nécessitant la présence du titulaire sur site en région Ile-de-France.

1.2.1 Périmètre

Cette prestation vise des PME/TPE et collectivités territoriales **disposant déjà des premiers réflexes d'hygiène de sécurité numérique** et qui nécessitent d'approfondir l'évaluation de leur maturité sur une vision dite « 360° » dans un contexte de structure **de taille importante** et nécessitant un temps d'investigation plus poussé que pour un diagnostic argent. Cette catégorie vise à accompagner des sociétés assujetties aux directives NIS ou NIS2 prochainement, voire à d'autres réglementations (DORA, CRA notamment).

Le niveau retenu sera défini par l'équipe CYBIAH après la réunion d'embarquement. Les critères retenus pour identifier si une structure relève d'un diagnostic argent ou or.

1.2.2 Description de la prestation attendue

Il est attendu de la part du sous-traitant la réalisation des actions suivantes :

1. Rencontres avec les parties prenantes **(1/2 jour)** :
 - Rencontre du gérant de la structure (1 à 2 heures)
 - Rencontre du responsable informatique (s'il existe) et du prestataire en charge de la gestion du parc informatique (s'il existe) (2 heures)
 - Rencontre du responsable cyber (s'il existe) (2 heures)
 - Objectif :
 - Compréhension du périmètre métier de la structure, des risques auxquels elle fait face, des besoins de sécurité et de la stratégie d'entreprise (développement, marchés à conquérir, concurrents, partenaires stratégiques).
 - Identification des « macro » actifs informatique de la structure (cartographie DSI)
2. Déroulé du questionnaire de maturité **(2 jours)** sur la base d'un référentiel de maturité inspiré du guide d'hygiène numérique de l'ANSSI² (environ 70 questions).
3. Optionnel : réalisation d'un pentest technique en boîte blanche sur les infrastructures du bénéficiaire **(3 jours maximum)** comprenant :
 - Une évaluation de la configuration réseau et des actifs exposés (scan nmap)

² <https://cyber.gouv.fr/publications/guide-dhygiene-informatique>



- Un scan actif du réseau afin d'identifier des composants vulnérables (scanner de vulnérabilités de type openvas, nessus ou autre)
 - Un audit de la configuration de l'annuaire Active Directory le cas échéant (via un outil de type PingCastle, Purple Knight, etc)
 - Evaluation de la sécurité de l'environnement cloud (O365 ou google workspace)
4. Déroulé du questionnaire « DMA » (digital maturity assesment) sur la base du référentiel européen fourni en annexe 3 (1 heure).
 5. Rédaction d'un rapport dit « plan de sécurisation » accompagné d'un support de présentation proposant des mesures couvrant, le cas échéant, les aspects suivants (**3 jours**) :
 - Techniques
 - Organisationnels
 - Formations
 6. Débriefing du rapport de sécurisation à l'attention du dirigeant de la structure accompagnée (**1/2 jour**)

1.2.3 Délais de réalisation

Un diagnostic argent est réalisé par le titulaire sur un planning de deux semaines au maximum, en fonction de la disponibilité de la structure diagnostiquée.

Le titulaire propose un planning de réalisation selon son estimation et valide ce planning avec CYBIAH.

Le délai de réalisation court à partir de la date de réalisation de la réunion d'embarquement.

1.2.4 Réalisation

La prestation est forfaitaire mais les heures de présence des consultants doivent être également consignées par émargement afin de s'assurer du bon respect des contraintes de sécurité du site.

En fonction de la durée des travaux, un suivi régulier devra être mené avec le responsable de projet CYBIAH afin :

- De valider le bon avancement de la prestation
- D'identifier les risques ou les difficultés pouvant survenir en phase de diagnostic
- De mettre en œuvre les actions correctives pour garantir d'une part, la bonne délivrance des livrables, et d'autre part, la qualité et l'adéquation de la prestation avec le besoin initial.

1.2.5 Synthèse diagnostic or

Intitulé
{UO-DIAG-OR} - Réalisation d'un diagnostic de maturité cyber – PME niveau « or »
Livrables attendus



Questionnaire de maturité cyber complété Questionnaire « DMA » complété Rapport « plan de sécurisation » Support de présentation de la réunion de restitution CR de la réunion de restitution Cartographie DSI Option : rapport de pentest
Charge estimée
6 jours / homme + 3 jours/ homme de pentest en option
Délai de réalisation
3 semaines

1.3 Prestation d'initialisation du contrat - (UO-INIT)

Cette prestation consiste en la réalisation d'un atelier d'une journée en présentiel au Campus Cyber à Puteaux afin de présenter les enjeux du contrat, la méthodologie utilisée par CYBIAH ainsi que la définition des modalités d'échange et de collaboration entre les équipes Campus Cyber et le titulaire du contrat. Cette prestation sera réalisée entre les équipes CYBIAH et le directeur du projet du titulaire.

Cette prestation est forfaitaire et ne sera réalisée qu'une seule fois pour toute la durée du contrat au démarrage de la prestation globale.

1.3.1 Synthèse initialisation

Intitulé
{UO-INIT} - Prestation d'initialisation du contrat
Livrables attendus
CR de la réunion de restitution
Charge estimée
1 jour / homme

1.4 Prestation de pilotage du contrat - (UO-COPIL)



Cette prestation consiste en la réalisation d'un comité de pilotage du contrat afin d'assurer le suivi des différents diagnostics réalisés par le titulaire. Elle a pour objectif :

- De donner de la visibilité au titulaire sur les prochaines échéances et les prochains bénéficiaires à embarquer
- De suivre les prestations réalisées, leur état d'avancement et la qualité des rendus
- D'assurer le suivi financier du contrat.

Cette unité d'œuvre sera réalisée de manière périodique à raison d'une réunion par mois au minimum et se tiendra en visioconférence Teams.

Une fois par trimestre, elle aura lieu en présentiel au Campus Cyber à Puteaux.

1.4.1 Synthèse initialisation

Intitulé
{UO-COPIL} - Prestation de pilotage du contrat
Livrables attendus
CR de la réunion de pilotage
Charge estimée
0,5 jour / homme



2. Exigences

2.1 Exigences techniques

2.1.1 DIAG_REFERENTIEL_001

Les intervenants seront à même de réaliser un diagnostic de cybersécurité d'une entreprise de type PME sur la base des thèmes fournis en annexe 2.

2.1.2 DIAG_REFERENTIEL_002

Les intervenants démontreront une capacité à réaliser des audits de cybersécurité organisationnels et mettront en avant leurs formations, les méthodologies qu'ils maîtrisent ainsi que les capacités techniques de pentest éventuelles.

2.1.3 DIAG_REFERENTIEL_003

Les intervenants démontreront une expérience dans la réalisation de diagnostics de maturité cyber, en mettant en avant des références passées.

2.1.4 DIAG_REFERENTIEL_004

Les intervenants mettront en avant toutes les certifications, labels ou formations éventuelles dont ils bénéficient (ISO27001, CIS, SANS, CISSP, CISM, PASSI...).

2.1.5 DIAG_REFERENTIEL_005

Les intervenants seront suffisamment acculturés aux innovations relatives à l'intelligence artificielle afin d'identifier au cours de la réalisation du diagnostic si la structure bénéficiaire est susceptible de nécessiter un accompagnement pour la mise en place de technologies de ce type et veillera à remonter cette information au responsable de projet CYBIAH. Toute formation ou expérience réalisée au contact de ces technologies seront valorisés dans la réponse du candidat.

2.1.6 DIAG_REFERENTIEL_006

Les sociétés candidates devront obligatoirement mettre en avant la présence de plusieurs profils à même de réaliser des diagnostics de conformité relatifs aux nouvelles réglementations cyber en vigueur : DORA, NIS2, CRA.

Les candidats mettront également en avant leur capacité à se former sur de nouvelles réglementations qui pourraient entrer en vigueur durant la période d'exécution du contrat.

2.1.7 SECU_NUMERIQUE_001

En vue de prévenir le vol des données de l'Acheteur contenues dans les postes de travail nomade du Titulaire, celui-ci met systématiquement en place les mesures de protection suivantes :

- Câbles antivols et filtre de confidentialité ;



- Installation d'une solution de chiffrement surfacique nécessitant de préférence une authentification forte pour le déchiffrement.

2.1.8 SECU_NUMERIQUE_002

Le Titulaire applique une durée de verrouillage automatique de session sur l'ensemble des postes qu'il met à disposition de ses personnels. Cette durée ne doit pas excéder 15 minutes.

2.1.9 SECU_NUMERIQUE_003

Le Titulaire doit privilégier l'authentification forte pour tout déverrouillage de session des postes de travail utilisés au cours de la prestation, ou à défaut, un mot de passe de complexité et longueur suffisante (minimum 8 caractères).

2.1.10 SECU_NUMERIQUE_004

Le Titulaire rend obligatoire l'utilisation de l'authentification forte (ex. carte à puce, token usb, TOTP...) au poste de travail utilisé pour l'administration technique des systèmes de l'Acheteur.

2.1.11 SECU_NUMERIQUE_005

Tous les postes de travail du Titulaire doivent disposer d'une solution de chiffrement robuste, qualifiée par l'ANSSI afin de permettre le chiffrement des données sensibles de l'Acheteur que les personnels du Titulaire seraient amenés à stocker ou communiquer dans le cadre de leurs missions.

2.1.12 SECU_NUMERIQUE_006

Le Titulaire s'assure de la bonne installation et mise à jour d'un logiciel EDR sur tous les postes de travail dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un poste de travail utilisé dans le cadre de la prestation devra avoir été préalablement validée par l'Acheteur.

2.1.13 SECU_NUMERIQUE_007

Le Titulaire contacte les interlocuteurs sécurité de l'Acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'Acheteur. Si cet incident a lieu sur le SI du Titulaire, le Titulaire autorisera l'Acheteur ou un tiers désigné à participer au traitement de l'incident (si l'Acheteur le souhaite).

2.1.14 SECU_NUMERIQUE_008

Le Titulaire conserve et traite les données de l'Acheteur de manière séparée de ses propres données ou de données d'autres clients du Titulaire. Le Titulaire doit restreindre l'accès aux données de l'Acheteur suivant le principe de restriction au besoin d'en connaître. L'Acheteur doit donner ses performances dans sa réponse technique : droits d'accès, machines virtuelles séparées, disques séparés, machines physiques séparées.

2.1.15 SECU_NUMERIQUE_009



Le Titulaire garantit que les modalités de stockage et d'échanges d'informations permettent d'en assurer la confidentialité et l'intégrité.

2.2 Exigences projet

2.2.1 ASSURANCE_RC_001

Le prestataire doit souscrire à une assurance de responsabilité civile professionnelle ou RC Pro qui couvre le champ d'activité de la présente consultation. L'attestation d'assurance doit mentionner clairement que les interventions sur les SI des clients du prestataire sont couvertes. Le prestataire peut également souscrire à une assurance spécifique cyber couvrant son propre système d'information.

2.2.2 PROJET_COMITO_001

Le prestataire propose une comitologie de suivi de la prestation adaptée.

2.2.3 PROJET_RESSOURCES_001

Le prestataire assure une capacité à remplacer les ressources défaillantes ou indisponibles, temporairement ou de manière définitive afin d'assurer la continuité d'exécution de la prestation.

2.2.4 PROJET_RESSOURCES_002

Le titulaire assure avoir réalisé les diligences nécessaires des intervenants du projet afin de garantir la sureté de la prestation (vérifications légales) et la sureté des bénéficiaires CYBIAH. Le titulaire présente dans la réponse un processus permettant de décrire les diligences réalisées.

Le Titulaire effectue les enquêtes sur le casier judiciaire (demande du bulletin n°3) de tous les personnels du Titulaire amenés à intervenir dans le cadre du contrat. Aucun personnel ne doit intervenir sur le périmètre de l'Acheteur sans une vérification préalable de ses antécédents Judiciaire. Le Titulaire doit être en mesure d'apporter la preuve de la gestion de ces opérations de contrôles. Un personnel présentant des antécédents judiciaires incompatibles avec les enjeux des activités de l'Acheteur, est récusé par défaut.

2.2.5 DOC_CHARTE_001

Les documents rédigés devront respecter la charte graphique de CYBIAH.

2.2.6 DOC_CHARTE_002

Les documents rédigés devront respecter la charte de rapport d'audit (mise en forme, parties, titres, etc).

2.2.7 HUM_POSTURE_001

Bien que la réalisation des diagnostics au sein des structures bénéficiaires du programme CYBIAH puisse s'apparenter à des audits de sécurité, ces prestations doivent conserver un



caractère et une démarche volontaire de la part du bénéficiaire et ne saurait être assimilé à un audit. Le Titulaire veille à adopter une posture bienveillante, constructive et d'accompagnement et de conseil plutôt que de contrôle.



3. Modalités de la consultation

3.1 Critères d'évaluation

Les critères d'évaluation des propositions seront les suivants :

- Conformité aux exigences fonctionnelles et techniques spécifiées dans le document Excel joint
- La pertinence et l'étendue des dimensions prises en compte,
- Représentativité et exploitabilité du score,
- Qualité de la teneur du rapport et des recommandations émises,
- Rapport qualité prix et cohérence des coûts proposés avec l'évolution de la demande,
- Méthodologie proposée incluant le plan de projet, les ressources humaines et les processus de gestion des incidents

Une commission d'achat sera réunie pour noter les réponses.

3.2 Documents de réponse

Les répondants devront fournir :

Un mémoire de réponse contenant au moins :

- Un descriptif exhaustif de l'entreprise répondant à l'appel d'offre (taille localisation, descriptif de l'expertise technique de l'entreprise, références client)
- La réponse aux exigences renseignées dans l'annexe 1 Exigences
- La proposition financière renseignée dans l'annexe 5 BPU
- Présenter les références de mission réalisées en lien avec la cybersécurité de PME en précisant pour chacune :
 - les dates de réalisation,
 - l'objet de la prestation,
 - le client (si confidentiel, a minima nombre de salariés et activité),
 - le périmètre de la prestation,
 - les intervenants dans votre structure,
 - la méthodologie appliquée,
 - les principaux résultats obtenus.
- La méthodologie envisagée pour la réalisation des diagnostics,
- Les profils envisagés pour le pilotage du projet et la réalisation des diagnostics,
- Un plan d'assurance qualité afin de garantir la qualité de la prestation durant toute la durée du contrat,
- L'attestation d'assurance responsabilité civile professionnelle.

Le document de réponse ne pourra pas excéder un nombre de page égal à 30 (hors annexe 1 et 5).

3.3 Proposition financière

Les prestataires devront fournir une proposition financière détaillée comprenant les prix et leur structure, pour chacune des unités d'œuvre, les modalités de paiement telles que le calendrier des paiements et les méthodes de facturation acceptées, les échéanciers et toute autre information pertinente.



3.4 Grille d'analyse des offres

La commission d'achat a mis en place une grille d'analyse des offres qui attribue des points aux différents critères d'évaluation, tels que le prix, la qualité, la conformité aux spécifications, les délais, etc. Les membres de la commission évalueront les offres en utilisant la grille d'analyse. Une réunion de la commission sera organisée pour discuter des évaluations et attribuer un score global à chaque offre.

Les offres seront jugées au regard de deux critères : un critère prix et un critère qualité.

3.4.1 Critère prix

L'offre du candidat présentant le prix minimal obtient la note maximale de 100 pour le critère prix. Les autres offres des candidats x sont évaluées en rapport de prix pour la référence maximale par la formule suivante :

Note au critère prix(x) = (Prix de l'offre minimale / Prix de l'offre(x)) x 100

3.4.2 Critère qualité

Le critère qualité est composé de deux sous-critères :

- **Technique**
 - o Adéquation de l'offre proposée par le candidat aux besoins de CYBIAH, permettant ainsi de répondre aux exigences concernant :
 - La qualité et l'expertise du dispositif proposé,
 - Les éventuelles certifications ou garanties de sécurité proposées,
 - La compréhension des enjeux de la consultation,
 - La capacité de la solution proposée à répondre au besoin formulé,
 - L'organisation du dispositif et son adéquation à la structure CYBIAH,
 - La sécurité de l'environnement technique du titulaire.
- **Projet**
 - o Adéquation de l'offre proposée par le candidat aux de CYBIAH, permettant ainsi de répondre aux exigences concernant :
 - La qualité des livrables ;
 - La qualité des documentations ;
 - La qualité du pilotage et de la méthodologie.

Pour chaque exigence, une note de 0 à 2 est attribuée à chaque candidat :

- 0 : le critère n'est pas satisfait
- 1 : le critère est partiellement satisfait
- 2 : le critère est entièrement satisfait

Chaque exigence dispose d'un coefficient de pondération :

- 1 : l'exigence est dispensable
- 2 : l'exigence est préférable
- 3 : l'exigence est indispensable

Sur la base de la somme des points attribués au candidat pour chaque exigence, une note au sous critère est attribuée.

3.4.3 Note finale attribuée au candidat

La note globale attribuée au candidat est composée des deux sous-critères décrits précédemment.



Tout candidat ayant obtenu une note inférieure à 30/100 à un des sous-critères est rejeté d'office de la sélection.

3.5 Modalité d'attribution

CYBIAH retiendra deux offreurs de services dans le cadre de cet AMI.

Les deux offreurs les mieux notés seront retenus dans **un mode d'attribution à la discrétion du programme CYBIAH** pour chacun des 90 diagnostics à réaliser.

En cas de défaillance de l'un des candidats retenus, le candidat arrivé 3^{em} à la notation finale sera sollicité pour s'y subsister et ainsi de suite.

3.6 Calendrier de l'appel d'offres

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

- Publication de l'appel d'offres : 2 septembre 2024
- Date limite d'envoi de questions : 13 septembre 2024
- Date limite de réception des propositions : 1^{er} octobre 2024
- Sélection du prestataire retenu et communication des résultats : 29 octobre 2024

3.7 Méthode de communication & de candidature

Les candidatures doivent être envoyées à l'adresse **contact@cybiah.eu**

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**

3.8 Conditions contractuelles

Le contrat sera régi par les termes et conditions générales spécifiés dans les documents contractuels fournis aux prestataires retenus. Les principales clauses contractuelles incluront les points suivants :

3.8.1 Obligations en termes d'assurance

Le prestataire doit disposer d'une assurance couvrant sa responsabilité civile professionnelle. Une attestation devra être fournie dans le mémoire de réponse.

3.8.2 Obligation de conseil et d'information

Le prestataire a un devoir de conseil s'il se rend compte, lors de ses interventions, de dysfonctionnements potentiels au titre de ses prestations. Ce devoir de conseil est formel et fondé sur la production d'un rapport mensuel qui décrit les risques et menaces et propose des actions pour les réduire le cas échéant. Le prestataire est tenu de signaler à l'acheteur tous les éléments qui lui paraissent de nature à compromettre la bonne exécution des prestations

3.8.3 Procédures de résiliation du contrat



Le contrat est renouvelé par tacite reconduction entre l'année 1 et l'année 2. Il sera remis en concurrence à l'issue des 24 mois d'exécution. En cas de non-exécution par le prestataire de tout ou partie de l'une quelconque de ses obligations contractuelles, CAMPUS CYBER pourra résilier de plein droit le Contrat dans un délai d'un (1) mois suivant la date de mise en demeure de l'Utilisateur indiquant ses manquements, notifiée par lettre recommandée avec accusé de réception et restée sans effet. Le Contrat peut être résilié par CAMPUS CYBER dans le cas où le prestataire a violé une ou plusieurs obligations essentielles au Contrat, notamment les stipulations relatives à la confidentialité, la Propriété Intellectuelle, l'utilisation malveillante du Service, à réception d'une lettre recommandée avec accusé réception et sans mise en demeure préalable. En cas de résiliation, chaque Partie sera déliée envers l'autre de toutes obligations dues au titre de l'exécution du Contrat, à l'exception de celles relatives à la confidentialité, à la responsabilité et la Propriété Intellectuelle. Enfin, en cas de redressement judiciaire ou de liquidation judiciaire du prestataire, le présent contrat pourra être résilié de plein droit par CAMPUS CYBER, sauf décision contraire de l'administrateur, telle que prévue à l'article L. 622-13 du code de commerce.

3.8.4 Gestion des litiges et règlement des différends

Les litiges découlant de l'interprétation et/ou de l'application du Contrat sont soumis à la loi française. Il en est ainsi pour les règles de fond comme pour les règles de forme. En cas de litige, les lois des pays où se trouvent les serveurs virtuels ne s'appliquent pas et le Contrat reste soumis au droit français. En cas de rédaction du Contrat en plusieurs langues ou de traduction, la version française prévaut. Pour l'exécution des présentes, les Parties font respectivement élection de domicile en leurs sièges sociaux indiqués en première page. Toute modification du siège social ou de l'adresse de l'une des Parties ne sera opposable à l'autre Partie que huit (8) jours calendaires après le lui avoir été dûment notifiée. Les Parties conviennent de considérer les messages électroniques et plus généralement les documents électroniques échangés entre elles sous forme électroniques au sens de l'article 1366 du code civil, comme des écrits d'origine. Chaque Partie s'interdit de modifier le contenu des messages électroniques qu'elle a reçus ou émis. Chacune des Parties informera l'autre Partie de tout manquement aux obligations contractuelles commis par cette dernière, dès que ce manquement aura été découvert. En cas de difficulté pour l'interprétation et/ou à l'exécution du présent Contrat ou l'un de ses avenants, les Parties s'engagent, dans un premier temps, à coopérer avec diligence et bonne foi en vue de trouver une solution amiable à leur différend. A cet effet, dès qu'une Partie identifiera un différend avec l'autre 8 Partie, elle demandera la convocation d'une réunion ad hoc des responsables de chaque Partie, afin de discuter du règlement de la question objet du différend. Cette convocation sera effectuée par courrier recommandé avec accusé-réception. Cette réunion se tiendra dans un délai maximal de quinze (15) jours à compter de la date d'envoi de la demande. Faute d'un tel règlement amiable, tout litige éventuel qui n'aurait pas été réglé dans un délai de trente (30) jours à compter de la date d'envoi de la demande de réunion sera porté par la partie la plus diligente devant le tribunal de commerce de Paris auquel les parties attribuent compétence exclusive nonobstant pluralité des défendeurs ou appel en garantie. Restitution des données à la fin du contrat. À la fin du contrat, le prestataire s'engage à restituer toutes les données qui lui ont été confiées par le client dans le cadre de la prestation de services informatiques. Les données comprennent, mais ne se limitent pas à, tous les fichiers, documents, bases de données, logiciels, codes sources, éléments multimédias, et toute autre information ou matériel numérique associé à la prestation de services informatiques. La restitution des données doit être effectuée dans un format standardisé, aisément utilisable et transférable vers d'autres systèmes ou environnements informatiques, conformément aux normes de l'industrie en vigueur. Le prestataire garantit que toutes les données restituées seront complètes, exactes et exemptes de toute altération, suppression ou modification non autorisée. La restitution des données doit



être effectuée dans les 20 jours suivant la résiliation ou l'expiration du contrat. Le prestataire s'engage à maintenir la confidentialité des données pendant toute la durée du contrat et après sa résiliation, conformément aux clauses de confidentialité et de protection des données spécifiées dans le contrat. Le prestataire doit également s'assurer que toutes les copies ou sauvegardes des données effectuées pendant la prestation de services informatiques sont supprimées de manière sécurisée et irréversible, conformément aux meilleures pratiques de l'industrie.

Le prestataire s'engage à mettre en œuvre les moyens appropriés afin de garder confidentiels les informations, les documents et les objets auxquels il aura eu accès lors de l'exécution du marché, sans qu'il soit besoin d'en expliciter systématiquement le caractère confidentiel. Une attention particulière est portée sur l'hébergement des données récoltées. Un hébergement SECNUMCLOUD est à privilégier. Cependant, le prestataire peut proposer d'autres solutions techniques en produisant des éléments d'architecture. Il peut proposer différentes solutions avec différents prix. Les informations, documents ou objets ne peuvent être, sans autorisation expresse de l'acheteur, divulgués, publiés, communiqués à des tiers ou être utilisés directement par le 9 prestataire, hors du marché ou à l'issue de son exécution. Le prestataire s'engage à faire respecter ces obligations à l'ensemble de son personnel, le cas échéant à ses sous-traitants et fournisseurs. L'acheteur peut demander, à tout moment, au prestataire, de lui retourner ou de détruire les éléments ou supports d'informations confidentielles qui lui auraient été fournis. La violation grave des obligations de confidentialité par le prestataire peut entraîner la résiliation du marché aux torts du titulaire. Le prestataire s'interdit toute publication relative à sa mission quel que soit le support et quelle que soit la destination, sans l'accord préalable écrit de l'acheteur.

- Le titulaire s'engage à faire respecter ces dispositions par toute personne qui interviendrait directement ou indirectement pour son propre compte.

- Le titulaire reconnaît avoir été avisé que toute divulgation d'information confidentielle est susceptible de tomber sous le coup de l'article 226-3 du Code Pénal. Le prestataire, et le cas échéant ses sous-traitants, est tenu de respecter la réglementation en vigueur applicable au traitement des données à caractère personnel et notamment le règlement (UE) 2016/679 du Parlement européen, dit Règlement Général sur la Protection des Données (RGPD), relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le prestataire assure ne faire un autre usage des données que celui nécessaire à l'exécution du marché. Il ne peut en aucun cas transmettre ou utiliser ces données à titre commercial sous peine de résiliation du marché aux torts du prestataire.



4. Annexes

Annexe 1 : Liste des exigences

Voir fichier **Annexe 1 - Exigences.xlsx**

Annexe 2 : Liste des thématiques abordées au cours des diagnostics

Thèmes évalués au cours du diagnostic :

- Niveau de formation des équipes IT (interne ou prestataires) sur le sujet Cyber
- Niveau de sensibilisation des utilisateurs sensibles du SI
- Niveau de sensibilisation des utilisateurs classiques du SI
- Organisation de la sensibilisation des utilisateurs par l'entreprise
- Existence d'un porteur du sujet Cybersécurité au sein de la direction / du management
- Rôles et les responsabilités en matière de cybersécurité
- Approche des risques incluant les risques cyber
- Outillage et pilotage des indicateurs Cyber
- Gestion de la sécurité dans les projets et développements
- Formalisation de l'architecture du SI
- Existence d'un inventaire des applications
- Existence d'un inventaire des données
- Identification des informations et outils sensibles
- Inventaire des utilisateurs et droits
- Comptes individuels
- Comptes techniques
- Procédure entrée / sortie / changement de poste
- Politique de MDP
- Sécurisation des accès sensibles / VPN, 2FA
- Gestion des certificats
- Gestion des dérogations d'accès
- Sécurisation physique des postes
- Durcissement du système et chiffrement - Postes utilisateur
- Lutte contre les logiciels malveillants
- Décommissionnement des postes
- Sauvegarde des postes
- Sécurisation des éléments IoT / produits connectés
- Firewall & outils de contrôle
- Réseau et cloisonnement
- Messagerie
- WiFi
- Accès Web
- Sécurité physique des infrastructures
- Durcissement du système et chiffrement - Serveurs
- Lutte contre les logiciels malveillants - Serveurs
- Décommissionnement des infrastructures



- Sauvegarde des serveurs
- Sécurité des sauvegardes
- Réseau administrateur
- Accès et outils d'administration sur les postes et serveurs
- Accès d'administration à distance
- Nomadisme & Télétravail
- Shadow IT
- BYOD & Smartphone
- Lutte contre les fuites de données
- Politique de mise à jour : OS
- Politique de mise à jour : Applicatifs
- Abonnements à des flux d'informations sur les vulnérabilités découvertes
- Supervision & journalisation
- Security Operation Center
- Audit / PenTesting
- Préparation à la crise
- Politique de sauvegarde
- Test de restauration
- Continuité et Reprise d'activité

Thèmes optionnels selon la structure :

- Maîtrise des risques liés à l'infogérance et aux prestations SI
- Identification des tiers critiques
- Gestion des paiements et données fournisseurs
- Stratégie d'hébergement Cloud
- Stratégie de sécurisation Cloud
- Gouvernance Cloud
- Gestion des fournisseurs Cloud
- Sauvegarde Cloud
- Résilience Cloud
- Administration Cloud
- Protection des services Cloud
- Gouvernance OT
- Cartographie OT
- Sécurité projets OT
- Réseau OT
- Gestion des accès OT
- Protection SI industriels
- Dérogations OT
- Supervision, détection et réaction OT
- Sauvegarde et résilience OT
- Fiabilité et sécurité des bibliothèques externes
- Intégration les pratiques DevSecOps dans vos projets d'IA



- Interdiction de l'utilisation automatisée de systèmes d'IA pour des actions critiques sans supervision humaine
- Source de données utilisées pour l'entraînement
- Sensibilisation sur les risques liés au code source généré par l'IA
- Journalisation de l'ensemble des traitements réalisés au sein du système d'IA
- Protection des interactions entre IA et applications métiers
- Protection de l'IA en filtrant les entrées et les sorties des utilisateurs
- Administration sur le système d'IA

Annexe 3 : Questionnaire DMA

Voir fichier **Annexe 3 – DMA.xlsx**

Annexe 4 : Modèle de rapport de diagnostic

01	RAPPEL DU CADRE	04	RADAR DE MATURITÉ CYBER	07	ELABORATION DU PLAN D' ACTIONS
02	SYNTHÈSE DU DIAGNOSTIC	05	CONSTATS ET RECOMMANDATIONS	08	RECOMMANDATIONS TECHNIQUES
03	CARTOGRAPHIE DE L'EXISTANT	06	PRÉPARATION À LA GESTION DE CRISE CYBER		

Annexe 5 : Bordereau de prix unitaire

Voir fichier **Annexe 5 - BPU.xlsx**