



CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Marché n°2025-0083-00-00 MPA

Acheteur

Numih France

GIP mipih

12 rue Michel Labrousse

CS 93668

31036 Toulouse Cedex 1

Siret n° 18310021300028

Acquisition et maintenance des licences Cyberwatch

NB : Tout comme l'ensemble des documents de la consultation, le présent document ne peut être modifié à l'initiative du Titulaire.

SOMMAIRE

Article 1. Objet du marché	3
Article 2. Présentation de Numih France	3
Article 3. Description du besoin	3
3.1 Distribution	4
3.1.1 E1 – Partenaire agréé	4
3.1.2 E2 – Notification de renouvellement	4
3.1.3 E4 – Délai de livraison / activation des licences	4
3.1.4 E5 – Type de licence	4
3.1.5 E6 – Prestations supplémentaires	4
3.2 Support.....	4
3.2.1 E7 – Capacité à faire du support technique	4
3.2.2 E8 – Délai de réponse du support.....	5
3.2.3 E9 – Lien avec l’éditeur.....	5
3.2.4 E10 – Suivi récurrent	5
3.3 Maintenance	5
3.3.1 E11 – Notifications proactives.....	5
3.3.2 E12 – Suivi des bulletins de sécurité de l’éditeur	5
3.3.3 E13 – Mise à disposition de la documentation	5
Article 4. Environnement d’exécution du marché	6
4.1 Environnement technique	6
4.2 Environnement applicatif	6
Article 5. Support et engagement du Titulaire.....	7
5.1 Niveau d’engagement en cas d’incident	7
5.2 Maintenance.....	7
Article 6. Gestion des données à caractère personnel	7

Article 1. Objet du marché

La présente consultation a pour objet la mise en concurrence de distributeurs agréés pour l'acquisition de licences du logiciel Cyberwatch ainsi que pour les prestations associées (maintenance, support, accompagnement, etc.).

La présente procédure vise à retenir le distributeur qui fournira les licences, et les services associés, aux meilleures conditions techniques, financières et contractuelles.

Article 2. Présentation de Numih France

Numih France est une structure publique de coopération inter-hospitalière spécialisée dans l'informatique, travaillant avec des établissements de santé répartis sur l'ensemble du territoire (Centres Hospitaliers Universitaires, Centres Hospitaliers, Établissements de Santé Privés d'Intérêt Collectif, Hôpitaux locaux, Maison de retraite, Établissement d'hébergement pour personnes âgées dépendantes, Établissements de santé privés d'intérêt collectif...).

Éditeur de progiciels hospitaliers et de santé sur des domaines complémentaires s'appuyant sur des dizaines d'années d'expérience, et hébergeur de données de santé certifié depuis 2018, Numih France accompagne les établissements de santé dans la construction et le développement de leur système d'information.

Article 3. Description du besoin

La solution de gestion des vulnérabilités est imposée, il s'agit de Cyberwatch.

Cette solution de gestion des vulnérabilités est utilisée à Numih France pour le scan des vulnérabilités des serveurs à sa charge. Cette solution doit être et est hébergée dans les datacenters de Numih France.

Pour se faire, cette solution :

- Se connecte via divers protocoles sur les serveurs : SSH, WinRM, SNMP
- Se connecte via un agent sur les serveurs et poste de travail.
- Liste l'ensemble des technologies et applications installées
- Fait la corrélation entre les technologies et applications installées avec une base de connaissances des vulnérabilités alimenter de différentes sources telles que les bases de vulnérabilités CVE et EUVD.

La solution, est également capable, via l'option de « Conformité » de réaliser des scans de configuration sur les serveurs supervisés en fonction de différents référentiels comme le CIS Benchmark ou le CERTFR_AD.

La solution, permet tagguer les actifs, de leur assigner un groupe.

Elle permet également de réaliser des tableaux de bord et de statistiques personnalisés sur les actifs supervisés, et notamment en fonction des tags/groupes.

L'authentification des utilisateurs se réalise avec un fournisseur d'identité (identity provider) via les protocoles OIDC ou SAML.

Enfin, il est possible d'affecter différents niveaux de droits aux utilisateurs en fonction de leur rôle (administrateur, administrateur d'un ou plusieurs actifs supervisés, administrateur opérationnel, lecture seule).

Le parc actuel contient un serveur maître et 3 serveurs satellites, chacun destiné à une zone réseau différentes.

Cyberwatch supervise actuellement 1500 actifs, avec une cible autour de 4000 actifs.

Les exigences ne reposent donc pas sur la solution elle-même, mais sur la distribution, le support et la maintenance de cette solution.).

3.1 Distribution

3.1.1 E1 – Partenaire agréé

Le Titulaire du marché doit être partenaire agréé par l'éditeur pour la revente de cette solution spécifique.

Le titulaire fournit une attestation de l'éditeur ou certification.

3.1.2 E2 – Notification de renouvellement

Le Titulaire du marché doit être capable de fournir des notifications sur les délais de renouvellement de la licence à 90, 60 et 30 jours avant l'échéance.

L'offre doit impérativement porter sur la dernière version du logiciel supportée par l'éditeur (à minima la 14.8, ou toute version ultérieure validée par l'éditeur à la date de remise des offres).

A chaque nouvelle version validée par l'éditeur, le Titulaire du marché devra notifier au plus tard dans la semaine qui suit qu'une nouvelle version est disponible et la durée de support des versions précédentes.

3.1.3 E4 – Délai de livraison / activation des licences

Le Titulaire du marché doit être capable de fournir une licence fonctionnelle dans un délai maximum de 5 jours ouvrés après la commande.

3.1.4 E5 – Type de licence

Le Titulaire du marché doit être capable de fournir différent type de licence en fonction des options choisies :

- Licence Vulnérabilité : permet de réaliser le scan des technologies associés à une base de connaissance des vulnérabilités pour déduire les vulnérabilités présentes sur les actifs supervisés par la solution.
- Licence Conformité : permet de réaliser des scans de la configuration des actifs supervisés en fonction de différents référentiels.

3.1.5 E6 – Savoir-faire et plus-value

Le Titulaire du marché peut également proposer des prestations supplémentaires d'accompagnement autour de la solution. Par exemple des prestations de suivis des vulnérabilités, ou de configuration spécifique. Elles doivent être décrites dans le CRT.

3.2 Support

3.2.1 E7 – Capacité à réaliser et assurer un support technique

Le Titulaire du marché doit proposer un support technique, en français, de 8h à 18h durant les jours ouvrés.

Le Titulaire du marché doit décrire les modalités de contact du support.

Le support doit être capable de répondre à diverses demandes, par exemple :

- Explication ou correction sur un comportement inattendue de l'application
- Aide à la configuration de la solution
- Aide à la mise à jour et à la maintenance de la solution
- Aide à l'évolution des serveurs en fonction de la charge (nombre de serveurs supervisés)
- Prise en compte des demandes d'évolutions de la solution

3.2.2 E8 – Délai de réponse du support

Le Titulaire du marché doit proposer des délais concernant le support ne pouvant excéder les limites suivantes :

- Délai maximum de première réponse : 2 jours ouvrés
 - Délai maximum d'aide à la résolution du problème rencontré selon la gravité du problème :
 - o Application complètement indisponible : 5 jours ouvrés
 - o Fonctionnalité indispensable indisponible : 10 jours ouvrés
 - o Fonctionnalité secondaire indisponible : 20 jours ouvrés
 - o Autres demandes : 30 jours ouvrés
- Jours ouvrés : Lundi au Vendredi

3.2.3 E9 – Lien avec l'éditeur

Le Titulaire du marché fait le lien avec l'éditeur de la solution pour les demandes qui le nécessitent, par exemple les demandes d'évolutions ou la correction de bug.

3.2.4 E10 – Suivi récurrent

Au cours du marché, une réunion de pilotage et de suivi se tiendra une fois par semestre entre le Titulaire et l'acheteur .

Elle aura pour ordre du jour :

- L'état d'avancement de la prestation,
- Les problèmes rencontrés et leur avancement,
- Le suivi contractuel du marché,
- désaccords sur la classification d'une ou plusieurs Anomalies
- les statistiques de maintenance
- Les évolutions à prévoir,
- Tout autre élément utile à la bonne réalisation de la prestation.

Les équipes opérationnelles du Titulaire et de l'acheteur tiendront des réunions d'avancement sur les parties forfaitaires et à bons de commandes en fonction de l'exigence des sujets traités.

A l'issue de chaque réunion, le titulaire présentera un compte rendu.

Le montant de cette prestation est forfaitairement inclus dans le prix des prestations

3.3 Maintenance

3.3.1 E11 – Notifications proactives

Le Titulaire du marché doit émettre des alertes actives les problèmes ou des limitations connues.

3.3.2 E12 – Suivi des bulletins de sécurité de l'éditeur

Le Titulaire du marché doit émettre des notifications actives concernant les bulletins de sécurité de l'éditeur.

Le Titulaire doit impérativement signaler les vulnérabilités du produit conformément au Cyber Resilience Act et la Loi de Programmation Militaire (LPM).

3.3.3 E13 – Mise à disposition de la documentation

Le titulaire s'engage à mettre à disposition :

- 1) des services émetteurs :

- **Pour l'acquisition de nouvelles licences :**

Le titulaire s'engage à fournir les livrables suivants correspondant aux bons de commande émis par les services émetteurs en fonction de leurs besoins :

A la livraison des licences, le Titulaire fournira :

- L'activation de la licence ;
- Les documents suivants rédigés **en français** (documentation électronique téléchargeable):
 - ✓ La notice de mise en œuvre du produit décrivant les fonctions et les modalités d'emploi des logiciels fournis et permettant leur mise en œuvre
 - ✓ Les procédures d'exploitation du produit comprenant les incidents possibles au cours du fonctionnement courant de l'application, ainsi que la conduite à tenir pour chaque type d'incident
 - ✓ Le guide de paramétrage du produit et le descriptif des fonctionnalités du produit

Le titulaire met à jour de façon périodique cette documentation et s'engage à communiquer toute information permettant de juger du caractère pertinent de celle-ci.

- **pour la maintenance préventive**

- ✓ le bulletin relatif à la prévention des problèmes et la mise en œuvre des évolutions ;

- **pour la maintenance corrective**

- ✓ les correctifs des licences détenues et des solutions connexes ;
- ✓ la fiche de mise en production comprenant entre autres les conditions d'installation, les différentes étapes d'installation de la nouvelle version, les procédures de retour arrière;
- ✓ une documentation électronique téléchargeable, en français, décrivant les fonctions et les modalités d'emploi des logiciels fournis et permettant leur mise en œuvre ;
- ✓ les mises à jour périodiques des documents par tout moyen (Internet ou autre).

- **Pour la maintenance évolutive**

- ✓ la fiche de mise en production comprenant entre autres les conditions d'installation, les différentes étapes d'installation de la nouvelle version, les procédures de retour arrière;
- ✓ la fiche de livraison récapitulant le détail du contenu de la version.
- ✓ Les dates d'échéance de supports des versions précédentes

2) **du comité de suivi semestriel :**

- le compte-rendu des dysfonctionnements et problèmes rencontrés ;
- la liste des problèmes récurrents identifiés et les résolutions mises en place.

Article 4. Environnement d'exécution du marché

4.1 Environnement technique

En cas d'intervention nécessitant un accès direct aux serveurs de la solution, l'accès sera réalisé via :

- L'utilisation d'un kit VPN, permettant d'accéder au bastion,
- L'utilisation d'un bastion, permettant d'accéder aux serveurs
- Superviser en temps réel par un agents Numih

4.2 Environnement applicatif

Dans le cadre de manipulation via l'interface applicative de la solution, ces manipulations seront réalisées via la prise de contrôle de l'écran partagé.

Article 5. Support et engagement du Titulaire

5.1 Niveau d'engagement en cas d'incident

Les actions correctives sont engagées selon les délais d'intervention suivants, en fonction de la sévérité de l'incident ou de la demande.

Classification	Définition	Délai de prise en compte	Garantie de Temps de Rétablissement (GTR)
Sévérité de l'incident ou de la demande	<p>Critique (Sévérité 1)</p> <p>Dysfonctionnement entraînant une interruption totale de la solution</p> <p>Ou</p> <p>Découverte d'une vulnérabilité de niveau critique (CVSS)</p>	2j ouvrés	5j ouvrés
	<p>Haute / urgente (Sévérité 2)</p> <p>Dysfonctionnement entraînant une qui entraîne une gêne significative dans l'utilisation de la solution</p> <p>Ou</p> <p>Découverte d'une vulnérabilité de niveau élevé (CVSS)</p>	5j ouvrés	10j ouvrés
	<p>Normal (Sévérité 3)</p> <p>Dysfonctionnement minime dont les conséquences n'ont pas d'incidence sur l'utilisation de la solution</p> <p>Ou</p> <p>Découverte d'une vulnérabilité de niveau moyenne (CVSS)</p>	20j ouvrés	30j ouvrés
Demande de service	<p>Questions générales sur la solution dans son environnement standard.</p> <p>Sollicitation de l'expertise technique du Titulaire</p>	30j ouvrés	90 jours

5.2 Maintenance

L'Acheteur assure la maintenance de niveau 1 et 2 et transmet au Titulaire la maintenance de niveau 3 :

- Niveau 1 : assistance aux utilisateurs
- Niveau 2 : traitement des problématiques liées à des incidents connues et répertoriées, liées à de l'interopérabilité
- Niveau 3 : traitement des problématiques nécessitant une intervention au sein du code source ou de la responsabilité du Titulaire

Le périmètre des niveaux de support sera précisé au sein d'un RACI support partie intégrante du Plan Assurance Qualité.

Article 6. Gestion des données à caractère personnel

S'agissant de l'achat de licence, il n'y a pas de sous-traitance au sens du RGPD. Le fournisseur devra toutefois nous tenir informé de l'usage qu'il fera en tant que Responsable de Traitement des données à caractère personnel des agents Numih France collectées durant la période du marché. Assurance et contrôle de la sécurité des services d'intervention fournis.