Questions

Question 1 : III.3.2 - page 53

Approach

"Capacité à intégrer le produit de filtrage des messages électroniques avec d'autres systèmes de sécurité et de gestion de la confidentialité des données":

quels types d'autres systèmes ?

Réponse au soumissionnaire

Cela dépendra de chaque pouvoir local. Une réunion de planification sera organisée avec chaque pouvoir local en amont du projet. Cela peut concerner des antivirus, des XDR, du firewall, un SOC/SIEM, solution DLP. La liste ne pourrait être complète, mais au vue des pouvoirs locaux, rien d'extravagant n'est implémenté.

Question 2 : III.3.2 - page 53

Approach

"Capacité à fournir une solution de filtrage des messages électroniques adaptée aux besoins et aux contraintes des Pouvoirs locaux wallons":

quels sont ces besoins et contraintes (autres que les éléments décrits dans le document) ?

Réponse au soumissionnaire

Aucune autre contrainte ou besoin spécifique connu.

Question 3 : III.3.2 - page 53

Approach

"Capacité à gérer les fichiers joints de grande taille et à protéger contre les virus et les logiciels malveillants":

quoi comme grande taille, car les mails sont par nature de taille limitée

Réponse au soumissionnaire

Nous avons vu des limitations d'emails jusqu'à 50Mo lors des audits. Idéalement, la capacité à gérer des fichiers joints devrait être garanti jusqu'à 50Mo

Question 4 : III.3.2 - page 53

Approach

" Capacité à intégrer le produit de filtrage des messages électroniques avec les pares-feux et les autres systèmes de sécurité du réseau des Pouvoirs locaux wallons":

Orienté pour un système intégré? quels autres systèmes ?

Réponse au soumissionnaire

Cela dépendra de chaque pouvoir local. Une réunion de planification sera organisée avec chaque pouvoir local en amont du projet. Cela peut concerner des antivirus, des XDR, du firewall, un SOC/SIEM. La liste ne pourrait être complète, mais au vue des pouvoirs locaux, rien d'extravagant n'est implémenté.

Question 5 : III.3.2 - page 53

Approach

"Capacité à intégrer le produit de filtrage des messages électroniques avec les systèmes de messagerie existants des Pouvoirs locaux wallons"

> Quels sont ces systèmes ?

Réponse au soumissionnaire

Principalement, nous avons eu Microsoft Exchange avec Office 365, du Exchange On-Premise et également du Google Workspace.

Question 6 : III.3.3.3 - Page 58

Approach

"Capacité à intégrer le produit de filtrage des messages électroniques avec d'autres outils de gestion de la messagerie, tels que les boîtes aux lettres partagées et les listes de diffusion": gestion au niveau serveur, pas au niveau user?

Réponse au soumissionnaire

Les deux peuvent être demandés. Potentiellement à la demande du Pouvoir Local.

Question 7 : III.3.3.3 - Page 58

Approach

"Capacité à prendre en charge les protocoles de chiffrement de bout en bout pour assurer la confidentialité des messages électroniques"

Quid ? Plutôt lié à un système de chiffrement dans ce cas.

Réponse au soumissionnaire

Ce point est une confirmation que le filtrage par email fonctionnerait également dans le cas d'emails chiffrés.

Question 8 : III.3.3.5 - Page 60

Approach

"Un temps de réponse inférieur à T secondes pour la réception et le traitement des messages électroniques"

> en contradiction avec la notion de sandboxing

Réponse au soumissionnaire

Question à préciser ?
Tous les mails ne doivent pas forcément passer dans la sandbox, mais, nous souhaiterions une solution qui pourrait éventuellement incorporer une sandbox pour test.

Question 9 : III.3.3.6 - Page 60

Approach

Domaines d'expertise à maîtriser" > une bonne partie est la copie de la partie pour l'authentification

Réponse au soumissionnaire

Est-ce une question ?

Oui car nous considérons cela correct pour le besoin du marché.

Question 10 : III.3.4.2 - Page 61

Approach

Mise à jour automatique des définitions de virus et de menaces en temps réel >

Rapide oui, mais les mises à jour en temps réel, c'est compliqué pour tous les éditeurs. Et encore nous sortons des micro mises à jour plusieurs fois par jour.- car à notre système de télémétrie.

Réponse au soumissionnaire

Le prestataire propose la solution la plus adéquate. Le temps réel n'est pas de l'immédiateté.

Question 11 : III.3.4.2 - Page 61

Approach

Intégration avec les outils de gestion de la sécurité existants (SIEM, EDR, etc.) > Pas clair, la demande est formulée bizarrement. S'agit-il d'un système EDR qui s'intègre dans un autre EDR ?

Réponse au soumissionnaire

Coquille lors de la rédaction, EDR n'a rien à faire ici.

Question 12 : III.3.4.2 - Page 61

Approach

Prise en charge des plateformes de système d'exploitation couramment utilisées par les Pouvoirs locaux wallons > liste de ceux-ci?

Réponse au soumissionnaire

Windows, MacOS, Linux

Question 13 : III.3.4.2 - Page 61

Approach

Capacité à intégrer des données provenant de sources externes pour améliorer la détection des menaces > quels types de données?

Réponse au soumissionnaire

Un exemple probant est l'intégration d'IoCs connus issues de potentielles attaques en cours dans d'autres pouvoir locaux ou à l'échelle de la région/ État Belge

Question 14 : III.3.4.3 - Page 62

Approach

Compatibilité avec les différents systèmes d'exploitation et logiciels utilisés par votre organisation: quels OS?

Réponse au soumissionnaire

Idem Q12

Question 15 : III.3.4.3 - Page 62

Approach

Intégration avec les outils de gestion de la sécurité existants du Pouvoir local, tels que les pares-feux et les gestionnaires de mots de passe: orienté pour un système intégré global typé SIEM/SOAR

Réponse au soumissionnaire

Est-ce une question ?

Question 16 : III.3.4.4 - Page 62

Approach

...rapport et documentations .. En ce sens, seront demandés les documents suivants : .. > à quel moment est-ce que cela est demandé ?

Réponse au soumissionnaire

Les documents doivent être fournis au moment de la soumission. Les documents ne sont pas obligatoires mais conseillés car chaque document fait partie de la pondération finale.

Question 17 : III.3.4.4 - Page 62

Approach

Des mises à jour régulières sur l'état de la sécurité et les menaces en cours, ainsi que sur les mises à jour et les correctifs appliqués aux produits Antivirus/Antimalware/EDR/XDR > que signifie régulières ? 1x jour/mois/année ?

Réponse au soumissionnaire

Chaque fournisseur ayant ses propres fonctionnalités, c'est à vous de nous indiquer ce qui est possible/normalement usage avec la solution que vous proposez

Question 18 : III.3.4.4 - Page 62

Approach

Des rapports de performance et de couverture de la solution antivirus/antimalware, présentant les taux de détection et de faux positifs >pouvez-vous préciser SVP?

Réponse au soumissionnaire

Un white paper ou un statement des scores garantis de détection de l'antivirus.

Question 19 : III.3.4.5 - Page 63

Approach

Garantie de couverture complète contre les menaces informatiques, y compris les virus, chevaux de Troie, ransomwares et autres types de logiciels malveillants > Garantie de couverture complète contre des futurs éléments inconnus ? Impossible pour n'importe quel éditeur.

Réponse au soumissionnaire

Il n'est pas question d'une couverture complète concernant les éléments encore inconnus. Il est cependant demandé d'être évolutif.

Question 20 : III.3.4.5 - Page 63

Approach

Ils doivent également être en mesure de fournir une protection contre les attaques de phishing et de ransomwares, ainsi que contre les menaces liées aux réseaux sociaux > on sort ici du scope de la gestion logiciel/process puisqu'on est clairement dans de la gestion/assistance utilisateur (qui dépasse le périmètre logiciel). Quid ?

Réponse au soumissionnaire

Problème de phrasé, on parle ici d'analyse comportementale des liens vérolés.

Question 21 : III.3.4.5 - Page 63

Approach

Offrir une assistance technique de qualité pour aider les utilisateurs à résoudre tous les problèmes liés à la sécurité: on sort d'un scope purement logiciel. Il est question d'assistanat par utilisateur. Quid ?

Réponse au soumissionnaire

Problème de phrasé, il est question ici de d'assistance au niveau logiciel.

Question 22 : III.3.4.5 - Page 63

Approach

"Résoudre « tous les problèmes liés à la sécurité » ? On sort du scope purement de l'XDR, pourriez-vous clarifier?

Réponse au soumissionnaire

Problème de phrasé, il est question ici de d'assistance au niveau logiciel.

Question 23 : III.3.4.5 - Page 63

Approach

Nous demandons à chaque soumission de nous faire parvenir les éléments suivants auquel vous vous engagez :

● Un taux de détection de spam supérieur à X%

● Un taux de détection de virus supérieur à Y%

● Un taux de faux positifs inférieur à Z%

● Un temps de réponse inférieur à T secondes pour la réception et le traitement des messages électroniques

● Une disponibilité de service supérieure à X% en termes de temps de fonctionnement ininterrompu par mois

● Une assistance technique disponible H/24 et 7/7 avec un délai de réponse maximum de Y heures pour les demandes de niveau 1 et de Z heures pour les demandes de niveau 2

● Des mises à jour logicielles et de sécurité mensuelles ou trimestrielles

● Une formation initiale et continue pour les utilisateurs finaux sur l'utilisation du

produit et ses fonctionnalités

> Travail non fini ? Quid des valeurs ?

> Concernant la formation continue : quid des services de gestion et maintenance avec un partenaire de qualité et compétent en mode SaaS ? + Verrouiller le plus de fonctionnalités aux utilisateurs permet de réduire la surface d'attaque.

Réponse au soumissionnaire

Un service managé est possible. Les outils doivent reporter les indicateurs mentionnés.

Question 24 : III.2.3.7 – Page 48

CIVADIS

Le scénario technique décrit aux points III.2.3.7 servira de base pour remplir l'inventaire du lot M2.

Question : cela signifie-t-il qu'on sera obligé de proposer cette seule et unique offre dans le cadre des marchés subséquents des PAB ou pourra-t-on adapter notre proposition aux besoins réels des PAB (changement de modèle, de licences, de prestations, …) ?

Réponse au soumissionnaire

L'attribution reposant sur les équipements et services proposés, il est strictement interdit de faire recours à d'autres moyens que ceux proposés. Les variantes sont interdites.

Question 25 : III.2.4.7 – Page 52

CIVADIS

Le scénario technique décrit aux points III.2.4.7 servira de base pour remplir l'inventaire du lot M3.

Question : cela signifie-t-il qu'on sera obligé de proposer cette seule et unique offre dans le cadre des marchés subséquents des PAB ou pourra-t-on adapter notre proposition aux besoins réels des PAB (changement de modèle, de licences, de prestations, …) ?

Réponse au soumissionnaire

Idem Q24

Question 26 : III.2.4.7 – Page 52

CIVADIS

Le scénario technique auquel nous devons répondre est de type « matériel et logiciel ». Pouvons-nous également proposer un scénario de solution de sauvegarde uniquement logiciel dans le « Cloud » (Par exemple : Veeam Cloud Backup) ?

Réponse au soumissionnaire

Il est possible de proposer une solution uniquement cloud.

Question 27 : III.3.2.7 – Page 62

CIVADIS

Le scénario technique décrit aux points III.3.3.7 servira de base pour remplir l'inventaire du lot L3.

Question : cela signifie-t-il qu'on sera obligé de proposer cette seule et unique offre dans le cadre des marchés subséquents des PAB ou pourra-t-on adapter notre proposition aux besoins réels des PAB (changement de licences, de prestations,…) ?

Réponse au soumissionnaire

Idem Q24

Question 28 : III.3.4.7 - Page

CIVADIS

Le scénario technique décrit aux points III.3.4.7 servira de base pour remplir l'inventaire du lot L4.

Question : cela signifie-t-il qu'on sera obligé de proposer cette seule et unique offre dans le cadre des marchés subséquents des PAB ou pourra-t-on adapter notre proposition aux besoins réels des PAB (changement de licences, de prestations, …) ?

Réponse au soumissionnaire

Idem Q24

Question 29 : III.2.3.3.1 – Page 44

CIVADIS

Question : Pourquoi le pare-feu se trouve dans la partie matériel et le titre du paragraphe III.2.3.3.1 est « Pare-feu virtuel » ?

Réponse au soumissionnaire

Il est question ici de pare-feu matériel et virtuel. Afin de ne pas doubler les lots, nous avons incorporé la partie virtuelle avec le lot déjà présent.

Question 30 : III.2.3 – Pages 42 - 49

CIVADIS

Pare-feu capable de prendre en charge les configurations active/active et active/passive.
Question : Peut-on envisager uniquement active-passive ?

Réponse au soumissionnaire

Non, les prescrits techniques renseignent les configurations à supporter, une solution ne supportant uniquement l'actif/passif sera déclarée irrégulière, le soumissionnaire verra alors son offre écartée.

Question 31 : III.2.3.5 – Pages 43

CIVADIS

Intégration avec d'autres équipements et solutions : le soumissionnaire doit être capable de démontrer comment son pare-feu peut être intégré et utilisé en conjonction avec d'autres équipements et solutions de sécurité, tels que les systèmes de détection d'intrusion, les logiciels de gestion de réseau, etc. ;
Question : Quels équipements et solutions pourraient être concernés ?

Réponse au soumissionnaire

Idem Q1

Question 32 : III.2.3.7 – Pages 44

CIVADIS

Capacité de gestion des utilisateurs distants : Jusqu'à 100 utilisateurs.
Question : il s'agit bien de connexions Client-to-Site simultanées ?

Réponse au soumissionnaire

Correct

Question 33: III.3.3.7 – Page 67

CIVADIS

La solution de filtrage des messages électroniques sera déployée au sein de l'infrastructure du pouvoir local pour sécuriser la messagerie électronique des utilisateurs.
Question : Une solution Cloud peut-elle être envisagée ?

Réponse au soumissionnaire

Oui

Question 34 : III.3.3.7 – Page 67

CIVADIS

Elle sera intégrée aux **solutions de sécurité existantes** du pouvoir local, permettant **une gestion centralisée** des politiques de sécurité et une vue d'ensemble des menaces liées aux emails.
Question : Quelles sont les **solutions de sécurité existantes possibles ?**

Réponse au soumissionnaire

Idem Q1.

Question 35 : III.2.3.3.1 - Page 40

Prodata Systems

Veuillez préciser l'exigence suivante dans la section III.2.3.3.1 (page 40)

- Paires de commutateurs DMS dédiés par interface physique

Réponse au soumissionnaire

Ceci est à prendre en considération pour le pare-feu physique.

Question 36 : III.2.3.3.2 - Page 41

Prodata Systems

Veuillez préciser l'exigence suivante dans la section III.2.3.3.2: (page 41)

- Paires de commutateurs DMS dédiés par interface physique

Réponse au soumissionnaire

Cela concerne tout ce qui touche aux données et services de messages.

Question 37 : Section correspondante - Page

Fortinet:
Est-ce que les prix doivent être valables sur 4 ans.

S'il s'agit de prix nets, ceci implique que les constructeurs et partenaires vont devoir prendre une marge de sécurité sur le prix dans leurs réponses.
Les prix peuvent beaucoup varier, et impossible quelle sera la situation dans 4 ans.

Nous aimerions répondre avec des discounts sur prix liste. Dans notre cas, les prix liste sont envoyés à tous nos partenaires en moyenne deux fois par trimestre.
Avec un discount sur prix liste, nous allons pouvoir être beaucoup plus agressifs dans notre réponse, car nous ne prenons pas de risque quant à l'évolution de prix (qui peut d'ailleurs aller dans les deux sens).
C'est comme cela que nous travaillons dans la plupart des contrats cadre (Forem, Irisnet, Stib, Icity, SMALS, ONVA…)

Réponse au soumissionnaire

La révision des prix est prévue au point II.7 du cahier spécial des charges.

Question 38 : Motifs d'exclusion et sélection qualitative- Page 9

NSI

Nous sommes tenu par un NDA auprès de nos clients lors de la réalisation de nos projets et il continue même après. Fournir des informations concernant nos clients surtout sur leurs systèmes de sécurité n'est donc pas envisageable. Nous pouvons vous fournir les secteurs d'activités pour lesquels nous travaillons avec des tailles moyennes de clients. Est-ce que cela vous convient ?

Réponse au soumissionnaire

Dans le cadre des vérifications des références, vous devez mettre à disposition les personnes de contact des références avancées, cela ne vous dégage en rien de l'engagement sur l'honneur duquel découle le DUME.

Question 39 : Lot M2 : Pare-feu- Page 39-40

NSI

Vous parlez de mises à jour et évolution logicielle, est-ce que cela veut dire que nous devons intégrer des managed services dans l'offre ?

Il y a une référence à un pare-feu virtuel avec des caractéristiques peu probante, comme un système de montage en rack 19, n'y-t-il pas une erreur dans la description ? Quelle est la finalité de ce type de pare-feu ? Même question pour le pare-feu back-office.

Réponse au soumissionnaire

1/ vous devez intégrer les services nécessaires aux mises à jour demandées.

2/ Si l'installation du composant logiciel nécessite des prestations sur l'environnement physique, il est demandé que ces prestations soient incluses. Ce qui ne concerne pas les infrastructures purement cloud.

Question 40 : Lot M2 : Pare-feu – Page 44

NSI

Y-a-t-il un rapport entre le scénario pour compléter l'inventaire et les pare-feu virtuel et backoffice ? Les caractérisques de l'un n'étant pas du tout en adéquation avec les caractérisques de l'autre.

Réponse au soumissionnaire

Le scénario repose sur un firewall physique (Backoffice)

Question 41 : Section correspondante - Page

Econocom

Est-il possible de répondre à la fois en offre d'achat et en location, incluant le matériel, les logiciels et les services ?

Réponse au soumissionnaire

Non, ce modèle n'est pas prévu dans le présent marché.

Questions posés en séance

Question 42 : Section correspondante - Page

Question de Civadis (Pierre Koumoth) : 15h58

Pour chaque lot, vous avez une spécification technique, auquel notre solution doit être

conforme.

Ensuite il y a le scénario pour compléter l'inventaire. Qui peut aller plus loin que les spécifications techniques qui sont reprises dans votre cahier des charges.

Et quand on voit la liste des clients (petites et grandes communes).

Comment peut-on avoir une solution similaire, basée sur un même type de matériel, valable pour une petite commune comme pour une grande commune ?

Réponse au soumissionnaire

On vous demande effectivement de proposer une solution qui doit être adaptable aux différents scénarios rencontrés et, donc, ce que vous devez faire dans le premier exemplaire du bordereau de prix, est de constituer la liste d'articles de logiciels et matériel, de prestations ou de services que vous proposez et de mettre en application cette liste là dans le deuxième bordereau de prix.

Donc, oui, vous devez répondre aux marchés subséquents avec le matériel et logiciel qui sera proposé en réponse à cet appel d'offre et pas autre chose.

Une fois que le marché est attribué, il est basé sur ce qui a été proposé en réponse à l'appel d'offre et il n'est plus question de le faire évoluer librement en fonction d'un paramètre ou l'autre

Question 43: Section correspondante - Page

Question Silvain Nzukou - Proximus : 16h02 → 26:05

Si on propose une solution pour le pare-feu, il existe plusieurs types comme EDR, XDR, …

Au niveau prix, certaines solutions ne sont peut-être pas adaptées à l'utilisation d'une commune (pas besoin de la Rolls).

Si propose une seule solution (ex XDR) qui comprendrait l'ensemble des sous-services anti-virus, anti-malware, est-ce qu'au niveau prix ce serait quelque chose qui frapperait puisque les communes n'ont pas spécialement d'une grosse solution XDR ?

Comment évalueriez-vous ce type de solution par rapport à plusieurs outils séparés ?

Réponse au soumissionnaire

Il y a deux parties à la réponse.

1. la partie budgétaire : comparaison sur base du scénario que vous compléterez
2. la partie fonctionnelle : si le produit permet une granularité de fonction, ce sera à vous de voir comment l'exprimer, si le produit ne permet pas cette granularité, c'est un peu dommage.

Si vous voulez savoir quelle serait la meilleure offre à faire, tout est très clairement expliqué dans le cahier des charges par rapport à la manière dont cela va être évalué

(règle de trois, pondérations, …). Vous pouvez vous-même faire l'exercice en fonction des différentes offres et choisir la meilleure offre que vous voulez proposer.

Question 44 : Section correspondante - Page

Daniel

Comment tenez-vous compte du cycle de vie produit (end of life ...)

Réponse au soumissionnaire

Il appartient aux soumissionnaires de choisir un fournisseur fiable et en mesure de maintenir les équipements disponibles, les évolutions de versions n'étant pas une fin de vie de produit. Par ailleurs, vu la limite financière de la centrale d'achat, et le nombre de candidatures, il est vraisemblable que la centrale d'achat arrive plus rapidement à son terme par la limite budgétaire que sa limite de temps (4 ans).

Question 45 : Section correspondante - Page

Laure stuto - Proximus

Le nombre de références par lot est un nombre max ou min?

Réponse au soumissionnaire

Un nombre minimal

Question 46 : Section correspondante - Page

Question de Charles Sadones - Nomios : 16h14 - 38:55

Par rapport au nombre de référence que vous demandez, vous en demandez 50, pour de l'EDR par ex.

Est-ce que ces 50 références ou est-ce que c'est 50 unités qui feraient parties d'une même structure ?

Est-ce que l'on doit vous donner 50 structures différentes qui ont de l'EDR ou est-ce que c'est une seule structure qui a 50 postes ?

Réponse au soumissionnaire

C'est bien 50 structures/organisations (pour autant que ce soit des installations distinctes) et chacune d'elle devant contenir un nombre de poste défini dans le cahier des charges.

Question 47 : Section correspondante - Page

Charles sadon - Nomios 16h15 40:07

Concernant les modules EDR.

Qu'est ce que vous entendez par EDR, XDR car c'est assez vaste ?

Sachant qu'il y a de l'MDR aussi, du VPN. Est-ce que c'est spécifiquement EDR - XDR ?

Réponse au soumissionnaire

Vous pouvez proposer une autre solution du moment que l'on reste dans le cadre des fonctionnalités et des contraintes techniques demandées et qui correspond aux pouvoirs locaux.

On va se baser sur ce que vous allez écrire en fonction de ce qui a été demandé dans le cahier des charges (fonctionnel et technique)

Question 48 : Section correspondante - Page

Sylvain Nzukou - Proximus : 16h17 - 42:12

Les lots sont séparés et nous pouvons donc répondre à l'un et pas à l'autre.

Je voulais confirmer avec vous que l'on pouvait bien se positionner sur l'un et par sur l'autre, cela n'impacte pas votre jugement dans sa globalité ?

Réponse au soumissionnaire

Tout à fait.

Question 49 : Section correspondante - Page

Sylvain Nzukou - Proximus : 16h20 - 44:32

Dans le bordereau, vous avez un ensemble de lignes avec les spécificités techniques basées sur le cahier des charges.

Est-ce que nous pouvons ajouter quelques détails techniques sur la mise en place ou sur la solution?

Est-ce que vous vous appuierez uniquement sur le bordereau ou est ce que le complément d'information fourni serait pris en compte aussi ?

Réponse au soumissionnaire

Le bordereau à pour objectif de structurer votre réponse réponse.

Il est conseillé de l'utiliser car cela facilite le travail d'analyse, ce qui rend l'analyse plus efficace. Ce qui rend la qualité de l'analyse meilleure et donc, l'attribution aussi.

Si vous désirez ajouter des documents, il faudra bien les référencer. N'oubliez pas d'indiquer de manière claire, et très explicite, les éléments que vous voulez que l'on prenne en compte dans chaque document pour que nous ne devions pas lire la totalité des documents envoyés. Cela facilite le travail d'analyse et donc sa qualité.

Question 50 : Section correspondante - Page

Laure Stuto

Avez-vous prévu un délai complémentaire pour la réponse ?

Réponse au soumissionnaire

N'étant pas dans un des cas de figure définis par la loi sur les marchés publics et l'arrêté royal relatif à la passation, aucun délai complémentaire n'est octroyé.

L'ensemble des éléments relatifs aux marchés étant fournis à dater du 26 juin, et complété le 19 juillet, laisser 33 jours à dater de la dernière publication a été jugée comme suffisante et vous permettant de remettre votre offre.

Question 51 : Section correspondante - Page

Charles Sadones - Nomios

Qu'est-ce qui doit être en Français et peut-être en Anglais ? (Descriptifs techniques)

Réponse au soumissionnaire

Tous les éléments devant être pris en compte dans les soumissions doivent être en français comme le prévoit le cahier spécial des charges.

Question 52 : Section correspondante - Page

Guillaume VERHAEGEN - QUANT ICT : 16h26 - 50:56

Question par rapport aux références.

Quels moyens de preuve attendez-vous par rapport à ces références ?

Réponse au soumissionnaire

Le DUME est un engagement sur l'honneur. C'est clairement ça dans un premier temps.

Il faut qu'on ait dans ces éléments la possibilité de vérifier qu'effectivement ça cadre avec le niveau minimum requis exprimé dans le cahier des charges.

D'autre part, nous devrons peut-être vous demander les points de contact pour que l'on puisse vérifier les preuves.

Il ne faut donc plus fournir des attestations comme avant 2016.

Question 53 : Section correspondante - Page

Charles Sadone - Nomios : 16h28 - 52:56

2 questions :

1. Est-ce que vous avez besoin d'une confirmation ISO, constructeur ou autre ?
2. Pour les CV, vous acceptez les cv qui pourraient être d'un groupe rattaché à la société, par ex. Français ?

Réponse au soumissionnaire

1. Nous n'avons pas demandé ce type de certification
2. Cela ne doit pas être des personnes spécifiquement en Belgique, par contre, si vous faites appel à votre groupe pour répondre et que cet autre société est à considérer comme un sous-traitant, n'oubliez pas que celui-ci doit également compléter un DUME. Sinon, ces personnes qui découlent d'un autre organisme, ne seront pas prises en compte.

Question 54 : Section correspondante - Page

Guillaume Verhaegen -QUANT IC - 16h30- 54:55

2 questions

1. Concernant le bordereau de réponse technique (page 93) : il s'agit d'une grille avec 3 colonnes sur la droite avec expert 1 à 3.
   Vous attendez à ce que, quand on répond "oui" à l'une de ces colonnes, on renvoie à un endroit spécifique d'un cv ? Concrètement comment cela doit être présenté ?
2. Concernant la qualité de la documentation, au point 5 du critère 4, on parle de "failles constatées".
   Failles constatée de quoi ? De la solution qu'on propose ?

Réponse au soumissionnaire

1. Oui. Dans le cv, il a une expérience dans le domaine demandé.
2. Oui. Une documentation sur les failles détectées, comment cela a-t-il été détecté, comment cela a-t-il été résolu.
   Comment a-t-elle été traitée. Comment vous traitez ces situations là.
   Tous les documents ne sont pas obligatoires. Il faut les fournir dans la mesure de leur disponibilité.