SERVICES PARTAGÉS CANADA

Demande de renseignements pour le processus d'approvisionnement concernant la consultation sur une solution évoluée de sécurité aux points d'extrémité et de gestion des licences logicielles

N° de la demande de renseignements	15-35615	Date	**24 février 2016**
Bureau émetteur	Services partagés Canada 180, rue Kent, 13e étage, 13-125 Ottawa (Ontario) K1P 0B6		
Autorité contractante (L'autorité contractante est le représentant de SPC pour tous les commentaires et toutes les questions portant sur le présent document.)	Nom	Betty-Jane Horton	
	N° de téléphone	613-301-5643	
	Courriel	betty-jane.horton@canada.ca	
	Adresse postale	Services partagés Canada 180, rue Kent, 13e étage, 13-102 Ottawa (Ontario) K1P 0B6	
Date et heure de clôture	10 mars 2016 à 14 h		
Fuseau horaire	Heure normale de l'Est (HNE)		
Destination des biens ou des services	Sans objet – Demande de renseignements uniquement		
Courriel auquel la réponse doit être envoyée avant la date de clôture	betty-jane.horton@canada.ca		

Table des matières

SERVICES PARTAGÉS CANADA

Demande de renseignements pour le processus d'approvisionnement concernant la consultation sur une solution évoluée de sécurité aux points d'extrémité et de gestion des licences logicielles

1. Renseignements généraux

1.1 Présentation

1) **Phase 1 du processus d'approvisionnement :** Cette demande de renseignements (DDR) constitue la première phase d'un processus d'approvisionnement mené par Services partagés Canada (SPC) afin d'obtenir des conseils sur une solution évoluée de sécurité aux points d'extrémité et de gestion des licences logicielles (le « **Projet** »). Les fournisseurs sont invités à présenter des réponses afin d'aider le gouvernement du Canada à préciser ses exigences concernant le Projet. Les fournisseurs ne sont pas tenus de présenter une réponse à la présente DDR pour participer aux phases subséquentes du processus d'approvisionnement lié au Projet.

2) **L'étape de la DDR n'est pas une demande de soumissions :** La présente DDR ne constitue pas une demande de soumissions ou un appel d'offres. Aucun contrat ne sera attribué à la suite des activités tenues dans le cadre de la présente DDR. Le gouvernement du Canada se réserve le droit d'annuler toute exigence préliminaire décrite dans le cadre du Projet à tout moment pendant la DDR ou pendant toute autre étape du processus d'approvisionnement. Le processus de DDR et toute activité d'approvisionnement connexe étant susceptibles d'être partiellement ou entièrement annulés par le gouvernement du Canada, l'étape de la DDR peut ne pas aboutir à des processus d'approvisionnement subséquents.

3) **Coûts des réponses :** SPC ne remboursera pas au fournisseur ou à ses représentants les dépenses ou les frais généraux liés à la participation aux activités de l'étape de la DDR. Il leur incombe par ailleurs d'assurer leurs propres recherches indépendantes, processus de diligence raisonnable et enquêtes, ainsi que d'obtenir les conseils indépendants qu'ils jugent nécessaires et souhaitables dans le cadre de leur participation au processus de la DDR et à tout processus d'approvisionnement à venir.

1.2 Aperçu du Projet

1) **Aperçu du Projet**

Le Center for Internet Security est un organisme sans but lucratif qui a pour mission d'améliorer l'état de préparation et les interventions des secteurs public et privé touchant de la cybersécurité. Il a récemment publié, en partenariat avec le SANS Institute, l'un des fournisseurs de formation sur la sécurité de l'information les plus renommés au monde, la dernière version des 20 principaux contrôles de sécurité critiques (CSC)[1]. Le Centre de la sécurité des télécommunications (CST) reconnaît que ces CSC « renferment d'excellentes

[1] https://www.sans.org/critical-security-controls

suggestions pour les réseaux génériques »[2]. Les contrôles suivants se trouvent tout en haut de cette liste :

a) Liste des dispositifs autorisés et non autorisés (CSC 1);
b) Liste des logiciels autorisés et non autorisés (CSC 2);
c) Configurations sécurisées pour le matériel et les logiciels : appareils mobiles ordinateurs portatifs, postes de travail et serveurs (CSC 3); et
d) Évaluation continue de la vulnérabilité et restauration (CSC 4).

Même si plusieurs initiatives et projets ont pour but d'améliorer la sécurité des réseaux de SPC, du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), les CSC précisés ci-dessus ne sont pour l'instant que mis partiellement en œuvre à l'échelle de l'organisation.

a. Objectif du Projet

À l'aide de cette DDR, SPC et le MDN cherchent à recueillir de l'information sur des solutions évoluées de sécurité aux points d'extrémité et de gestion des systèmes qui pourraient les aider à respecter ces CSC et à combler les lacunes actuelles. Les solutions proposées doivent également tenir compte du CSC relatif à la sécurité de la configuration des dispositifs réseau (CSC 11), de la détection et de la correction des menaces pour le point d'extrémité, ainsi que de l'analyse criminalistique des appareils à distance.

Enfin, les ministères s'efforcent également d'améliorer l'efficacité des activités liées à la gestion des licences. À cette fin, SPC et le MDN sont à la recherche de solutions qui pourraient automatiser la gestion des licences à l'échelle de l'organisation et recueillir des statistiques sur l'utilisation de la solution logicielle.

b. Objet de la présente demande de renseignements

Le but de cette DDR consiste à recevoir de la rétroaction, des idées et des suggestions de la part des fournisseurs au sujet de solutions évoluées de sécurité aux points d'extrémité et de gestion de licences. Les principaux objectifs de la présente DDR sont :

a) Confirmer la disponibilité des solutions de sécurité aux points d'extrémité et de gestion des systèmes, et recueillir de l'information sur ces éléments;
b) Confirmer la disponibilité des solutions de gestion des licences, et recueillir de l'information sur ces éléments;
c) Cerner les aspects techniques importants à prendre en considération; et
d) Estimer le niveau d'efforts et le délai de mise au point requis pour mettre en œuvre les solutions proposées.

Compte tenu de la portée de cette DDR, il est fort possible qu'une solution ne puisse à elle seule satisfaire à toutes ces exigences. Par conséquent, les fournisseurs sont invités à présenter leur proposition même si leur solution ne satisfait qu'à certaines des exigences.

On demande aux fournisseurs de préciser, parmi les fonctionnalités suivantes, celles au sujet desquelles ils aimeraient présenter de l'information :

a) Gestion des biens de TI/gestion de la configuration;
b) Gestion des licences logicielles;
c) Gestion de la solution logicielle et des correctifs;
d) Détection/intervention en cas d'incident; et
e) Analyse criminalistique des appareils à distance.

[2] https://www.cse-cst.gc.ca/fr/node/1297/html/25231

Remarque : À la section 4 du présent document, tous les fournisseurs sont invités à répondre aux *Questions générales* (point 4.4). Les fournisseurs sont doivent également invités à répondre aux *Questions propres aux fonctionnalités* (point 4.5) sélectionnées ci-dessus.

Le présent document est de nature évolutive, et les répondants ne doivent pas tenir pour acquis qu'aucune nouvelle disposition ou exigence ne sera ajoutée à toute demande de soumissions finalement publiée par le MDN, SPC ou un autre ministère ou organisme. Les répondants ne doivent pas non plus supposer qu'aucune des dispositions ou aucun des besoins ne sera supprimé ou révisé. Les observations concernant cet aspect du document préliminaire sont les bienvenues. Si les répondants estiment qu'une question ou un aspect clé a été omis, nous les invitons à formuler des commentaires ou à fournir des renseignements à cet égard dans leur réponse.

2) Portée du processus d'approvisionnement prévu

   a. **Clients utilisateurs potentiels :** Cette DDR est produite par SPC, en partenariat avec le MDN. Il est prévu que le contrat découlant de toute demande de soumissions ultérieure sera utilisé par le MDN et par SPC pour fournir des services partagés à un ou plusieurs de leurs clients. Les clients de SPC comprennent SPC lui-même, les institutions fédérales pour qui ses services sont obligatoires à tout moment pendant la durée de l'instrument subséquent, ainsi que les autres organisations qui, sur une base facultative, choisissent de recourir à ses services de temps en temps, à tout moment pendant la durée de l'instrument subséquent. Tout processus d'approvisionnement subséquent n'empêchera pas SPC d'avoir recours à une autre méthode d'approvisionnement pour ses clients qui ont des besoins identiques ou semblables, à moins qu'une demande de soumissions subséquente concernant le Projet indique expressément le contraire.

   b. **Nombre de contrats :** Pour l'instant, le Canada envisage l'attribution de plus d'un contrat.

   c. **Durée de tout contrat subséquent :** Le Canada n'a pas encore déterminé la durée du contrat ou si celui-ci sera assorti d'années d'option.

3) **Exception au titre de la sécurité nationale :** Le Canada a invoqué l'exception au titre de la sécurité nationale à l'égard de la présente demande et, par conséquent, aucun des accords commerciaux ne s'applique à celle-ci.

1.3 Soumission de questions

1) Les questions sur la présente DDR peuvent être transmises à l'autorité contractante à l'adresse électronique indiquée sur la page couverture. Ces questions doivent être présentées à l'intérieur de la période de questions indiquée ci-dessous. Il est possible qu'on ne puisse pas répondre aux questions reçues après cette période.

   Période de questions : Les questions doivent être présentées avant le 10 mars 2016, à 14 h (heure normale de l'Est).

2) Les répondants doivent indiquer le plus exactement possible le numéro d'article de la DDR auquel renvoie leur question, et prendre soin d'expliquer chaque question en donnant suffisamment de détails pour permettre au Canada d'y apporter des réponses exactes.

3) Pour garantir l'uniformité et la qualité des renseignements communiqués aux fournisseurs, les questions importantes reçues et les réponses à celles-ci seront affichées sur le site du

Service électronique d'appels d'offres du gouvernement (SEAOG), sous forme de modification de cette DDR.

2. Réponse des fournisseurs

2.1 Présentation d'une réponse

1) **Date et lieu de présentation des réponses :** Les fournisseurs qui souhaitent fournir une réponse doivent l'envoyer à l'autorité contractante, par courriel, à l'adresse électronique destinée à la présentation des réponses qui figure sur la page de couverture avant la date et l'heure limites indiquées sur la page de couverture du présent document.

2) **Responsabilités en ce qui a trait à la présentation des réponses dans les délais prescrits :** Il incombe à chaque fournisseur de s'assurer que sa réponse est livrée à la bonne adresse électronique et qu'elle est reçue dans les délais prescrits.

3) **Identification de la réponse :** Chaque fournisseur veillera à ce que son nom, l'adresse de l'expéditeur, le numéro de la demande d'information et la date de clôture apparaissent bien en vue dans la réponse. Le fournisseur doit également désigner un représentant avec lequel le gouvernement du Canada pourra communiquer au sujet de la réponse et indiquer le nom de la personne, son titre, son adresse, son numéro de téléphone et son adresse électronique.

4) **Nature et présentation des réponses demandées :** Les répondants sont invités à présenter leurs commentaires, suggestions, préoccupations et, le cas échéant, des recommandations pertinentes sur la façon de répondre aux besoins et aux objectifs énoncés dans la présente DDR. Les répondants sont priés d'expliquer les hypothèses qu'ils avancent dans leur réponse.

   a. **Page couverture :** Si la réponse comprend plusieurs volumes, les répondants doivent indiquer sur la page couverture de chaque volume le titre de la réponse, le numéro de la demande de renseignements, le numéro du volume et la dénomination sociale complète du répondant.

   b. **Page du titre :** La première page de chaque volume de la réponse, qui suit la page couverture, devrait être la page du titre et contenir ce qui suit :

      a) Le titre de la réponse et le numéro du volume;
      b) Le nom et l'adresse du répondant;
      c) Le nom, l'adresse et le numéro de téléphone de la personne-ressource désignée par le répondant;
      d) La date; et
      e) Le numéro de la DDR.

   c. **Système de numérotation :** Les répondants sont priés d'utiliser dans leur réponse un système de numérotation correspondant à celui de la présente DDR. Les renvois à des documents descriptifs, des manuels techniques et des brochures faisant partie de la réponse devraient être numérotés en conséquence.

   d. **Nombre de copies :** Le MDN et SPC exigent que les répondants soumettent par courriel une copie de leurs réponses à chacune des organisations.

3. Examen des réponses par le gouvernement du Canada

3.1 Examen des réponses

Les réponses ne feront pas l'objet d'une évaluation officielle. Toutefois, le gouvernement du Canada pourra utiliser les réponses reçues afin d'élaborer ou de modifier sa stratégie d'approvisionnement. Le gouvernement du Canada examinera l'ensemble des réponses reçues avant l'heure et la date de la clôture de la DDR. Il peut, à sa discrétion, les examiner après la date de clôture de la DDR.

3.2 Équipe d'examen

Une équipe d'examen composée de représentants du gouvernement du Canada passera en revue et examinera les réponses. Le gouvernement du Canada peut faire appel à ses propres experts-conseils ou personnes-ressources pour examiner les réponses. Les membres de l'équipe d'examen ne participeront pas nécessairement tous à l'ensemble du processus d'examen.

3.3 Suivi

Le Canada peut, à sa discrétion, communiquer avec tous les fournisseurs pour leur poser des questions supplémentaires ou obtenir des précisions sur un aspect ou l'autre d'une réponse. Le suivi du gouvernement du Canada peut nécessiter une réponse écrite supplémentaire ou une réunion avec les représentants du gouvernement du Canada.

3.4 Rencontres individuelles

Le MDN, SPC et les autres ministères et organismes du gouvernement du Canada se réservent le droit de communiquer avec tout répondant pour poser des questions supplémentaires ou obtenir des précisions sur tout aspect d'une réponse au moyen de rencontres individuelles.

4. Renseignements demandés par le gouvernement du Canada

4.1 Questions pour l'industrie

4.1.1 Environnement de SPC

SPC est responsable des réseaux de 43 ministères. Ces réseaux seront regroupés, mais représentent à l'heure actuelle des environnements distincts. Lorsqu'ils présentent leurs réponses, les fournisseurs doivent tenir compte de la façon dont leur solution sera intégré à l'environnement, notamment selon les caractéristiques et les exigences suivantes :

1) Infrastructures de réseau complexes dotées de différentes enclaves et zones de sécurité, ce qui nécessite des points d'interface de zone et des passerelles d'échange d'information, ainsi que de fournir des commandes et des droits de contrôle à l'équipe responsable du soutien du réseau local et à un système central.

2) Présence de plusieurs clients et réseaux, ce qui nécessite de recourir à un processus d'identification simplifié des biens par client ou réseau (qui peuvent avoir des adresses IP similaires) et d'établir une distinction au moyen de contrôles d'accès entre les clients (p. ex., l'exécution d'une commande pour certains clients plutôt que pour l'ensemble de l'organisation).

3) Réseaux distincts regroupés en un seul réseau.

4) Vastes infrastructures de réseau (plus de 450 000 clients).

5) Environnements virtuels et non virtuels.

6) Temps d'attente élevé et connexions à bande passante étroite au réseau étendu (RE) entre des sites spécifiques.

7) Connexions directes périodiques à l'intranet du gouvernement du Canada (p. ex., des rapports peuvent devoir être stockés jusqu'à la prochaine connexion directe au réseau du gouvernement du Canada de l'appareil de l'utilisateur final, y compris à un réseau privé virtuel [RPV], ou être recueillis sur Internet plutôt que sur le réseau du gouvernement du Canada).

8) Utilisation de dispositifs de chiffrement de calibre commercial et de calibre militaire limités au niveau de la couche réseau.

9) Présence de différents systèmes d'exploitation (serveurs et clients) incluant MS Windows pour les ordinateurs de bureau, les ordinateurs portatifs et les serveurs, Mac OS pour les ordinateurs de bureau et Linux pour les serveurs.

10) Présence de différentes formes de contrôles de ports réseau (couche 2) qui comprennent, sans toutefois s'y limiter, la norme 802.1x et le filtrage MAC.

4.1.2 Environnement du MDN

Lorsqu'ils présentent leurs réponses, les fournisseurs doivent tenir compte de la façon dont leur solution sera intégrée à l'environnement, notamment selon les caractéristiques suivantes :

1) Infrastructures de réseau complexes dotées de différentes enclaves et zones de sécurité ce qui nécessite d'utiliser des points d'interface de zone et des passerelles d'échange d'information.

2) Vastes infrastructures de réseau (plus de 100 000 clients pour le réseau non classifié principal et plus de 8 000 clients pour le réseau classifié principal).

3) Environnements virtuels et non virtuels.

4) Temps d'attente élevé et connexions à bande passante étroite au RE entre des sites spécifiques (réseaux épisodiques déployés à l'échelle mondiale).

5) Utilisation étendue de dispositifs de chiffrement de calibre commercial et de calibre militaire au niveau de la couche réseau.

6) Présence de différents systèmes d'exploitation (serveurs et clients) incluant MS Windows pour les ordinateurs de bureau, les ordinateurs portatifs et les serveurs, et Linux pour les ordinateurs de bureau et les serveurs.

7) Présence de différentes formes de contrôles de ports réseau (couche 2) qui comprennent, sans toutefois s'y limiter, la norme 802.1x et le filtrage MAC.

8) Responsabilité relative à l'environnement de TI partagée entre SPC (p. ex., l'infrastructure de réseaux et de serveurs) et le MDN (p. ex., les applications et les points d'extrémité).

Remarque : Tous les fournisseurs doivent répondre aux questions de la section *Questions générales* et répondre uniquement aux questions de la section *Questions relatives à la fonctionnalité* liées aux catégories pour lesquelles ils souhaitent fournir des renseignements.

4.2 Questions générales

4.2.1 Questions relatives à l'architecture et à l'infrastructure

1) Votre solution offre-t-elle des solutions sans agent ou avec agent?

2) Si votre solution est avec agent, le traitement des tâches (requêtes, évaluations de la vulnérabilité, etc.) est-il effectué centralement ou les données doivent-elles être extraites de façon centralisée aux fins de traitement?

3) Votre solution prend-elle en charge d'autres agents (Mandiant Intelligence Response, GRR Rapid Response, etc.)?

4) Quelles sont les exigences matérielles en vue de l'intégration de votre solution à un réseau existant (fournir un aperçu de l'architecture de base du système, incluant les serveurs, les réseaux et le stockage requis)?

5) Quelles sont les exigences logicielles et techniques en vue de l'intégration de votre solution à un réseau existant?

6) Votre solution peut-elle être intégrée à LDAP (p. ex., Active Directory) aux fins d'authentification?

7) Votre solution offre-t-elle des capacités de gestion répartie et de surveillance hiérarchique (p. ex., les différents ministères peuvent gérer leurs propres ressources, mais la surveillance peut être effectuée de façon centralisée)?

8) Votre solution peut-elle d'appuyer un environnement à clients et réseaux multiples au sein duquel les recherches et les actions effectuées doivent respecter un processus d'identification et de distinction des clients (une action entraîne des changements pour trois clients spécifiques ou une action entraîne des changements pour tous à l'exception de trois clients spécifiques, les rapports par client, etc.)?

9) Votre solution peut-elle être déployée au sein de réseaux dont les zones de sécurité de la TI et les limites diffèrent (expliquer de quelle façon – p. ex., un serveur est-il requis avec chacune des zones)?

10) De quelle façon votre solution permet-elle de résoudre les problèmes d'extensibilité dans le cadre de vastes déploiements (plus de 500 000 clients) en vue de réduire les répercussions pour le réseau (bande passante, disponibilité, etc.)? Quelles sont les exigences relatives à la capacité estimée du réseau par rapport aux points d'extrémité?

11) Votre solution prend-elle en charge les fonctionnalités (balayage, déploiement de mises à jour, etc.) hors bande (p. ex., un chemin d'accès réseau IP non accessible)?

12) Votre solution permet-elle l'extraction et l'utilisation de renseignements hors bande (fichiers journaux, paramètres de sécurité, etc.)?

13) De quelle façon et à quelle fréquence (quotidiennement, sur demande, etc.) votre solution assure-t-elle la tenue à jour des renseignements recueillis à partir des systèmes?

14) Votre solution offre-t-elle une interface de programmation d'applications (API) riche permettant l'intégration à d'autres systèmes tiers :

a. Système de gestion des événements et des incidents de sécurité (SGEIS)?
b. Outils d'analyse de fichiers journaux?
c. Systèmes d'émission de billets de centres d'assistance?
d. Outil de gestion des biens?
e. Outil de gestion de la configuration?
f. Outil de gestion des incidents?
g. Outil de balayage des vulnérabilités?
h. Autres (veuillez préciser)?

4.2.3 Questions relatives à la sécurité, la certification et l'accréditation

15) Votre solution a-t-elle été certifiée ou accréditée par des membres de l'OTAN, des organisations gouvernementales dignes de confiance ou de vastes sociétés privées (banques ou autres)? Le cas échéant, quelles sont les certifications ou les accréditations obtenues?

16) Quels sont les justificatifs d'identité requis pour effectuer des actions ou des activités de balayage à l'échelle d'un réseau, quels sont les mécanismes en place pour le transfert de ces justificatifs à l'échelle du réseau et de quelle façon sont-ils protégés?

17) De quelle façon les communications entre l'autorité centrale et les dispositifs sont-elles protégées? Votre solution peut-elle en charge des technologies et des processus de gestion des clés approuvés par le CSTC?

18) Si des clés de chiffrement sont utilisées, de quelle façon celles-ci sont-elles protégées sur les ordinateurs principaux?

19) Votre solution offre-t-elle des contrôles d'accès granulaires fondés sur les rôles et permet-il de gérer les autorisations selon les responsabilités des utilisateurs?

20) Votre solution offre-t-elle des fonctionnalités de sécurité et de vérification? À quel endroit les fichiers journaux sont-ils stockés (de façon locale, centrale ou les deux)?

21) Votre solution comprend-elle d'autres fonctionnalités de sécurité (veuillez préciser)?

4.2.4 Questions relatives à la personnalisation

22) Quelles sont les capacités de production de rapports offertes par votre solution? Quels sont les formats pris en charge pour ces rapports (PDF, RTF, MS Word, etc.)? Ces rapports peuvent-ils être personnalisés?

23) Quelles sont les capacités offertes par votre solution en ce qui a trait aux tableaux de bord? Dans quelle mesure les tableaux de bord peuvent être personnalisés? Les tableaux de bord peuvent-ils inclure des renseignements provenant de solutions d'autres fabricants?

24) Votre solution permet-elle aux utilisateurs de créer des requêtes et des recherches personnalisées relativement à des renseignements spécifiques? Quels sont les langages et les mécanismes utilisés (format de type moteurs de recherche Internet, expressions régulières, etc.)?

25) Votre solution permet-elle d'utiliser des scripts personnalisés en vue d'automatiser certaines de ses fonctionnalités? Quel est le langage utilisé ou pris en charge par votre solution?

26) Votre solution offre-t-elle des capacités analytiques et d'analyse des tendances (veuillez préciser)?

27) Quelles sont les langues et les mesures de soutien régional offertes par votre solution (FR-CA, EN-CA, etc.)?

4.2.5 Questions relatives au soutien du fournisseur

28) Quelle est la fréquence de diffusion des mises à niveau de la solution ou des nouvelles capacités, et quelle est la période pendant laquelle le soutien des anciennes versions est assuré?

29) Quelle est la fréquence de diffusion des correctifs et/ou des ensembles de modifications provisoires de votre solution et quels sont les mécanismes utilisés pour appliquer les correctifs et les mises à niveau?

30) Quel est le processus utilisé pour installer les mises à niveau et les correctifs sans connexion directe à Internet?

31) Le fournisseur de votre solution autorise-t-il les essais de configuration au sein d'un environnement de laboratoire du gouvernement du Canada?

32) Quel est le modèle de licence de votre solution (licence avec inscription, licence perpétuelle avec frais annuels, etc.)?

33) Quel est le modèle de soutien de votre solution (p. ex., le soutien direct par le fabricant d'équipement d'origine ou le soutien offert par un tiers)?

4.3 Questions relatives aux fonctionnalités

4.3.1 Questions relatives à la gestion des biens de technologie de l'information et à la gestion de la configuration

34) Votre solution peut-elle détecter les dispositifs suivants sur un réseau?

a. Équipement réseau (routeurs, commutateurs, pare-feu, passerelles de RPV, etc.) ?
b. Ordinateurs principaux et serveurs?
c. Imprimantes et appareils multifonctions?
d. Points d'accès sans fil?
e. Dispositif de vidéoconférence?
f. Ordinateurs de bureau et clients légers (incluant les appareils directement connectés comme les imprimantes, les dispositifs de stockage USB, les cartes et les dispositifs sans fil, etc.)?
g. Hyperviseurs (p. ex., VMware, IBM pSeries; veuillez préciser)?
h. Machines virtuelles (p. ex., invité virtuel Windows ou Linux)?
i. Appareils voix sur IP (VoIP)?
j. Appareils mobiles? Veuillez préciser lesquels (Android, Apple, BlackBerry, Windows, etc.)?
k. Autres (veuillez préciser)?

35) Votre solution peut-elle détecter les dispositifs ci-dessus sans le recours à des agents installés utilisant des protocoles comme ICMP, SNMPv3 et le balayage de ports?

36) Votre solution permet-elle le regroupement dynamique des dispositifs découverts selon leur configuration dans le but d'entreprendre des actions spécifiques à chacun (p. ex., l'installation logicielle fondée sur des conditions ou la collecte de renseignements de configuration axée sur des conditions)?

37) Votre solution offre-t-elle la possibilité de transmettre des alertes lorsque des événements spécifiques surviennent (nouveaux dispositifs découverts, inaccessibilité, seuil de saturation du lien au réseau, etc.)?

38) Votre solution offre-t-elle la possibilité de découvrir des connexions entre les dispositifs du réseau?

39) Votre solution offre-t-elle la possibilité d'afficher de façon graphique ou visuelle la topologie du réseau?

40) Votre solution peut-elle surveiller l'état des dispositifs associés au réseau?

41) Votre solution peut-elle fournir des données et des statistiques historiques relatives à l'utilisation du matériel (utilisation de l'unité centrale et de la mémoire, utilisation du disque, etc.)? Quel type de données et de statistiques votre solution peut-elle fournir?

42) Votre solution peut-elle surveiller l'utilisation du lien au réseau en ce qui a trait aux commutateurs, aux routeurs, aux pare-feu, etc.?

43) Votre solution peut-elle surveiller les renseignements relatifs à la configuration pour les dispositifs suivants :

    a. Équipement réseau (routeurs, commutateurs, pare-feu, passerelles de RPV, etc.)
    b. Ordinateurs principaux et serveurs?
    c. Imprimantes et appareils multifonctions?
    d. Points d'accès sans fil?
    e. Dispositif de vidéoconférence?
    f. Ordinateurs de bureau et clients légers (incluant les appareils directement connectés comme les imprimantes, les dispositifs de stockage USB, les cartes et les dispositifs sans fil, etc.) ?
    g. Hyperviseurs (p. ex., VMware, IBM pSeries; veuillez préciser)?
    h. Machines virtuelles (p. ex., invité virtuel Windows ou Linux) ?
    i. Appareils voix sur IP (VoIP)?
    j. Appareils mobiles? Veuillez préciser lesquels (Android, Apple, BlackBerry, Windows, etc.)?
    k. Autres (veuillez préciser)?

44) Quel est le type de renseignements de configuration pouvant être recueillis pour chacun des types de dispositifs désignés dans les questions précédentes (p. ex., pour l'ordinateur principal : version du système d'exploitation, version des correctifs, paramètres de registre, etc.; pour les routeurs : version logicielle, interfaces actives, etc.)?

45) Des scripts personnalisés peuvent-ils être déployés avec votre solution en vue de recueillir des renseignements de configuration supplémentaires? Quel est le langage utilisé ou pris en charge par votre solution?

46) Votre solution peut-elle intégrer et exécuter des essais de conformité de la configuration de type Security Content Automation Protocol (SCAP)?

47) Votre solution offre-t-elle une interface de programmation d'application (API) permettant d'exporter et d'importer des requêtes et des résultats SCAP à partir d'outils tiers et vers ceux-ci?

48) Votre solution offre-t-elle la possibilité de transmettre des alertes et de résoudre les problèmes de configuration relevés par rapport aux dispositifs du réseau (et ainsi de garantir la conformité à une configuration de base spécifique)?

49) Votre solution peut-elle être intégrée au langage Open Vulnerability and Assessment Language (OVAL)?

50) Votre solution peut-elle établir une connexion directe à des bases de données de vulnérabilités et de gestion de la configuration provenant de sources ouvertes, comme la base de données National Vulnerability Database (NVD) et la Base de données de gestion des configurations (BDGC)?

51) Votre solution peut-elle être intégrée à des systèmes à l'aide des langages Structured Threat Information eXpression (STIX), Trusted Automated Exchange of Indicator Information (TAXII) et Cyber Observable Expression (CybOX) en vue de consulter et de fournir des renseignements relatifs aux cybermenaces (p. ex., les indicateurs de compromission)?

52) Votre solution permet-elle d'appuyer des partenariats ou des alliances courants au sein de l'industrie offrant une valeur ajoutée au moyen de l'intégration à d'autres solutions? Le cas échéant, quels sont les partenariats, les alliances, les solutions et les API en question?

53) Votre solution peut-elle être intégrée à LDAP (p. ex., Active Directory) aux fins de l'extraction de renseignements supplémentaires sur les biens (emplacement physique, utilisateur assigné, but, etc.)?

54) Votre solution comprend-elle une fonctionnalité d'intégration des données provenant de multiples balayages (p. ex., la comparaison entre de multiples codes d'horodatage et entre de multiples réseaux locaux d'un même réseau étendu)?

55) Des droits et des autorisations pour les activités de balayage peuvent-ils être accordés selon les contrôles d'accès granulaires fondés sur les rôles?

56) Votre solution offre-t-elle la possibilité d'exporter des renseignements sur les biens en format XML ou CSV?

4.3.2 Questions relatives à la gestion des licences logicielles

57) Votre solution peut-elle fournir les renseignements suivants en ce qui a trait à la gestion des applications et des logiciels?

a. Liste des applications installées sur l'ordinateur principal ou le serveur et les postes de travails, dont :

a) La version?
b) La date de sortie?
c) Les clés de licences et les identifiants utilisés?
d) Le fabricant et l'éditeur?

b. Données et statistiques historiques sur l'utilisation (logiciel de comptage), dont :

a) L'installation (nombre d'instances logicielles)?
b) La date d'installation?
c) La dernière date d'utilisation?
d) L'utilisation au cours d'une période donnée?

58) Votre outil peut-elle effectuer des recherches et recueillir des renseignements au sujet de logiciels à l'aide d'un format normalisé (p. ex., une recherche pour Adobe devrait également donner les résultats Adobe Systems, Adobe systems Inc., Adobe Inc., etc.)?

59) Votre solution offre-t-elle un module de gestion des licences et des mécanismes automatisés permettant de vérifier la conformité en ce qui a trait notamment aux éléments suivants :

a. Respect du nombre de licences spécifiées dans les contrats?
b. Licences en surplus (non utilisées)?
c. Utilisation concurrente de licences?
d. Capacité d'assurer le suivi et la gestion de différents modèles complexes de licence (Oracle, IBM, VMware, Microsoft, etc.)?

60) Votre solution prend-elle en charge la valorisation des licences à distance (le processus permettant de transférer les licences logicielles non utilisées des utilisateurs actuels et de les réassigner à d'autres utilisateurs)?

61) Votre solution peut-elle réaliser les activités de gestion des licences susmentionnées pour :

a. Les appareils mobiles? Veuillez préciser lesquels (Android, Apple, BlackBerry, Windows, etc.) ?
b. Les machines virtuelles?
c. Les ordinateurs de bureau et les clients légers?
d. Les serveurs et les ordinateurs principaux?

4.3.3 Questions relatives à la gestion et au déploiement des logiciels et des correctifs

62) Votre solution permet-elle de déployer et d'installer des correctifs et des logiciels à l'échelle d'un réseau (veuillez expliquer la façon dont les correctifs et les logiciels sont déployés)?

63) Votre solution permet-elle de dresser des listes blanches et des listes noires d'applications et de logiciels sur le réseau?

64) Votre solution permet-elle d'effectuer des procédures de retour en arrière dynamiques ou manuelles pour les logiciels préalablement installés?

65) Votre solution offre-t-elle la possibilité d'effectuer des actions antérieures ou postérieures à l'application de trousses de déploiement (p. ex., les tâches faisant partie du processus lié aux trousses logicielles, comme l'interruption et le lancement de services, la copie de fichiers vers des emplacements spécifiques, la transmission d'avis aux utilisateurs, etc.)?

66) Votre solution offre-t-elle la possibilité de personnaliser le processus d'application de correctifs au moyen de règles et d'exceptions définies et de calendriers prédéfinis?

67) Votre solution offre-t-elle des mesures de rendement en ce qui concerne la gestion des correctifs et le déploiement de logiciels, comme le nombre de correctifs diffusés par mois, les taux de réussite et d'échec des correctifs (par correctif), des indicateurs d'état (p. ex., 95 % – Bon état; mesure quotidienne), etc.?

68) Votre solution offre-t-elle la possibilité de produire des rapports sur les relations et les dépendances entre les applications? Quel est le type de relations (p. ex., un à un, un à plusieurs)?

69) Votre solution permet-elle de s'assurer que les codes d'horodatage correspondent à l'heure et à la date auxquelles les renseignements ont été balayés et vérifiés, plutôt qu'à l'heure et à la date auxquelles le rapport a été produit?

70) Votre solution offre-t-elle la possibilité de déployer des systèmes d'exploitation d'ordinateur de bureau ou de serveur vers les dispositifs aux points d'extrémité à l'échelle du réseau, dont :

   a. des fonctions évoluées, comme les vérifications de la conformité des dispositifs aux points d'extrémité avant leur déploiement et l'application d'une logique évoluée de déploiement de systèmes d'exploitation (p. ex., l'installation de logiciel selon des conditions dans le cadre du déploiement d'un système d'exploitation)?

   b. Votre solution offre-t-elle la possibilité d'installer des pilotes matériels de base (p. ex., des fichiers .inf) sur les systèmes d'exploitation d'ordinateurs de bureau et de serveurs?

   c. Votre solution offre-t-elle la possibilité de déployer des systèmes d'exploitation d'ordinateurs de bureau et de serveurs en vue de déconnecter des dispositifs aux points d'extrémité à l'aide de supports hors ligne (p. ex., les supports de stockage USB)?

   d. Votre solution offre-t-elle la possibilité de déployer des systèmes d'exploitation d'ordinateurs de bureau et de serveurs vers des systèmes UEFI?

   e. Votre solution permet-elle l'intégration à des utilitaires de gestion de pilotes matériels, comme Deploy Expert, ENGL Driver Manager et Big Bang LLC Universal Imaging Utility?

   f. Votre solution offre-t-elle la possibilité de déployer et de gérer des logiciels virtuels, et plus particulièrement les trousses logicielles Microsoft App-V et VMware ThinApp?

71) Votre solution permet-elle de réaliser les activités de gestion des logiciels et des correctifs susmentionnées à partir de ce qui suit :

   a. les appareils mobiles? Veuillez préciser lesquels (Android, Apple, BlackBerry, Windows, etc.)?
   b. les machines virtuelles?
   c. les ordinateurs de bureau et les clients légers?
   d. les serveurs et les ordinateurs principaux?

4.3.3 Questions relatives à la détection des incidents et à la réponse aux incidents

72) Votre solution peut-elle fournir les plus récents renseignements d'inventaire suivants au sujet des ordinateurs principaux?

   a. Processus et scripts en cours d'exécution?
   b. Liste des fichiers couramment ouverts par les utilisateurs?
   c. Écoute des ports de données du réseau?
   d. Connexions réseau établies?
   e. Paramètres du registre?
   f. Comptes d'utilisateur en cours d'utilisation ?
   g. Dispositifs directement connectés (p. ex., les dispositifs USB)?
   h. Renseignements sur les registres d'événements?
   i. Autres (veuillez préciser)?

73) Votre solution peut-elle détecter les dispositifs non autorisés et/ou inconnus sur un réseau?

74) Votre solution peut-elle surveiller l'intégrité des fichiers et diffuser des alertes automatisées en temps réel lorsque des changements surviennent en ce qui concerne les fichiers exécutables essentiels? Votre solution peut-elle prévenir les changements aux fichiers exécutables essentiels?

75) Votre solution peut-elle reconnaître et évaluer les situations de compromission possibles au moyen d'indicateurs, comme les noms de fichiers, les chemins d'accès aux fichiers, les paramètres de registre, les adresses IP, le trafic sur le réseau, les empreintes de fichiers ou les comportements suspects observables?

76) Votre solution peut-elle intégrer des flux de données sur les menaces provenant de services de source ouverte (Virus Total, ThreatStream, McAfee TIE, Yara, OpenIOC, etc.) et vérifier automatiquement l'infrastructure pour déceler la présence de ces indicateurs?

77) Quelles sont les fonctionnalités de réponse aux incidents à distance offertes par votre solution (processus d'arrêt à distance, arrêt des services ou des ports, modification des paramètres de registre, etc.)?

78) Votre solution peut-elle de transmettre des avis aux utilisateurs des dispositifs aux points d'extrémité? Est-il possible de sélectionner la langue de ces avis? Ces avis peuvent-ils être personnalisés?

79) Quelles sont les capacités de corrélation offertes par votre solution en ce qui a trait à la détection des menaces et des incidents?

80) Quelles sont les capacités de coordination offertes par votre solution en ce qui a trait à la réponse aux menaces (p. ex., lorsqu'un fichier malicieux est détecté dans un système, votre solution peut-elle résoudre ce problème rapidement sur tous les systèmes de l'organisation, notamment en empêchant l'enregistrement et l'exécution de copies du fichier en cause)?

81) Quelles sont les méthodes offertes par votre solution pour établir la priorité des menaces et signaler celles-ci aux responsables de la sécurité?

82) Votre solution inclut-elle une fonction de gestion des cas permettant de conserver des documents au sujet des incidents et de leur résolution (p. ex., la rédaction de rapports d'analystes expliquant les raisons pour lesquelles certaines mesures ont été prises pour donner suite à un incident)?

4.3.4 Questions relatives à l'investigation informatique pour les appareils à distance

83) Votre solution peut-elle consigner et fournir des données historiques au sujet des activités suivantes liées aux points d'extrémité; le cas échéant, pendant combien de temps ces données sont-elles conservées?

a. Fichiers consultés?
b. Fichiers créés?
c. Connexions réseau établies?
d. Processus et scripts exécutés?
e. Applications installées?
f. Applications, commandes et scripts utilisés?
g. Comptes d'utilisateurs en cours d'utilisation?
h. Registres d'événements?
i. Utilisation du navigateur Internet?
j. Autres (veuillez préciser)?

84) Votre solution permet-elle d’accroître la mémoire disponible à distance et en temps réel?

85) Votre solution permet-elle d’extraire des artéfacts d’enquête à distance en temps réel (p. ex., l’extraction de fichiers suspects aux fins d’inspection)?

86) De quelle façon l’intégrité de ces artéfacts est-elle préservée pendant l’extraction ou le transfert de fichiers?

87) De quelle façon votre solution permet-elle l’analyse hors ligne et en temps réel de ces artéfacts? L’analyse doit-elle être réalisée à partir d’un emplacement central ou peut-elle être réalisée à l’aide d’une interface à distance?