350 Albert Street, Suite 700
Ottawa, Ontario K1A 0S6
Canada

350, rue Albert, Bureau 700
Ottawa, Ontario K1A 0S6
Canada

ADDENDA N° 2

Questions et réponses (Q&R) N° 2

DP n° : 106205.138

SERVICES DE SÉCURITÉ GÉRÉS (SSG)

Le 11 septembre 2023

N°	Questions	Réponses
1	L'Appendice 1 de l'annexe A fait référence à 250 points terminaux. Veuillez fournir des détails sur ces points d'accès. S'agit-il d'une combinaison de postes de travail, de serveurs ou des deux ? Veuillez fournir des détails.	Combinaison de postes de travail et de serveurs.
2	L'annexe A fait référence aux actifs sur site et en nuage. Veuillez confirmer le nombre de centres de données et de fournisseurs de services en nuage.	Microsoft est le principal système en nuage. Il existe une poignée d'autres systèmes en nuage essentiels que nous pourrions également prendre en considération, par exemple le SIRH.
3	La CCC exige-t-elle que les services soient fournis par des ressources canadiennes ? Dans l'affirmative, ces ressources ont-elles besoin d'une habilitation de sécurité canadienne ?	Oui. Une habilitation de sécurité serait préférable.
4	La CCC exige que la solution soit conforme à la directive du gouvernement du Canada sur la résidence des données électroniques. Pour ce faire, l'auteur de la proposition demande des éclaircissements sur la manière dont la CCC classifie ses données. Comment la CCC classe-t-elle et catégorise-t-elle (Protégé B, C, autre) les informations spécifiques dans le cadre des services requis, y compris les journaux et les données collectées dans le SIEM.	Nous ne savons pas exactement comment la classification des données s'applique aux données d'enregistrement dans le cadre de ce projet. La CCC suit les niveaux de classification de sécurité du PSPC, mais ils ne sont pas systématiquement appliqués dans l'ensemble de l'organisation.
5	Nous comprenons que la CCC n'a pas d'exigences spécifiques pour le test de pénétration annuel. Toutefois, veuillez confirmer que la CCC n'attend pas de prix pour cette capacité à ce stade.	Ces services de test de pénétration ne sont pas inclus dans les critères d'évaluation et ne seront pas notés. Toutefois, ces services ainsi que d'autres services liés aux meilleures pratiques seront exigés.
6	Les services de test de pénétration peuvent-ils être fournis à distance par une équipe internationale ?	Non.

7	À un niveau élevé, veuillez décrire votre processus actuel de gestion et de réponse aux incidents de sécurité.	Il est en cours d'élaboration, mais nous avons besoin de l'expertise d'un tiers pour nous aider à remédier et à réagir en cas d'incident, d'où le présent appel d'offres.
8	Veuillez indiquer la fréquence ou le calendrier de la chasse au Dark Web.	Inconnu, nous voulons travailler avec le partenaire pour dimensionner et adresser correctement cette organisation.
9	Veuillez confirmer : Nous comprenons, d'après la section 1.4.1, qu'une fois sélectionné, le soumissionnaire devra fournir les conditions générales et la description du service pour examen.	Oui.
10	La section 1.4.2 ne précise pas le nombre de renouvellements. La CCC peut-elle préciser le nombre maximum de renouvellements annuels dans le cadre du contrat qui en résultera ?	Non.
11	Veuillez confirmer quels sont les agents EDR et antivirus actuellement déployés (ou dont le déploiement est prévu) sur l'infrastructure de la CCC.	Microsoft 365 Defender (MDE, MDO, MDI), Windows Defender AV, Symantec AV.
12	Les agents EDR et les antivirus sont-ils déployés sur tous les actifs de l'infrastructure (à la fois dans les locaux et dans le nuage) ?	Oui, à quelques exceptions près.
13	Combien d'incidents majeurs ou critiques la CCC a-t-elle subis au cours des 12 derniers mois ?	Zéro.
14	Si vous disposez d'une solution SIEM actuelle :	Non.
15	- Combien d'EPS ou de MPS (événements/messages par seconde) votre solution actuelle génère-t-elle ?	S/O.
16	- Si ce n'est pas le cas, combien de Gb par jour/mois de données de journalisation recueillez-vous ?	Moins de 1 Go/jour dans les locaux (sur la base des journaux d'audit du pare-feu / AD) ; les journaux M365 sont difficiles à estimer. L'organisation comprend environ 120 utilisateurs actifs et nous utilisons les capacités de journalisation de l'E5.
17	- Combien de cas d'utilisation avez-vous actuellement ou aimeriez-vous que nous développions ?	Nous ne comprenons pas cette question.
18	- Avez-vous des playbooks SOAR configurés ? Si oui, combien ?	Non.
19	Quel est le nombre de sites où sont déployés des serveurs (sources de logs) ?	Un centre de données sur site et quelques systèmes basés sur le cloud. La portée complète devra être déterminée. La CCC est une petite organisation.
20	Le délai peut-il être prolongé de deux semaines ?	Non.

21	Veuillez confirmer que les serveurs d'application, SQL et DC font partie des 40-50 machines virtuelles.	Oui.
22	Pour l'intégration avec le système central de billetterie CCC Team Dynamix, veuillez confirmer que les notifications par courriel répondront à vos besoins.	Le courrier électronique devrait suffire, mais l'intégration de l'API serait idéale.
23	Afin de vous fournir une réponse de qualité, nous demandons respectueusement une prolongation jusqu'au 6 octobre 2023.	Une extension n'est pas accordée.
24	Il y a une demande concernant l'intégration avec le système de billetterie de l'équipe CCC. Comment ce système de billetterie est-il censé être utilisé ? Veuillez préciser.	Quelle que soit la méthode habituellement utilisée avec vos autres clients.
25	Section 4.2, point concernant l'installation et la configuration du SIEM. Le délai prévu est de 45 jours entre la signature et l'achèvement de l'intégration. Est-ce que TOUTES les sources de logs et TOUTES les règles de cas d'utilisation doivent être mises en œuvre dans ces 45 jours ?	Le SIEM doit être basé sur le cloud. La flexibilité est de mise pour tous les fichiers journaux.
26	Section 4.2, il est fait référence aux accords de niveau de service pour le contrôle de la sécurité, mais les détails ne sont pas donnés (ou ne sont pas clairs). Pouvez-vous préciser les attentes en matière d'"accords de niveau de service" ?	Veuillez indiquer ce que vous fournissez à la majorité des clients.
27	L'exigence de conservation en ligne pendant 3 mois est-elle obligatoire ?	Oui.
28	En ce qui concerne le système de billetterie central Dynamix, pourrions-nous préciser s'il s'agit du système de billetterie de Microsoft Dynamics 365 ou de Team Dynamix ITSM ?	Team Dynamix ITSM.
29	Avez-vous un ELA (Enterprise License Agreement) avec Microsoft ?	Oui.
30	Pour les besoins de l'équipe de réponse aux incidents, veuillez confirmer le nombre d'heures par an pour la rémunération de la réponse aux incidents.	Le fournisseur devrait fournir cette estimation sur la base de son expérience.
31	Quel est le nombre d'utilisateurs ? (Utilisateur : une personne disposant d'une adresse électronique et d'un appareil appartenant à l'entreprise).	120 utilisateurs.
32	Quel est le nombre d'utilisateurs d'Office 365 ?	120 utilisateurs.

33	Combien de sites comptant plus de 50 utilisateurs, des serveurs sur place, un accès direct à l'internet et un pare-feu possédez-vous ? (si vous utilisez une technologie comme Zscaler pour relier l'internet à un site principal, cela compte pour un site).	Un seul site, la majorité du personnel travaille à distance avec des appareils clients gérés.
34	Quels sont vos environnements en nuage (AWS, Azure, GPS) et quel est votre niveau de licence ?	Locataire Microsoft 365 avec licence E5 ; Azure AD (pas encore de VM ou d'autres IaaS déployés dans Azure) ; SIRH, site web de l'entreprise (Wordpress).
35	Combien de serveurs avez-vous dans votre environnement (sur site, dans le nuage, physique et virtuel) ?	Environ 50.
36	Disposez-vous d'appareils dotés d'un système d'exploitation Windows de base en français ou d'un système d'exploitation anglais sur lequel est ajouté un pack linguistique français ?	Non.
37	Est-il entendu que le fournisseur inclus le prix du système SIEM dans la proposition? Si oui, serait-il possible de fournir les informations suivantes ; Quantités de log journalier du pare-feux?	Moins de 1 Go/jour dans les locaux (sur la base des journaux d'audit du pare-feu / AD) ; les journaux M365 sont difficiles à estimer. L'organisation comprend environ 120 utilisateurs actifs et nous utilisons les capacités de journalisation de l'E5.
38	Acceptez-vous que le SIEM soit hébergé dans vos environnements Azure/Microsoft avec une facturation directement intégré dans votre contrat Microsoft?	Il s'agit d'un SIEM basé sur le cloud et géré par le fournisseur.
39	Est-ce que vous acceptez d'avoir une machine virtuelle (linux) agissant comme collecteur et filtreur de log/journaux? • Cette machine virtuelle étant la responsabilité du CCC au niveau maintien?	Oui.
40	Serait-ce possible de fournir le manufacturier de la grappe de pare-feux?	Watchguard.
41	Mis à part les outils/équipements mentionnés dans l'annexe A, existe d'autres sources de Logs à intégrer dans le SIEM (ex. Darktrace, système maison, applications, ...) ?	Oui.
42	Quelle est la taille actuelle de votre équipe de cybersécurité et le nombre de personnes chargées de surveiller les alertes et d'y répondre ?	1 personnel.
43	Veuillez nous faire part des points douloureux et de toute exigence critique en matière de services de sécurité qui nécessiterait une attention immédiate ?	S/O.

44	La CCC fait-elle actuellement partie d'une communauté d'échange de renseignements sur les menaces ? Dans l'affirmative, ces flux sont-ils déjà intégrés au SIEM ?	S/O.
45	La CCC est-elle ouverte à une solution SIEM telle que Microsoft Sentinel qui sera déployée dans son environnement ?	Le besoin porte sur un SIEM basé sur le cloud et géré par le fournisseur.
46	Est-il possible de fournir une ventilation du nombre d'utilisateurs ?	120 utilisateurs.
47	Combien d'adresses IP externes doivent être testées dans le cadre du test de pénétration annuel ?	Environ 5.
48	Y a-t-il des applications web et, dans l'affirmative, combien y en a-t-il ?	1 application web.
49	Existe-t-il un nombre de Go/jour ou d'événements par seconde (EPS) prévus pour le SIEM ?	Notre empreinte totale est assez faible et nous n'avons donc pas prévu de nombre minimum d'EPS ou de Go/jour.
50	Existe-t-il un diagramme du réseau ?	Nous pouvons fournir des diagrammes de réseau rudimentaires.
51	Quels sont les services en nuage utilisés en dehors d'O365, comme Azure, AWS, Google ?	WP Engine pour nos sites Wordpress qui utilise Google Cloud Platform.
52	Microsoft Defender est-il la solution AV/EDR actuelle ou une autre solution est-elle déployée ?	Pour les appareils distants, oui, sur place nous utilisons Symantec SEP avec un serveur de gestion SEPM sur place.
53	Compte tenu du fait que vous disposez actuellement d'une licence E5, avez-vous envie de poursuivre sur la voie de Microsoft avec Microsoft Sentinel (SIEM) ?	Oui, nous serions ouverts à l'utilisation de Sentinel car il est logique de consolider sous l'égide de Microsoft, mais nous sommes également ouverts à d'autres solutions potentielles.
54	Quel est le nombre actuel d'employés ?	Environ 120 membres actifs.
55	Quel est l'assureur actuel en matière de cybersécurité ?	Coalition.
56	Utilisez-vous un outil d'analyse des vulnérabilités ?	Nessus.
57	Existe-t-il un plan de RI en vigueur ? Si oui, a-t-il été revu ?	Il est en cours d'élaboration, mais nous avons besoin de l'expertise d'un tiers pour nous aider à remédier et à réagir en cas d'incident, d'où le présent appel d'offres.
58	Nous travaillons avec un sous-traitant dont le pipeline de données passe par AWS en Irlande sans être stocké. La location reste au Canada. Cette situation serait-elle acceptée par la CCC ?	Nous envisagerons cette solution.
59	Le promoteur et/ou le sous-traitant travaillant sur ce projet doivent-ils obtenir une habilitation de sécurité ?	Elle constituerait un atout, mais n'est pas obligatoire.

FIN AUX Q&R N° 2