Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A-7 : Énoncé des travaux – Gestion des informations et des événements de sécurité

Date : 12 juillet 2012

TABLE DES MATIÈRES

RÉFÉRENCE

Voir l'appendice C : Définitions et acronymes de l'annexe A pour obtenir une définition des termes et des acronymes utilisés dans la présente annexe.

1 GESTION DES INFORMATIONS ET DES ÉVÉNEMENTS DE SÉCURITÉ

(1) La gestion des informations et des événements de sécurité (GIES) constitue un des services de gestion des menaces du SSGGC. Lorsque le Canada en fait la commande par l'émission d'une autorisation de tâches, la GIES, telle qu'elle est gérée et mise en œuvre par l'entrepreneur, doit respecter ou dépasser toutes les exigences mentionnées dans la présente annexe et dans le reste de l'Énoncé des travaux, ainsi qu'ailleurs dans le contrat, et ce, avant son acceptation par le Canada et tout au long de la durée du contrat.

1.1 Collecte de données

(2) La GIES doit recueillir simultanément les renseignements concernant les événements, les journaux de sécurité et les journaux opérationnels (p. ex. utilisation de l'unité centrale et de la mémoire vive) et provenant d'une multitude de sources dont :

a) Les routeurs;

b) Les commutateurs;

c) Les pare-feu;

d) Le SDI/SPI;

e) Les bases de données;

f) Les serveurs Web;

g) Les agents antivirus et antipourriel;

h) Les serveurs Syslog;

i) Les serveurs mandataires Internet;

j) Les passerelles de courrier électronique et les ATM;

k) Les scanneurs de vulnérabilités;

l) Les scanneurs d'actifs;

m) Les scanneurs d'incidents de sécurité;

n) Les services de gestion des menaces du SSGGC;

o) Les RPV et les dispositifs d'accès à distance;

p) Les points d'accès sans fil et les capteurs;

q) Windows Server 2003 et supérieur;

r) Solaris;

s) IBM-AIX;

t) HP-UX;

u) Unix;

v) Linux (Redhat);

w) Toutes autres sources tel qu'en conviennent l'entrepreneur et le Canada.

(3) La GIES doit recueillir les données en recourant à au moins une des méthodes suivantes :

a) Agent collecteur sur le dispositif source;

b) Connexion directe au dispositif source;

c) Collecte des fichiers journaux;

d) Toutes autres méthodes tel qu'en conviennent l'entrepreneur et le Canada.

(4) La GIES doit pendre en charge la traversée TAR pour permettre la collecte d'événements au-delà des limites TAR.

(5) La GIES doit normaliser les données brutes recueillies selon une structure de données commune, dans un référentiel commun propre à l'organisation cliente.

(6) La GIES doit conserver une copie des données brutes recueillies.

(7) La GIES doit maintenir un lien entre les données normalisées et le données brutes recueillies.

(8) La GIES ne doit pas omettre de données brutes entrantes.

(9) La GIES soit stocker les données sur un réseau de stockage que précise le Canada pour l'organisation cliente.

1.2 Détection et réponse

(10) La GIES doit corréler les données normalisées en fonction de règles déterminées par le Canada.

(11) La GIES doit analyser les données entrantes, les comparer par rapport à des politiques ou règles de comportement normal et faire état de tout écart.

(12) La GIES doit analyser les données entrantes, les comparer par rapport à des politiques ou règles personnalisées de comportement normal précisées par le Canada et faire état de tout écart.

(13) La GIES doit analyser les données entrantes et concevoir automatiquement des règles ou des politiques de comportement normal en fonction des événements observés.

(14) La GIES doit corréler les alertes visant les opérations avec celles visant la sécurité et provenant d'une source commune.

1.3 Configuration

(15) La GIES doit permettre la configuration des politiques ou règles personnalisées de comportement normal.

(16) La GIES doit comprendre des périodes configurables de conservation et d'archivage des données.

1.4 Mises à jour de sécurité automatiques

(17) La GIES doit prendre en charge les mises à jour de sécurité automatiques des politiques ou règles exécutées directement depuis Internet (c'est-à-dire sans dépendre d'un dispositif intermédiaire) toutes les heures, au plus.

(18) L'entrepreneur doit fournir les mises à jour de sécurité automatiques dans les 15 minutes suivant le moment où le fournisseur les rend disponibles.

(19) La GIES doit appliquer les mises à jour de sécurité sans redémarrage dans les 15 minutes suivant leur réception.

1.5 Protocoles de collecte d'événements et de journaux

(20) La GIES doit prendre en charge les protocoles de collecte des événements et des journaux qui suivent :

a) Syslog;

b) APD de Microsoft;

c) Cisco RDEP;

d) OPSEC LEA;

e) Déroutement SNMP;

f) HTTP;

g) HTTPS;

h) Microsoft WMI;

i) SDEE;

j) NetFlow version 9 et supérieur;

k) IPFIX;

l) Journal des événements Windows;

m) Tout autre protocole de collecte d'événements ou de journaux tel qu'en conviennent l'entrepreneur et le Canada.

1.6 Sécurité

(21) La GIES doit protéger en tout temps la confidentialité et l'intégrité des données brutes recueillies et des données normalisées.

(22) La GIES doit stocker les données brutes recueillies et les données normalisées dans les locaux de l'organisation cliente.

1.7 Rapports

(23) La GIES doit produire des rapports de conformité (HIPPA, SOAX, etc.) préétablis.

1.7.1 Rapports mensuels

(24) L'entrepreneur doit fournir au Canada un rapport mensuel concernant la gestion de la GIES; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé comparant le nombre d'événements survenus pendant le mois courant par rapport au mois précédent et présentant en termes simples les écarts et les facteurs qui expliquent ces statistiques;

b) Le nombre de billets d'incident du type « demande d'information » en suspens;

c) Le résumé, sous forme de tableau, concernant la gestion d'un problème;

i) L'état du billet d'incident (ouvert, fermé, en suspens);

ii) Le numéro du billet d'incident;

d) Le nombre de demandes de changement traitées;

e) Une liste, sous forme de tableau, des billets d'incident du type « demande d'information » indiquant :

i) La date de fermeture;

ii) La date de création;

iii) Le numéro de billet;

iv) La gravité de l'incident;

v) La description de l'incident;

vi) Les commentaires;

vii) L'état de l'incident;

viii) Le temps de réponse (en secondes);

ix) Le temps de confinement (en secondes);

f) Une liste, sous forme de tableau, des billets relatifs aux demandes de changement indiquant :

i) Le numéro de billet;

ii) La description du changement;

iii) Les commentaires;

iv) L'état.

1.7.2 Rapports quotidiens

(25) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la GIES par dispositif source; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principaux dispositifs source, où :

i) Le nombre total d'événements concernant le dispositif source figure sur l'axe x;

ii) Le nom du dispositif source figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) Le dispositif source;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

(26) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la GIES selon la gravité de l'événement; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à colonnes empilées, des événements survenus pendant les deux semaines précédentes, où :

i) La date de l'événement figure sur l'axe x;

ii) Le nombre total d'événements selon la gravité, empilés, figure sur l'axe y;

b) Un résumé des événements survenus pendant les deux semaines précédentes, présentés sous forme de tableau, indiquant :

i) La date de l'événement;

ii) La gravité de l'événement;

iii) Le nombre d'événements.

(27) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la GIES par IP source; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principales IP source, où :

i) Le nombre total d'événements concernant l'IP source figure sur l'axe x;

ii) L'IP source figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) L'IP source;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

(28) L'entrepreneur doit fournir au Canada un rapport quotidien concernant la GIES par IP cible; ce rapport est présenté sous forme de tableau ou de graphique, est ventilé par organisation cliente et indique ce qui suit :

a) Un résumé, sous forme de graphique à bandes, des événements pour les cinq principales IP cible, où :

i) Le nombre total d'événements concernant l'IP cible figure sur l'axe x;

ii) L'IP cible figure sur l'axe y;

b) Un résumé des 50 principaux événements, présentés sous forme de tableau, indiquant :

i) L'IP cible;

ii) Les détails de l'événement;

iii) La gravité de l'événement;

iv) Le nombre d'événements.

1.8 Services de gestion

1.8.1 Gestion des changements

(29) L'entrepreneur doit configurer les périodes relatives à la conservation et à l'archivage des données, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(30) L'entrepreneur doit activer et désactiver les règles ou politiques, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

1.8.2 Gestion des incidents

(31) L'entrepreneur doit consigner comme incidents de sécurité les alertes provenant du GIES.