SPC – Exigences relatives au SGV d'entreprise

	OBLIGATOIRE	Fonction principale	Fonction secondaire	Réponse moyenne pondérée maximale de l'équipe de projet	Fournisseur n° 1		Fournisseur n° 2		Fournisseur n° 3	
					Satisfaite	Commentaire	Satisfaite	Commentaire	Satisfaite	Commentaire
O1	La solution doit soutenir pleinement la mise en œuvre, l'administration, la configuration et le balayage dans les réseaux IPv4 et IPv6.									
O2	La solution doit être capable d'effectuer des balayages de découverte des biens et des balayages des vulnérabilités pour 2 000 000 de dispositifs au minimum. Un balayage de découverte doit enregistrer 10 000 adresses IP en une seule journée. Un balayage complet de 10 000 adresses IP sans authentifiant doit être effectué sur une période de 2 jours, en l'étalant en dehors des heures de production de manière à réduire l'incidence sur les opérations quotidiennes. Un balayage complet de 10 000 adresses IP avec authentifiant doit être effectué sur une période de 3 jours, en l'étalant en dehors des heures de production de manière à réduire l'incidence sur les opérations quotidiennes.									
O3	Les communications entre le gestionnaire, les dispositifs de balayage, les agents, et les outils de rapports doivent avoir des intervalles de temps configurables avec l'horodatage des communications.									
O4	La solution doit être capable de personnaliser le classement des risques par ordre de priorité en fonction du contexte opérationnel.									
O5	La solution doit être capable de personnaliser le classement des risques par ordre de priorité en fonction du CVSS.									
O6	La solution doit avoir la capacité d'intégrer les résultats des balayages des vulnérabilités d'autres fournisseurs dans divers formats.									
O7	La solution doit avoir la capacité de consommer et d'exécuter le contenu personnalisé ou du secteur conforme à SCAP 1.2 ou version ultérieure.									
O8	Les composantes de la solution doivent être disponibles sous forme de dispositifs logiciels et matériels.									
O9	La solution doit tenir à jour et stocker les journaux de vérification sécurisés conformément aux politiques du GC. (Voir http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742)									
O10	La solution doit identifier de manière unique tous les biens découverts, y compris les logiciels et micrologiciels, hébergés dans l'infrastructure du GC, et en faire le suivi.									
O11	La solution doit être capable de traiter, de communiquer et de stocker les données en utilisant une méthode de chiffrement approuvée par le GC lorsque cela est jugé nécessaire (c.-à-d. sensibilité des données), utiliser des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques qui ont été approuvés par le CST, validés par le Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), et sont spécifiés dans la norme ITSB-111 (https://www.cse-cst.gc.ca/fr/node/1428/html/25015) ou une version ultérieure.									
O12	La solution doit fournir en détail l'ordre de priorité en matière de correction. Fournir des analyses et des recommandations sur les vulnérabilités à traiter en premier.									
O13	La solution doit identifier et authentifier les utilisateurs de l'organisation de manière unique par l'utilisation des services Active Directory de Microsoft.									
O14	La solution doit fournir une composante de balayage d'évaluation des vulnérabilités capable de balayer les environnements de machine virtuelle, de machine non virtuelle et infonuagiques.				.					
O15	La solution doit fournir des dispositifs de balayage logiciels dotés de consoles de gestion intégrées, qui peuvent fonctionner de manière autonome lorsqu'ils sont déconnectés d'un serveur de gestion.									
O16	La solution doit appliquer une relation fiable/authentifiée avec la source d'information sur les vulnérabilités.									
O17	La solution doit avoir la capacité de faire interface avec l'information sur les vulnérabilités de la base de données nationale sur les vulnérabilités au sujet des sources de flux de données.									
O18	La solution doit avoir la capacité de sauvegarder tous ses éléments, ce qui inclut, mais ne s'y limite pas, la configuration des données de balayage.									
O19	La solution doit permettre de déployer les correctifs et les mises à jour de ses outils de diverses manières approuvées, y compris, mais sans s'y limiter, par le réseau, une clé USB, et le téléchargement.									
O20	La solution doit fournir la capacité d'assurer que tous les journaux/informations de débogage/vidages de mémoire peuvent être purgés de l'information à caractère sensible pour les transmettre aux fournisseurs aux fins de soutien.									
O21	Exigence transférée à Rated - R23									

	OBLIGATOIRE	Fonction principale	Fonction secondaire	Réponse moyenne pondérée maximale de l'équipe de projet	Fournisseur n° 1		Fournisseur n° 2		Fournisseur n° 3	
					Satisfaite	Commentaire	Satisfaite	Commentaire	Satisfaite	Commentaire
O22	La solution doit être capable d'effectuer un balayage avec ou sans agent de la conformité de la configuration.									
O23	La solution doit prendre en charge un balayage configurable, planifié et ponctuel.									
O24	La solution doit être capable d'effectuer un balayage avec ou sans agent des vulnérabilités.									
O25	La solution doit être capable d'effectuer des balayages d'évaluation des vulnérabilités authentifiés ou non.									
O26	La solution doit fournir une méthode d'exclusion d'hôtes ou de groupes d'hôtes des balayages (plage IP, groupes de biens dynamiques, etc.).									
O27	La solution doit fournir des capacités de découverte, regroupement, classification, et gestion des biens.									
O28	La solution doit être capable de fournir des balayages de la conformité de la configuration.									
O29	La solution doit fournir un référentiel central des rapports avec de nombreux formats de sortie de rapport, y compris, mais sans s'y limiter, PDF, HTML, XML et CSV.									
O30	La solution doit fournir un modèle standard de sécurité conforme aux normes PCI.									
O31	La solution doit fournir des mises à jour des modèles de balayage normalisés et recommandés au sein du secteur.									
O32	La solution doit également donner la possibilité de créer, modifier et personnaliser les options de modèle de balayage, comme les ports, les protocoles et les caractéristiques comportementales des paquets réseau utilisés pour le balayage.									
O33	La solution doit avoir un accès configurable basé sur les rôles.									
O34	La solution doit avoir la capacité d'effectuer des balayages authentifiés ou non en utilisant les privilèges d'accès les moins privilégiés pour les balayages authentifiés.									
O35	La solution doit être en mesure de contrôler un balayage à un emplacement distant au moyen d'une liaison réseau lente de 512 K. La solution doit également être en mesure de communiquer les résultats de balayage et d'enregistrer l'information à partir de cet emplacement distant dans la base de données à l'emplacement central.									
	EXIGENCES COTÉES									
C1	La solution devrait prendre en charge des serveurs de gestion et rapports centralisés qui peuvent fonctionner de façon indépendante (y compris leurs dispositifs de balayage et agents dépendants respectifs), ainsi qu'être subordonnés à un échelon supérieur de serveurs de gestion et rapports. Les serveurs de gestion et rapports devraient prendre en charge plusieurs niveaux hiérarchiques de serveurs de gestion et rapports subalternes (y compris leurs dispositifs de balayage et agents dépendants respectifs).			10						
C2	La solution devrait prendre en charge le stockage des authentifiants dans un module de sécurité matériel validé par la norme FIPS140.			5						
C3	La capacité à fournir des capacités de regroupement, de gestion et de classification personnalisables des biens.			5						
C4	La capacité à regrouper plusieurs adresses IP en un seul bien.			5						
C5	Le système devrait pouvoir utiliser les mises à jour des signatures de la base de données des vulnérabilités dans les 6 heures suivant leur publication.			5						
C6	La capacité à s'intégrer avec les technologies SIEM en utilisant les formats de sortie et les protocoles de vérification suivants. Format de sortie de vérification : fichier texte, fichier texte continu et Comment Event Format (CEF). Protocoles d'authentification pour recueillir le fichier : SAMBA, FTP (SFTP), base de données utilisant un pilote JDBC, syslog, événements compatibles HP SmartConnector, événements compatibles CEF et Log Event Extended Format (LEEF).			10						
C7	La capacité d'envoyer une notification automatique par courriel à des destinataires configurables.			5						
C8	La capacité de balayer des plateformes cibles – Les normes existantes de SPC sont les suivantes (liste non exhaustive) : Windows, Redhat, CentOS, Debian, Ubuntu, Fedora, FreeBSD, SUSE, Mac OSX, AIX, Solaris, HP/UX, Cisco IOS, F5, SCADA. 1 point chacune, max 10 points			10						

OBLIGATOIRE		Fonction principale	Fonction secondaire	Réponse moyenne pondérée maximale de l'équipe de projet	Fournisseur n° 1		Fournisseur n° 2		Fournisseur n° 3	
					Satisfaite	Commentaire	Satisfaite	Commentaire	Satisfaite	Commentaire
C9	La capacité à s'intégrer avec les plateformes courantes de gestion des changements/flux de travail pour automatiser la génération de flux de travail et de billets externes. Fournir les listes des systèmes pris en charge. 1 point chacune, max 5 points				5					