Annexe D

Plan d’essai et résultats :

DP portant sur le service de gestion des vulnérabilités et de la conformité

Table des matières

1. Renseignements généraux

Le service de gestion des vulnérabilités et de la conformité (SGVC) est un ensemble de processus, de procédures et d'outils qui sont utilisés collectivement pour gérer de manière rentable les expositions aux menaces liées à la sécurité des TI des systèmes d'information, et réduire la surface attaquable accessible par un auteur de menaces délibérées ou non au sein des réseaux informatiques, des systèmes, et des applications d'entreprise et l'information importante qu'ils contiennent.

Le SGVC améliore la capacité du GC à :

- déterminer les propriétaires, et la criticité des biens de TI connectés au réseau;
- découvrir, inventorier ces biens, et en faire le suivi;
- gérer une base de données à jour et efficace, et détecter et identifier les vulnérabilités en matière de sécurité des TI en fonction du code et de la configuration (c.-à-d., la conception et la spécification, la mise en œuvre, et le fonctionnement et la configuration) au sein de ces biens;
- attribuer des cotes de gravité à ces constatations qui, en conjonction avec la criticité des biens concernés, permettent le classement des risques par ordre de priorité en fonction du contexte opérationnel, et déterminent les échéances et les seuils des activités de correction;
- regrouper ces constatations;
- proposer des conseils et des options en matière d'activités de correction et leur séquence pour atténuer les risques liés à la sécurité des TI associés à ces constatations.

Le SGVC ouvre également la voie à un système intégré et automatisé de détection et correction des vulnérabilités au sein des environnements de SPC et des partenaires.

L'ensemble de la solution repose sur les principes de conception suivants : privilège minimum, séparation des fonctions, mécanisme le moins commun, regroupement, interopérabilité, évolutivité, précision, couverture et échéances.

2. Introduction

Le but principal de la demande de propositions (DP) portant sur le SGVC est d'établir un mécanisme pour remplacer les solutions de SGVC en fin de vie et en fin de soutien actuellement déployées au sein des partenaires de Services partagés Canada (SPC), ainsi que satisfaire aux exigences futures en matière d'approvisionnement de SPC et des partenaires portant sur les équipements, les logiciels et les services professionnels nécessaires pour acquérir, développer, mettre en œuvre et maintenir un SGVC à l'échelle du GC pour les centres de données, les centres de données existants, l'infrastructure liée à Internet et un maximum de 2 000 000 de biens de TI connectés au réseau.

2.1. Plan d'essai relatif à la DP portant sur le SGVC

Le but principal du plan d'essai relatif au SGVC est de vérifier les exigences fonctionnelles et d'assurance de la sécurité, de valider la conception de la solution de SGVC, et d'évaluer le risque et les capacités du produit et des processus. En réalité, ce plan d'essai sera utilisé pour vérifier un sous-ensemble des exigences obligatoires de la solution de SGVC. Seule la proposition retenue sera soumise à ce plan d'essai; si le soumissionnaire échoue à démontrer les exigences à la satisfaction de SPC, le soumissionnaire sera automatiquement disqualifié et la soumission admissible suivante sera évaluée.

2.2. Portée du document

Ce document d'essai vise à détailler les exigences obligatoires de la DP qui seront mises à l'essai, et la façon de les mettre à l'essai.

Les exigences obligatoires suivantes seront mises à l'essai :

- 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 la découverte, l'inventaire et le suivi des biens, et les balayages des vulnérabilités pour 2 000 000 de biens de TI en réseau. 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.
- O4 – La solution doit être capable de personnaliser le classement des risques par ordre de priorité en fonction du contexte opérationnel.
- 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.
- 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)
- 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 précisés dans la norme ITSB-111 (https://www.cse-cst.gc.ca/fr/node/1428/html/25015) ou une version ultérieure.

- O13 – La solution doit identifier et authentifier les utilisateurs de l'organisation de manière unique par l'utilisation des services Active Directory de Microsoft.
- 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.
- O27 – La solution doit fournir des capacités de découverte, regroupement, classification, et gestion des biens.

2.3. Hypothèses

Le présent document part des hypothèses suivantes :

- Un représentant du FEO exécutera le plan d'essai, en présence des ressources en matière d'essai de l'État qui le noteront.
- Les vérificateurs représentant le FEO ont des connaissances approfondies sur tous les composants matériels et logiciels de la solution.
- Le représentant du FEO fournira l'équipement d'essai de la solution. L'équipement doit correspondre à ce qui est proposé.
- Toutes les données utilisées pour l'essai seront fournies par l'environnement de laboratoire du soumissionnaire et recueillies à partir de celui-ci.

2.4. Environnement d'essai

Le soumissionnaire fournira l'environnement d'essai, y compris tout le matériel et les logiciels nécessaires pour l'essai.

2.5. Terminologie et abréviations

Voir l'énoncé des travaux de la demande de propositions.

3. Plan d'essai

3.1. Description

La section suivante vise à vérifier un sous-ensemble des exigences obligatoires de la DP et à documenter les résultats de l'essai. Les cas d'essai qui ont été créés ne sont pas propres à la solution. L'environnement peut être réglé de façon dynamique selon les besoins d'exécution de chaque cas d'essai. En outre, l'État est libre d'adapter l'exécution de l'essai en fonction de la configuration de l'architecture par défaut du FEO.

3.2. Cas d'essai

N^{o} de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
O1	La solution doit soutenir pleinement la mise en œuvre, l'administration, la configuration et le balayage dans les réseaux IPv4 et IPv6.	Le soumissionnaire démontrera que la solution prend en charge entièrement la coexistence d'IPv4 et d'IPv6 (double pile), et qu'elle ne nécessite pas IPv4 pour assurer un bon fonctionnement complet. Le soumissionnaire démontrera que la prise en charge d'IPv6 est équivalente ou meilleure en termes de qualité et de fonctionnalité par rapport à la prise en charge d'IPv4. Ces essais démontreront que tous les sous-systèmes de la solution fonctionnent de manière adéquate et complète dans le cadre d'une mise en œuvre à double pile, et sans IPv4, notamment : • accès réseau du client à la gestion, moteur de balayage, référentiel/base de données, rapports, interface de ligne de commande (CLI) et interface utilisateur graphique (GUI); • accès réseau entre le moteur de balayage et les biens de TI connectés au réseau (p. ex., découverte des biens orientée réseau, balayage de réseau et de ports, balayage de ports, énumération des ressources et partages réseau, et contrôles de vulnérabilité et de conformité);	

N° de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
		• accès réseau entre le référentiel ou la base de données et les sites de mise à jour du fournisseur; • intercommunication entre les composants du moteur de balayage, du référentiel ou de la base de données, de la gestion et des rapports.	
O2	La solution doit être capable d'effectuer la découverte, l'inventaire et le suivi des biens, et les balayages des vulnérabilités pour 2 000 000 de biens de TI en réseau. 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.	Le soumissionnaire démontrera l'évolutivité de la solution en matière de découverte, d'identification, d'inventaire, de suivi, de balayage et de rapports portant sur 2 000 000 de biens de TI connectés au réseau. Le soumissionnaire démontrera cette exigence en utilisant 3 réseaux multizones distincts composés de plusieurs zones de TI par réseau multizone. Ces essais démontreront : • l'évolutivité au moyen d'une architecture comportant plusieurs hiérarchies de sous-systèmes et composants de SGVC de gestion et rapports distribués, coordonnés centralement; • la capacité à exécuter simultanément plusieurs balayages planifiés et sur demande à partir de plusieurs classes d'utilisateurs, à partir de plusieurs organisations clientes, et à travers plusieurs échelons hiérarchiques; • une méthode d'exclusion d'hôtes ou de groupes d'hôtes des balayages (plage IP, groupes de biens dynamiques, etc.); • la capacité de déterminer et de suivre les changements dans les états de vulnérabilité; • la capacité de visualiser l'état en temps réel de tous les balayages en cours d'exécution. Ce qui précède doit s'appliquer à une fréquence de balayage d'une semaine ou moins, sans perte de détection ou de précision.	

N° de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
O4	La solution doit être capable de personnaliser le classement des risques par ordre de priorité en fonction du contexte opérationnel.	Le soumissionnaire démontrera que le classement des risques par ordre de priorité peut être personnalisé et configuré à l'aide d'une démonstration à partir de la console. Les essais démontreront que les biens de TI connectés au réseau peuvent être classés en groupes d'après l'affectation de la valeur opérationnelle basée sur la criticité des processus opérationnels qu'ils soutiennent.	
O6	La solution doit avoir la capacité d'intégrer les résultats des balayages des vulnérabilités d'autres fournisseurs dans divers formats.	Le soumissionnaire démontrera que la solution prend en charge la capacité de consommer des rapports de balayage des vulnérabilités d'autres fournisseurs. Ces essais démontreront que la solution importe les rapports de découverte des biens et de balayage des vulnérabilités d'autres fournisseurs du marché d'évaluation des vulnérabilités sans perte de qualité de l'information importée.	
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.	Le soumissionnaire démontrera que la solution prend en charge une méthode pour utiliser une approche basée sur des normes pour automatiser la gestion des vulnérabilités. Y compris décrire les vulnérabilités et les expositions en matière de sécurité concernant des renseignements connus du public, déterminer la gravité relative des vulnérabilités liées aux défauts de logiciels et fournir un format normalisé pour communiquer les caractéristiques des vulnérabilités, et présenter les listes de contrôle de sécurité, les points de référence et les documents connexes sous une forme lisible par machine. Ces essais démontreront les éléments suivants : • la solution prend en charge une approche basée sur les normes pour décrire, communiquer et consommer les vulnérabilités et les expositions en matière de sécurité concernant des renseignements connus du public;	

N° de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
		• déterminer la gravité relative des vulnérabilités liées aux défauts de logiciels et fournir un format normalisé pour communiquer ou consommer les caractéristiques des vulnérabilités; • présenter, communiquer et consommer les listes de contrôle de sécurité, les points de référence et les documents connexes sous une forme lisible par machine.	
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)	Le soumissionnaire démontrera que la solution tient à jour et stocke les journaux de vérification sécurisés conformément aux politiques du GC. Les essais démontreront que la solution : • est synchronisée par le protocole de synchronisation réseau (NTP); • produit des journaux de vérification, y compris les traces réseau relatives à toute activité de balayage et les comptes d'administrateur associés pour assurer que cette activité se limite aux périodes de balayage légitime.	
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	Le soumissionnaire démontrera que la solution prend en charge les algorithmes de chiffrement approuvés par le GC pour sécuriser les canaux de communication entre tous les sous-systèmes de la solution. Ces essais démontreront que la solution utilise les algorithmes de chiffrement approuvés par le GC pour sécuriser les canaux de communication, y compris : • accès réseau du client à la gestion, moteur de balayage, référentiel/base de données, rapports, interface de ligne de commande (CLI) et interface utilisateur graphique (GUI);	

N° de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
	(https://www.cse-cst.gc.ca/fr/node/1428/html/25015) ou une version ultérieure.	• accès réseau entre le référentiel ou la base de données et les sites de mise à jour du fournisseur; • intercommunication entre les composants du moteur de balayage, du référentiel ou de la base de données, de la gestion et des rapports.	
O13	La solution doit identifier et authentifier les utilisateurs de l'organisation de manière unique par l'utilisation des services Active Directory de Microsoft.	Le soumissionnaire sera tenu de fournir un serveur AD, et de démontrer qu'AD peut être utilisé pour l'authentification auprès de la solution. Les essais démontreront que le contrôle d'accès basé sur les rôles (RBAC) peut être utilisé pour fournir différents droits et fonctionnalités, de manière à appliquer la séparation des fonctions à partir de plusieurs classes d'utilisateurs, à partir de plusieurs organisations clientes, et à travers plusieurs échelons hiérarchiques.	
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.	Le soumissionnaire démontrera que la solution peut être sauvegardée dans son intégralité. Les essais démontreront que : • le sous-système et les composants de la base de données sont sauvegardés, y compris la configuration, les authentifiants, les modèles et les données; • les configurations peuvent être réutilisées comme modèles de configuration. Un gestionnaire de rechange identique à l'original (appareil, serveur ou machine virtuelle) sera alors configuré par le soumissionnaire à l'état nécessaire pour permettre la restauration.	
O27	La solution doit fournir des capacités de découverte, regroupement, classification, et gestion des biens.	Le soumissionnaire démontrera la capacité à identifier de manière unique, regrouper, classer et gérer les biens de TI connectés au réseau à partir de ces identifiants ou d'autres identifiants connus ou de renseignements connus.	

N° de cas	Description	Exécution de l'essai	RÉUSSITE/ ÉCHEC
		Ces essais démontreront : • la capacité de découvrir et d'identifier les classes d'applications, systèmes d'exploitation et périphériques matériels présents parmi les biens de TI connectés au réseau découverts; • que ces biens de TI peuvent être : – regroupés par organisation cliente, et par chronologie; – classés en fonction de la criticité des biens de TI; – classés en fonction de la gravité des constatations; • que la découverte des biens ne pollue ni ne contamine les inventaires des biens de TI connectés au réseau découverts au sein d'autres environnements de clients, de SPC ou de partenaires. • que le sous-système de rapports peut faire l'objet de rapports en regroupant les données à partir de plusieurs classes d'utilisateurs, à partir de plusieurs organisations clientes, et à travers plusieurs échelons hiérarchiques, y compris : – organisations clientes – nœud du système de gestion – l'ensemble des organisations ou partenaires – plusieurs nœuds du sous-système de gestion • que les références aux mêmes biens peuvent être détectées et supprimées.	