Bureau du surintendant des institutions financières
Service de suivi du risque numérique (SSRN)

Annexe A – Énoncé des capacités à l’égard du SSRN
Exigences obligatoires minimales

TABLE DES MATIÈRES

1 INTRODUCTION

La présente annexe décrit les exigences obligatoires minimales du BSIF en matière de service de suivi du risque numérique (SSRN).

2 EXIGENCES OBLIGATOIRES MINIMALES

2.1 Renseignements sur les menaces

2.1.1 Vulnérabilités et expositions

a. Le SSRN doit couvrir l'ensemble des CVE (expositions et vulnérabilités courantes) se trouvant dans la National Vulnerability Database (NDV) du National Institute of Standards and Technology (NIST), y compris leur notation selon le système de notation des vulnérabilités courantes (CVSS pour Common Vulnerability Scoring System).

2.1.2 Renseignements sur les menaces

a. Le SSRN doit pouvoir fournir des renseignements au sujet des auteurs de menaces (le cas échéant), y compris :
   i. leurs noms courants;
   ii. s'ils représentent une menace persistante avancée (MPA), leur numéro de MPA;
   iii. les activités connues;
   iv. les capacités connues;
   v. les tactiques, techniques et procédures (TTP) connues;
   vi. leurs origines soupçonnées;
   vii. les motivations soupçonnées; et
   viii. les cibles.

b. Le SSRN doit fournir le fil des événements et des détails au sujet des TTP utilisées, mais aussi les répercussions des événements liés aux menaces pour chaque scénario de menace envisagé.

2.1.3 Collecte de renseignements sur les menaces

a. Pour soutenir la collecte massive de renseignements, le SSRN doit utiliser l'apprentissage automatique et le traitement du langage naturel pour recueillir et structurer le contenu textuel des sources provenant de tous les langages de programmation et le classer à l'aide d'ontologies et d'événements qui ne dépendent pas du langage.

b. Le SSRN doit être doté d'une importante capacité opérationnelle[1].

c. Le SSRN doit recueillir des renseignements et établir des rapports sur les menaces à l'échelle mondiale[2].

---

[1] Une importante capacité opérationnelle est définie comme une capacité minimale d'observation de 10 000 capteurs de réseau et de 15 000 000 terminaux dans au moins 50 pays.

[2] L'entrepreneur doit démontrer qu'il emploie au moins 700 analystes du renseignement cybernétique répartis dans au moins 50 pays pour satisfaire à cette exigence. Les analystes doivent également travailler dans au moins 25 langues, dont :

a. l'anglais;
b. le français;
c. le russe;
d. le chinois;

2.1.4 Expérience auprès des organismes de renseignement canadiens

a. L'entrepreneur responsable du SSRN doit avoir une expérience récente de travail dans le domaine du renseignement auprès d'au moins un des organismes du gouvernement du Canada suivant :
   i. Service canadien du renseignement de sécurité;
   ii. Centre de sécurité des télécommunications;
   iii. CANAFE;
   iv. Ministère de la Défense nationale;
   v. Sécurité publique; ou
   vi. Gendarmerie royale du Canada.

2.1.5 Expertise du secteur financier et orientation sectorielle

a. L'entrepreneur responsable du SSRN doit concentrer ses activités dans le secteur financier et compter plus de 250 clients à l'échelle mondiale issus du secteur financier.

b. L'entrepreneur doit avoir de l'expérience dans la prestation de services d'intervention en cas de cyberincidents visant les systèmes financiers mondiaux, y compris le système bancaire SWIFT.

c. L'entrepreneur doit démontrer qu'il est en mesure de repérer et de diffuser le nom de nouveaux groupes d'auteurs de menace dans le secteur financier, y compris des preuves suffisantes que le groupe est reconnu et accepté par la collectivité du renseignement sur le cyberrisque.

d. Le SSRN doit regrouper les rapports sur les renseignements sur les menaces par secteur, notamment :
   i. finances;
   ii. assurances;
   iii. États.

2.1.6 Indicateurs de compromission (IC)

a. Le SSRN doit fournir des IC à la solution de gestion des informations et des événements de sécurité du BSIF (Sentinel de Microsoft).

b. Les renseignements fournis en lien avec les IC doivent contenir le contexte détaillé des entités concernées, y compris les condensés numériques (valeurs de hachage), les adresses IP, les CVE et tout autre renseignement pertinent.

c. Le SSRN doit fournir le score de réputation, la qualité de la détection ou le score de risque des IC. Les scores doivent être justifiés et comporter les caractéristiques dynamiques des entités pour représenter le risque en temps réel des IC.

2.1.7 Sources techniques

a. Le SSRN doit puiser ses informations au sujet des menaces à même des sources techniques telles que le WHOIS et le système de noms de domaine (DNS).

---

   e. l'arabe;
   f. le persan;
   g. le coréen;
   h. le portugais.

2.1.8 Techniques, tactiques et procédures (TTP) relatives à la menace

a. Le SSRN doit fournir des TTP détaillées relatives aux menaces, y compris les procédures, mesures d'atténuation et méthodologies de détection précises selon le cadre MITRE ATT&CK3.

2.1.9 Maliciels

a. Le SSRN doit fournir des détails sur le nom, la fonction, les caractéristiques et l'origine des logiciels malveillants connus.

2.1.10 Analyse des maliciels

a. Le SSRN doit permettre l'analyse des maliciels téléchargés par les clients et l'extraction d'indicateurs tels que l'adresse IP, le nom de domaine, le Mutex, les modifications du registre Windows et les détails de l'exécution du processus. Il doit également fournir les familles de maliciels et les auteurs de menaces associés.

b. La fonction d'analyse des maliciels doit prendre en charge les fichiers de logiciels malveillants pour les systèmes d'exploitation courants, au minimum Windows, MacOS et Linux.

2.1.11 Extension du navigateur

a. Le SSRN doit fournir une extension de navigateur pour Google Chrome ou Microsoft Edge qui permet de parcourir les pages Web et d'analyser les détails concernant les indicateurs, les vulnérabilités et les auteurs de menaces présents sur ces pages. Les données et l'analyse qui en découle doivent pouvoir être exportées vers d'autres outils à l'aide de fichiers JSON.

2.1.12 Filtres

a. Le SSRN doit permettre aux utilisateurs de sélectionner les technologies, les systèmes d'exploitation, les auteurs de menace et les secteurs d'intérêt désirés pour réduire la quantité de renseignements reçus au sujet de menaces inappropriées.

2.2 Surveillance du Web caché

2.2.1 Surveillance du Web caché

a. Le SSRN doit assurer une surveillance du Web visible, invisible et caché.

2.2.2 Recherche de renseignements propres au BSIF

a. Le SSRN doit permettre au BSIF de définir certains renseignements précis (texte, noms et domaines) qui pourraient indiquer une fuite de ses données.

2.2.3 Détection de fuite de données

a. Le SSRN doit envoyer des alertes en cas de détection d'une fuite présumée des données du BSIF, y compris le type de données, la date/heure et la source de la fuite présumée.

2.3 Surveillance de la fraude

2.3.1 Surveillance de l'usurpation de l'identité de membres de la direction

a. Le SSRN doit intégrer à son système les personnes[4] et les rôles clés définis par le BSIF en fonction desquels les médias sociaux seront analysés afin de repérer d'éventuels comptes frauduleux usurpant l'identité de ces personnes et/ou de ces rôles.

[3] MITRE ATT&CK®

[4] Exemple : Fiches biographiques de la haute direction (osfi-bsif.gc.ca)

2.3.2 Surveillance des justificatifs d'identité

a. Le SSRN doit rechercher les domaines définis par le BSIF (@OSFI-BSIF.gc.ca) afin de relever et de signaler la compromission potentielle des justificatifs d'identité d'un utilisateur défini par le BSIF et lui envoyer une alerte par courrier électronique chaque fois que des fuites de justificatifs d'identité sont détectées.

2.4 Exigences en matière de services communs

2.4.1 Langue

a. Le SSRN doit être fourni en anglais.

b. Le SSRN doit recueillir des données dans plusieurs langues et les traduire automatiquement en anglais.

2.4.2 Accès au portail

a. Le SSRN doit être accessible par des liens sécurisés, conformément aux recommandations suivantes :

i. https://www.cyber.gc.ca/sites/default/files/itsp40111-cryptographic-algorithms-unclassified-protecteda-protectedb-information.pdf; et

ii. https://www.cyber.gc.ca/sites/default/files/itsp40111-algorithmes-cryptographiques-pour-information-nonclassifie-protegea-protegeb.pdf.

b. Le portail Web du SSRN ne doit pas avoir besoin d'infrastructure supplémentaire du côté du client (BSIF).

c. Le SSRN doit être compatible avec les navigateurs Web Microsoft Edge et Google Chrome.

2.4.3 Ressources d'apprentissage

a. Une documentation adéquate à l'intention de l'utilisateur doit accompagner le SSRN, notamment un manuel de l'utilisateur, un guide d'interrogation et une aide intégrée afin de faciliter l'utilisation du service sans que de la formation ciblée soit nécessaire.

2.4.4 Gestion des utilisateurs

a. Le SSRN doit accorder un rôle d'administrateur au BSIF pour que ce dernier puisse créer, modifier et supprimer des comptes d'utilisateurs du BSIF à même l'outil.

b. Le rôle d'utilisateur du BSIF ne doit cependant pas disposer de ces mêmes privilèges.

2.4.5 Recherche

a. Le SSRN doit fournir un portail de recherche permettant aux utilisateurs du BSIF de rechercher des éléments d'intérêt à partir des données collectées sur le Web (section2.2.1).

b. Les résultats de recherches doivent contenir une référence à la source de l'information (par exemple, Pastebin, Web caché, forum, etc.).

c. Le SSRN doit permettre la modification et la personnalisation de la logique d'interrogation.

2.4.6 Nettoyage du contenu

a. Le contenu recueilli à même Internet doit être nettoyé (mis en cache avec des liens inactifs).

2.4.7 Tableaux de bord

a. Le SSRN doit permettre aux utilisateurs de compiler des données pour créer et sauvegarder des tableaux de bord individuels.

b. Le SSRN doit fournir des tableaux de bord distincts pour les incidents et pour les renseignements sur les menaces.

2.4.8 Rapports

a. Le SSRN doit permettre l'exportation de rapports dans un format communément utilisable (Microsoft Word ou PDF)[5].

2.4.9 Exportation de données

a. Le SSRN doit permettre l'exportation des résultats des requêtes en format JSON (notation des objets du langage Java) et en format CSV (valeurs séparées par des virgules).

b. Le SSRN doit permettre l'exportation des indicateurs et des données associées sous forme de règles YARA.

c. Le SSRN doit permettre d'interroger et d'exporter des données au moyen d'une interface de programmation d'applications (API).

2.4.10 Alertes

a. Le SSRN doit permettre la configuration d'alertes électroniques en cas de nouvelles informations liées à des requêtes prédéfinies.

b. Le SSRN doit permettre au BSIF de créer, de surveiller et d'automatiser des alertes et des rapports sur les vulnérabilités et les menaces, y compris, mais sans s'y limiter, dans le secteur financier.

2.4.11 Accessibilité

a. Le SSRN doit demeurer accessible en tout temps (24 heures par jour et 7 jours par semaine) avec des interruptions de service ne dépassant pas un jour par mois.

b. Le SSRN doit offrir des services de renseignement sur les menaces (Centre des opérations de sécurité [COS]) géographiquement dispersés, en tout temps (24 heures par jour et 7 jours par semaine).

2.4.12 Expérience

a. L'entrepreneur responsable du SSRN doit avoir au moins 10 ans d'expérience dans la fourniture de services de collecte et d'analyse de renseignements sur les menaces, y compris le suivi des vulnérabilités et des IC.

2.4.13 Collecte des données

a. Le SSRN doit pouvoir contenir les données sur les menaces collectées au cours des 20 dernières années.

2.4.14 Protection des données personnelles

a. Si des données à caractère personnel sont fournies par le Canada, l'entrepreneur responsable du SSRN doit les sauvegarder et les chiffrer conformément aux recommandations suivantes :

[5] Les saisies d'écran ne sont pas acceptées.

i. https://www.cyber.gc.ca/sites/default/files/itsp40111-cryptographic-algorithms-unclassified-protecteda-protectedb-information.pdf; et
ii. https://www.cyber.gc.ca/sites/default/files/itsp40111-algorithmes-cryptographiques-pour-information-nonclassifie-protegea-protegeb.pdf.

2.4.15 Destruction des données

a. Le SSRN doit permettre à un utilisateur du BSIF de détruire les données qu'il fournit au système.

2.4.16 Caractère opportun

a. Le SSRN doit mettre à jour les nouvelles données de renseignement sur les menaces dans le portail, le jour même où elles sont recensées.

b. Lorsque des alertes sont déclenchées, le SSRN doit les transmettre par courriel le jour même de leur déclenchement.

c. Lorsque des IC sont détectés, le SSRN doit le signaler au BSIF le jour même de leur détection.

2.4.17 Soutien

a. L'entrepreneur responsable du SSRN doit offrir une assistance technique par téléphone et par courrier électronique pendant les heures de travail des jours ouvrables.

b. L'entrepreneur responsable du SSRN doit offrir ce soutien en anglais.

3 GLOSSAIRE

Cette section définit les termes inhabituels et les acronymes utilisés dans le présent document :

Terme	Définition
API	interface de programmation d'applications
BSIF	Bureau du surintendant des institutions financières
CEC	Centre d'excellence en cybersécurité
COS	Centre des opérations de sécurité
CSV	De l'anglais Comma Separated Value, signifie valeurs séparées par des virgules
CVSS	De l'anglais Common Vulnerability Scoring System, signifie système commun de notation des vulnérabilités.
DC	Division de la cybersécurité
DNS	De l'anglais Domain Name System, signifie système de nom de domaine.
entrepreneur responsable du SSRN	Il s'agit de l'entrepreneur qui a obtenu le contrat de SSRN ou son éditeur de logiciels, si l'entrepreneur n'est pas l'éditeur de logiciel.
exigence non fonctionnelle	Exigence qui précise des critères pouvant être utilisés pour juger du fonctionnement d'un système, plutôt que des comportements spécifiques[6].
exigence fonctionnelle	Fonction d'un système ou d'un de ses composants; une fonction étant décrite comme une spécification du comportement entre les entrées et les sorties[7].
forum	Un site de discussion en ligne où les gens peuvent tenir des conversations sous forme de messages affichés[8].
GFCI	De l'anglais Global Financial Centres Index, signifie indice des centres financiers mondiaux.
heures de travail	Heures de travail normales du BSIF : de 8 h à 17 h (HE), les jours ouvrables.
image de marque	Symbole d'un produit, d'une firme, d'une personne; représentation qu'on en a; réputation[9].
indicateur	Artéfact technique ou observable qui suggère qu'une attaque est imminente ou en cours, ou qu'une compromission a déjà eu lieu[10].
IC	Indicateur de compromission
IRC	De l'anglais Internet Relay Chat, signifie système de conversation par relais Internet ou service de clavardage.
jour ouvrable	Jour de travail établi par le gouvernement fédéral du Canada
JSON	De l'anglais Java Script Object Notation, signifie notation des objets du langage Java.
justificatifs d'identité	Un objet ou une structure de données qui lie officiellement une identité - grâce à un ou plusieurs identifiants - et (éventuellement) des attributs supplémentaires, à au moins un authentifiant possédé et contrôlé par un utilisateur[11]. Exemple : mot de passe.
MPA	Menace persistante avancée – Un adversaire qui possède une forte expertise et des ressources importantes qui lui permettent de créer des occasions pour atteindre ses objectifs au moyen de multiples vecteurs d'attaque (par exemple, cybernétique, physique et déception). Ces objectifs comprennent généralement

[6] Non-functional requirement - Wikipedia
[7] Functional requirement - Wikipedia
[8] Forum - Wikipédia
[9] Définition de la locution *Image de marque* - Le Robert
[10] indicator - Glossary | CSRC (nist.gov)
[11] Digital Identity Guidelines (nist.gov)

	l'établissement et l'extension de points d'appui dans l'infrastructure des technologies de l'information des organisations ciblées dans le but d'exfiltrer des informations, de saper ou d'entraver des aspects essentiels d'une mission, d'un programme ou d'une organisation, ou de se positionner pour atteindre ces objectifs à l'avenir. La menace persistante avancée : (i) poursuit ses objectifs de manière répétée sur une longue période; (ii) s'adapte aux efforts des défenseurs pour lui résister; et (iii) est déterminée à maintenir le niveau d'interaction nécessaire à la réalisation de ses objectifs[12].
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
P2P	De l'anglais Peer-to-peer, signifie pair-à-pair
Pastebin	Un type de service d'hébergement de contenu en ligne où les utilisateurs peuvent sauvegarder du texte brut (par exemple des extraits [snippets] de code source pour revue du code) sur les canaux IRC[13].
PDF	Portable Document Format
récent	Par « récent », on entend au cours des trois (3) dernières années.
scénario de menace	Un ensemble d'événements de menace discrets, associés à une source de menace précise ou à des sources de menace multiples, partiellement ordonnés dans le temps. Synonyme de campagne de cybermenace[14].
SDK	Trousse de développement logiciel (Software Development Kit)
SSRN	Service de suivi du risque numérique; solution proposée par un entrepreneur qui englobe l'ensemble de l'infrastructure, du matériel, des logiciels et des services professionnels de celui-ci associés à la satisfaction des exigences énoncées dans la présente annexe A - Énoncé des capacités à l'égard du SSRN.
Tor	De l'anglais The Onion Router, signifie routeur en oignon.
TTP	Tactiques, techniques et procédures
utilisateur	Personne ayant un rôle défini dans l'utilisation d'un système informatique.
Web caché	Partie d'Internet qui est intentionnellement cachée aux moteurs de recherche, qui utilise des adresses IP masquées et qui n'est accessible qu'à l'aide d'un navigateur Web spécial : c'est une partie du Web invisible[15].
Web invisible	Partie d'Internet qui est cachée aux moteurs de recherche conventionnels, comme par le cryptage. Ensemble des sites Web non indexés, des bases de données privées et d'autres contenus non liés sur le Web invisible[16].
Web visible	Contenu du World Wide Web (WWW) mis à la disposition du grand public[17].
WHOIS	www.whois.com pour la consultation de domaines.
XLSX	Feuille de calcul Microsoft Excel Open XML

[12] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
[13] Pastebin - Wikipedia
[14] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments
[15] Dark web Definition & Meaning | Dictionary.com
[16] Deep web Definition & Meaning | Dictionary.com
[17] Definition of surface Web | PCMag