Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR
CYBER SECURITY

Clauses contractuelles recommandées en matière d'approvisionnement pour les centres des opérations de sécurité

Gestionnaires

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements ou suggérer des modifications, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 23 avril 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	23 avril 2025

D97-4/00-500-2025F-PDF
ISBN 978-0-660-76379-8

Vue d'ensemble

Pour que votre organisation puisse se protéger efficacement contre les cybermenaces, il est essentiel qu'elle ait une connaissance et un contrôle complets de son infrastructure et de ses activités numériques. Mettre en place un Centre des opérations de sécurité (COS) constitue l'une des façons d'atteindre cet objectif. Pour déployer et gérer avec succès un COS, il est crucial de définir des clauses contractuelles et des principes clairs lorsqu'il s'agit de confier la mise en place d'un COS à un fournisseur de services gérés (FSG) ou à un fournisseur de services de sécurité gérés (FSSG). On s'assure ainsi de la compréhension mutuelle et de la documentation des attentes.

Ces contrats doivent préciser les composantes clés des services de cybersécurité. Parmi celles-ci, les accords sur les niveaux de service (ANS), les ordres de travail et les normes de gouvernance. Collectivement, ces documents forment un cadre de services normatif qui donne aux clientes et aux clients l'assurance d'obtenir les services et solutions escomptés. Ce cadre garantit également la sécurité de leurs données et de leurs identités.

La présente publication décrit les services, responsabilités et livrables précis attendus d'un FSG/FSSG, de même que de l'organisation qui fait appel à ces services. On doit interpréter les recommandations fournies en fonction des principaux aspects fonctionnels et juridiques de la conclusion de marchés de services avec un fournisseur de services gérés, quel qu'il soit.

Table des matières

1 Introduction 5
1.1 Portée 5
1.2 Publications consultées 5
1.2.1 Ressources du gouvernement du Canada 6
1.2.2 Ressources de l'industrie et autres ressources 6
1.2.3 Nomenclature recommandée 6
2 Processus de sélection d'un fournisseur de centre des opérations de sécurité 7
2.1 Principaux services à envisager pour un centre des opérations de sécurité 8
2.1.1 Opérations de sécurité, surveillance et signalement 9
2.1.2 Soutien en cas d'incident 10
2.1.3 Analyses des menaces et renseignement sur les menaces 12
2.1.4 Documentation et procédures normales d'exploitation 13
2.1.5 Capacités supplémentaires : soutien avancé en matière de gestion des incidents, de criminalistique et d'analyse de maliciels 14
2.1.6 Entretien et exploitation des technologies de sécurité : 15
3 État de préparation du fournisseur 17
4 Conditions générales 18
5 Résumé 20

1 Introduction

Avec l'intensification des cybermenaces, les organisations se reposent de plus en plus sur les services de centres des opérations de sécurité (COS) pour surveiller la sécurité de l'information et gérer les risques numériques de manière efficace. Bien que les fonctions précises d'un COS puissent varier, elles comprennent habituellement une surveillance centralisée de la posture de sécurité générale à partir des données de journaux provenant des systèmes et des périphériques réseau. Les COS exploitent par ailleurs des outils comme les systèmes de gestion des informations et des événements de sécurité (GIES), qui interprètent les données de journaux et établissent des corrélations entre ces dernières et les incidents réseau. Également, le renseignement sur les menaces joue un rôle de premier plan dans les activités des COS en évaluant les événements liés aux systèmes réseau.

Étant donné la complexité que représente la mise en place d'un COS à maturité à partir de zéro, la présente publication vise à définir les attentes fondamentales pour évaluer les contrats visant l'établissement de COS et identifier les risques en matière d'approvisionnement. Ces considérations devraient s'arrimer avec les principaux aspects fonctionnels et juridiques des approvisionnements, que votre organisation travaille avec un FSG ou un FSSG.

Bien que les fournisseurs de services puissent proposer, au départ, des conditions et des modalités de service de base, l'équipe de direction de votre organisation a la responsabilité de s'assurer que ces modalités répondent aux besoins de sécurité opérationnelle de votre organisation, et demeurent souples pour permettre des ajustements futurs. Les conditions et modalités du contrat de service devraient être conçues en vue d'assurer les meilleurs résultats opérationnels pour votre organisation. Il est crucial que votre organisation prenne des mesures proactives pour garantir la fourniture des services, dont des mécanismes pour identifier, éviter et détecter les risques de sécurité, y réagir et s'en remettre.

Les clauses décrites dans la présente publication ne doivent pas être considérées comme des conseils juridiques, mais proposent un contexte pour évaluer les services liés aux COS et comprendre les conditions et modalités des fournisseurs de service potentiels.

1.1 Portée

La présente publication fournit des avis et des conseils d'ordre pratique pour la conclusion d'un contrat de services de COS du point de vue de la cybersécurité. Elle est pertinente à la fois pour les organisations utilisatrices et pour les fournisseurs de services. Bien que les exemples décrits ici ne représentent pas l'éventail complet ou définitif des pratiques exemplaires, ils fournissent néanmoins de précieuses informations, recueillies lors d'applications réalisées avec succès par des partenaires du gouvernement et de l'industrie.

1.2 Publications consultées

Dans le cadre de la préparation de la présente publication, le Centre pour la cybersécurité a tenu compte des informations provenant des documents et cadres de référence suivants.

1.2.1 Ressources du gouvernement du Canada

- Pratiques exemplaires sur la mise en place d'un centre des opérations de sécurité (COS) – ITSAP.00.500
- Processus d'intégrité de la chaîne d'approvisionnement et exigences liées à l'évaluation (PDF)
- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Appendice 1 - Obligations en matière de sécurité pour SaaS de palier 2 (PDF)
- Appendice 2 - Obligations en matière de protection des renseignements personnels (PDF)

1.2.2 Ressources de l'industrie et autres ressources

- Federal Risk and Authorization Management Program (FedRAMP) - Guidance /Help page) (en anglais seulement)
- Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-171) Revision 2 (en anglais seulement)
- Enhanced Security Requirements for Protecting Controlled Unclassified Information (NIST SP 800-172): A Supplement to NIST Special Publication 800-171 (en anglais seulement)
- Building a Security Operations Centre (SOC) (National Cyber Security Centre) (en anglais seulement)

1.2.3 Nomenclature recommandée

La présente publication met en évidence les principales clauses contractuelles pertinentes pour l'obtention de services de COS, plus particulièrement s'ils se fondent sur l'infonuagique, du point de vue de la cybersécurité. Ces clauses sont pertinentes à la fois pour les besoins immédiats et en prévision des besoins futurs.

Ce qui suit présente un résumé des clauses essentielles à prendre en considération, selon les services particuliers de COS dont une organisation a besoin :

- Lors de l'établissement d'un contrat de service, il est crucial de distinguer entre les exigences obligatoires et les exigences cotées. Les exigences obligatoires correspondent à celles auxquelles le fournisseur de services a l'obligation de satisfaire (ces clauses emploient des formulations comme « doit » avoir ou « doit » fournir). Dans le cas des exigences cotées, qui sont plus souples, on emploie les termes « devrait », « pourrait » ou « envisage ». Ces formulations suggèrent que le fournisseur possède déjà ces capacités.
- Pour les services qui font partie d'une feuille de route future ou qui ne sont pas encore en places, on utilisera des tournures comme « devra » ou « devra pouvoir ». Ces expressions expriment l'engagement du fournisseur à répondre aux attentes futures.

Il est important de reconnaître que certains services pourront nécessiter du temps pour les reconfigurer en vue de répondre à des besoins précis ou pourraient comprendre des fonctionnalités qui seront mises à jour dans des feuilles de route ultérieures. Par conséquent, les organisations doivent trouver l'équilibre entre les exigences immédiates et celles qui permettront un développement et une évolution.

2 Processus de sélection d'un fournisseur de centre des opérations de sécurité

Bon nombre d'organisations pourraient envisager de s'adresser, pour des services de COS, à un FSG ou à un FSSG offrant différents modèles d'abonnement pour tenir compte du coût et des capacités d'un COS externalisé. Le COS peut être hébergé dans un environnement appartenant au FSG ou au FSSG, et dans ce cas votre organisation peut acheminer tous les journaux vers l'architecture infonuagique du FSG ou du FSSG. Par ailleurs, votre organisation pourrait aussi retenir les services d'un FSG ou d'un FSSG pour exploiter les fonctionnalités du COS dans son architecture, toujours, mais en votre nom.

Lors de la sélection d'un FSG ou d'un FSSG, il y a bon nombre de questions et de décisions sur lesquelles votre organisation devra statuer, à l'interne, concernant l'approche et les services dont elle a besoin.

- Portée des services et offres : Saisissez bien la gamme de services offerts par le FSG/FSSG, et établissez s'il propose des capacités de chasse proactive aux cybermenaces et des capacités d'intervention réactive en cas d'incident.
- Extensibilité et flexibilité : Évaluez la capacité du fournisseur d'élargir ou de restreindre son offre de services en fonction de l'évolution des besoins de votre organisation, et évaluez la souplesse des services en réaction à des menaces émergentes ou à la croissance organisationnelle.
- Adaptation et intégration : Assurez-vous que le service de COS offert par le FSG/FSSG peut être ajusté en fonction de votre environnement propre, de votre industrie et de l'infrastructure de sécurité existante, et vérifiez sa compatibilité avec vos systèmes et outils actuels.
- Gestion et protection des données :
    - Posez des questions au sujet des outils et des technologies employées pour faire la collecte et l'analyse de données;
    - Assurez-vous de comprendre quelles données seront recueillies, comment elles seront utilisées et où elles seront stockées;
        - vérifiez dans quel cas et avec qui vos données pourront être partagées;
        - établissez clairement le processus d'approbation ou d'autorisation de partage de données;
    - Vérifiez que des mesures robustes sont en place pour protéger vos données sensibles et confidentielles.
- Accord sur les niveaux de service (ANS) : Passez en revue l'ANS pour vous assurer qu'il contient des définitions claires des attentes en matière de services, des livrables et des temps de réponse, et pour comprendre comment l'ANS sera évalué, surveillé et appliqué.
- Conformité et normes de sécurité : Assurez-vous que le fournisseur de COS a des pratiques de sécurité conformes aux normes de l'industrie et respecte la réglementation pertinente afin d'atténuer les risques, y compris les vulnérabilités de la chaîne d'approvisionnement.

- Évaluation des risques et profilage des menaces : Effectuez une évaluation exhaustive des risques en matière de cybersécurité afin d'identifier des menaces et des vulnérabilités particulières offrant une pertinence pour votre organisation.
    - Les ministères du gouvernement du Canada devraient consulter la publication intitulée La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
    - Les organisations qui ne font pas partie du gouvernement du Canada devraient consulter la publication Structured Threat Information eXpression (STIX) 2.1 framework (en anglais seulement)
- Clarté contractuelle et responsabilités : Établissez des dispositions contractuelles claires, en soulignant les responsabilités de votre organisation de même que celles du fournisseur de services, conformément au modèle de responsabilité partagée.
- Principales considérations pour le choix d'un fournisseur de COS : Assurez-vous que des dispositions prévoient des examens et des mises à jour périodiques, et des ajustements aux services selon les besoins.

Pour plus d'information, veuillez consulter la publication Pratiques exemplaires sur la mise en place d'un centre des opérations de sécurité (COS) (ITSAP.00.500).

De manière générale, en qualité d'organisation qui demande les services, vous devez faire les démarches nécessaires, au préalable, pour décider d'une stratégie concernant le COS et de sa portée. Il vous faut donc identifier les actifs, dont les systèmes et les données, qui ont un caractère sensible et qui nécessitent une surveillance et une protection. Pour plus d'information sur l'inventaire et la catégorisation des actifs, veuillez consulter la publication Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103)

2.1 Principaux services à envisager pour un centre des opérations de sécurité

Voici certains des principaux services qui font partie d'un COS efficace, accompagnés d'exemples de clauses contractuelles pour vous aider à ébaucher le texte de vos ententes de service et à formuler vos attentes.

Examinez les services essentiels ci-dessous :

- **Opérations de sécurité, surveillance et signalement :** Surveillance et analyse en continu des événements de sécurité, et signalement en temps opportun. Exemple de clause : « Le fournisseur assurera une surveillance permanente et signalera les incidents en temps quasi réel. »
- **Soutien en cas d'incident :** Intervention et appui rapides en cas d'incident de sécurité. Exemple de clause : « Le fournisseur doit offrir des services d'intervention en temps quasi réel en cas d'incident. »
- **Analyses des menaces et renseignement sur les menaces :** Identification et analyse proactive des menaces potentielles. Exemple de clause : « Le fournisseur doit fournir régulièrement des mises à jour des informations sur les menaces. »
- **Documentation et procédures normales d'exploitation (PNE) :** Tenue à jour de documentation sur la sécurité et de PNE détaillées. Exemple de clause : « Le fournisseur doit conserver une documentation de sécurité et des PNE exhaustives et à jour, selon le modèle de responsabilité partagée. »

- **Capacités supplémentaires : Soutien avancé en matière de gestion des incidents, de criminalistique et d'analyse des maliciels :** Soutien spécialisé pour les incidents complexes, y compris en matière d'analyse criminalistique. Exemple de clause : « Le fournisseur doit offrir des capacités spécialisées en gestion des incidents et en analyse criminalistique. »
- **En continu, évaluation des vulnérabilités et analyse de l'assurance de la sécurité :** Évaluations régulières visant à identifier et à atténuer les vulnérabilités. Exemple de clause : « Le fournisseur doit effectuer de manière périodique des évaluations des vulnérabilités et fournir des rapports. »
- **Entretien et exploitation des technologies de sécurité :** Vérification de l'utilisation et de l'entretien efficaces des technologies de sécurité. Exemple de clause : « Le fournisseur doit exploiter et tenir à jour l'infrastructure et les technologies qui permettent d'assurer le service ».

Votre organisation devrait également songer à des services supplémentaires qui pourraient être nécessaires dès le départ ou le devenir ultérieurement, selon l'évolution des besoins en matière de sécurité. Parmi ceux-ci, la gestion de la conformité, l'évaluation des risques, la sécurité infonuagique et des initiatives de formation en matière de cybersécurité.

2.1.1 Opérations de sécurité, surveillance et signalement

Les opérations de sécurité, la surveillance et les signalements ont une importance cruciale pour l'examen et l'analyse des données liées aux événements, aux incidents ou aux violations, de même que pour évaluer l'état des systèmes d'information ou des réseaux. L'objectif premier consiste à détecter toute activité inhabituelle ou non autorisée, et à recueillir des données pertinentes pour la sécurité, afin de mieux comprendre le comportement des systèmes. Ce processus est essentiel pour atténuer les vulnérabilités réseau et identifier les menaces internes et externes.

Rôle et fonctionnalités des suites d'outils ou des capacités permettant l'agrégation de journaux comme les outils de GIES

Le système de gestion des informations et des événements de sécurité (GIES) constitue un outil essentiel pour les fins de ce processus. La GIES facilite la centralisation des données en provenance de diverses sources, y compris de dispositifs, d'applications et de points d'extrémité. Elle favorise :

- la surveillance des événements en temps réel et le suivi des événements passés;
- l'analyse détaillée et la mise en corrélation de l'information;
- de meilleures capacités de détection des menaces et d'intervention.

Principaux points à considérer pour l'externalisation

Lorsque l'on songe à impartir la surveillance et le signalement à un FSG/FSSG, il est important d'évaluer :

- l'ampleur et la fréquence des services de surveillance;
- les stratégies de stockage des données, y compris la question de la résidence des données et les mesures de sécurité;
- les certifications du fournisseur, particulièrement en ce qui a trait aux normes de cybersécurité et de conformité;
- la capacité du fournisseur d'intégrer ses services à votre infrastructure de sécurité existante, dans les cas où le fournisseur dispense ses services sur les lieux mêmes de l'organisation.

Clauses contractuelles recommandées

Le Centre pour la cybersécurité recommande aux organisations d'intégrer des clauses particulières liées à la surveillance, au signalement et à l'accessibilité, lors de la conclusion d'un contrat de COS avec un FSG ou un FSSG. Nous fournissons ci-dessous des exemples de formulations que votre organisation pourrait souhaiter inclure dans ses contrats.

Surveillance

L'entrepreneur doit :

- fournir un service ininterrompu (jour et nuit/toute l'année) de surveillance des événements de sécurité;
- aux fins d'enquête sur les incidents, analyser les données liées aux événements de sécurité à l'aide des journaux système et d'autres moyens de détection;
- passer en revue et enregistrer les journaux de vérification à la recherche d'activités inappropriées ou illégales, afin de faciliter la reconstruction des événements survenus à l'occasion d'incidents de sécurité;
- faire enquête et identifier précisément les anomalies décelées par les dispositifs de sécurité ou rapportées par diverses parties prenantes.

Signalement

L'entrepreneur doit :

- fournir des notifications, des renvois au palier supérieur et des rapports quotidiens exploitables en se fondant sur le renseignement sur les menaces et l'analyse des événements de sécurité;
- documenter toutes les activités d'enquête et les signalements d'incidents à l'appui du cadre d'intervention en cas d'incident de l'organisation;
- fournir par écrit des rapports exhaustifs au sujet de tous les événements de sécurité qui se produisent, en suivant les procédures établies et les protocoles de signalement;
- fournir à l'organisation la capacité de communiquer avec le fournisseur et de mener une enquête si des activités suspectes se produisent.

Disponibilité

L'entrepreneur doit assurer la disponibilité et l'intégrité opérationnelle permanentes de tous les systèmes et de toutes les applications du COS.

Références

- Journalisation et surveillance de la sécurité de réseau – (ITSAP.80.085)
- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137, Appendix D) (en anglais seulement)

2.1.2 Soutien en cas d'incident

Le soutien en cas d'incident constitue une composante cruciale d'un modèle de COS en tant que service (d'un FSG/FSSG). Votre organisation et le FSG/FSSG devez collaborer pour gérer les incidents efficacement. Il est crucial de disposer d'un plan

d'intervention en cas d'incident qui précise comment votre organisation procédera pour détecter les incidents, y réagir et s'en rétablir. Ce plan devrait définir clairement le rôle du COS, y compris l'étendue de son implication, de même que les responsabilités de l'équipe interne de votre organisation. Les deux scénarios qui suivent présentent les principaux aspects du soutien en cas d'incident, de même que des exemples de clauses contractuelles pour des COS hébergés dans l'environnement d'un FSG/FSSG (à l'extérieur de l'architecture de votre organisation) ainsi que pour des COS dont l'exploitation s'effectue au sein de l'architecture de l'organisation.

Dans les deux cas, il est essentiel d'établir un partenariat fondé sur la transparence, la confiance et la responsabilité partagée des résultats en matière de sécurité. L'entente contractuelle devrait être détaillée et claire, et accorder une attention particulière aux interventions en cas d'incident, à la protection des données, à la conformité et aux niveaux de service. Ceci permet de s'assurer que tant l'organisation que le FSG/FSSG ont une compréhension commune de leurs rôles et responsabilités respectifs en matière de protection des actifs numériques de l'organisation.

Scénario 1 : COS hébergé en dehors de l'architecture de votre organisation

Si votre COS est hébergé en dehors de l'architecture de votre organisation, envisagez les principaux aspects suivants en ce qui a trait au soutien en cas d'incident :

- **Détection et signalement des incidents :** Le FSG/FSSG doit rapidement identifier les incidents de sécurité et les signaler à l'organisation. L'entente devrait préciser les délais dans lesquels le signalement doit être effectué à la suite de la détection d'un incident.
- **Analyse des incidents et intervention en cas d'incident :** Le FSG/FSSG devrait fournir une analyse détaillée des incidents, y compris de leurs répercussions potentielles, et prendre les mesures d'intervention convenues.
- **Protection des données et confidentialité :** Le FSG/FSSG doit adhérer à de strictes normes de protection des données et de confidentialité, particulièrement du fait qu'il stockera et traitera des données organisationnelles sensibles dans son environnement.
- **Contrôles d'accès et pistes de vérification :** Le FSG/FSSG doit mettre en place des mesures de contrôle d'accès robustes et conserver des pistes de vérification de toutes les activités liées aux services de COS.
- **Conformité et exigences réglementaires :** Le FSG/FSSG doit se conformer aux exigences réglementaires et de conformité pertinentes, et fournir la documentation et le soutien requis pour les audits de conformité.

Exemples de clauses contractuelle pour le soutien en cas d'incident :

L'entrepreneur doit **:**

- lors de la détection de tout incident de sécurité, aviser le client dans les délais négociés ou convenus et fournir de l'information détaillée sur la nature, la portée et les répercussions de l'incident;
- mettre en place et maintenir des mesures exhaustives de protection des données, en conformité avec les lois et la réglementation applicables, afin de protéger les données du client contre tout accès et toute divulgation, modification ou destruction non autorisés;
- dès la détection d'un incident, s'engager à rétablir la disponibilité dans un délai de [insérer le délai convenu] conformément à l'ANS et à entamer les mesures correctrices dans un délai de [préciser le délai].

Scénario 2 : COS exploité dans l'architecture de votre organisation

Si votre COS est exploité au sein de l'architecture de votre organisation, envisagez les principaux aspects suivants en ce qui a trait au soutien en cas d'incident.

- **Intégration à l'infrastructure existante :** Le FSG/FSSG doit intégrer de manière transparente ses services de COS à l'infrastructure existante de l'organisation, en réduisant au minimum les perturbations.
- **Procédure de traitement des incidents :** Pour le renvoi des incidents aux paliers supérieurs, l'intervention en cas d'incident et la résolution des incidents, le FSG/FSSG doit définir des procédures claires, et adaptées aux politiques et procédures de l'organisation.
- **Formation et sensibilisation :** Le FSG/FSSG pourrait avoir à fournir de la formation et/ou à effectuer un transfert de connaissances au personnel de l'organisation concernant la sensibilisation à la sécurité et les procédures d'intervention en cas d'incident.
- **Suivi du rendement et production de rapports** : L'exécution d'examens du rendement et la production de rapports sur une base régulière constituent des activités essentielles pour s'assurer que les services du COS satisfont aux exigences de sécurité de l'organisation.
- **Amélioration continue :** Le contrat devrait comporter des dispositions sur l'amélioration continue des services du COS, y compris sur la mise à jour régulière des outils et des processus de sécurité.

Exemples de clauses contractuelle pour le soutien en cas d'incident

L'entrepreneur doit :

- s'assurer que les services du COS sont entièrement compatibles avec les systèmes existants et l'infrastructure du client, et assumer la responsabilité de toute modification requise pour leur intégration;
- respecter les procédures et les délais d'intervention en cas d'incident du client, afin de s'assurer que les incidents sont résolus de manière à en réduire les répercussions sur ses opérations;
- fournir des rapports de rendement mensuels précisant les incidents détectés, les délais d'intervention et les résultats de l'intervention, y compris toute recommandation qui contribuerait à améliorer la posture de sécurité;

Pour obtenir davantage de renseignements, consulter la publication Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)

2.1.3 Analyses des menaces et renseignement sur les menaces

L'analyse des menaces et le renseignement sur les menaces forment une composante cruciale d'un portefeuille de cybersécurité proactif. Le renseignement, lorsqu'il est précis et opportun, permet aux décideuses et décideurs de prendre des décisions éclairées et fondées sur les données. Le Centre pour la cybersécurité, ainsi que d'autres ressources, proposent de précieuses informations, par l'entremise de publications et de services actifs, afin d'aider les organisations à tirer le meilleur parti du renseignement sur les menaces. Il est essentiel pour les organisations de s'assurer que leur FSG/FSSG se tient au courant des cybermenaces émergentes et des cybermenaces sophistiquées.

Éléments clés du renseignement sur les menaces

- **Surveillance continue :** se tenir au courant de l'évolution des cybermenaces et des tendances;

- **Analyse technique :** faire l'analyse détaillée des incidents afin de comprendre les vecteurs et les méthodes d'attaque;
- **Partage de renseignement :** mettre à profit les ressources partagées pour obtenir une meilleure vue d'ensemble du contexte de menaces.

Exemples de clauses contractuelles concernant l'analyse des menaces et le renseignement sur les menaces

L'entrepreneur doit :

- détecter, surveiller, analyser et atténuer les cybermenaces qui se présentent comme ciblées, de nature très organisée ou sophistiquées;
- préserver une excellente connaissance de la situation en ce qui concerne les activités et risques en cours en matière de cybersécurité;
- mettre à profit diverses sources de renseignement pour obtenir de l'information sur les cybermenaces, et conduire des analyses techniques poussées des incidents qui touchent les réseaux de l'organisation;
- analyser les données sur les menaces regroupées à partir d'une multitude de sources afin d'être en mesure d'avertir rapidement d'attaques imminentes contre les réseaux de l'organisation;
- produire des rapports sur les vecteurs d'attaque du réseau technique et au niveau de l'hôte, les cybermenaces émergentes, les nouvelles vulnérabilités et les tendances en cours auprès des auteurs de menace malveillants;
- constituer et entretenir des bases de données pour cataloguer les menaces en cours et en faire le suivi, et améliorer ainsi la posture de sécurité de l'organisation;
- intégrer les informations fournies par le renseignement aux stratégies plus globales de l'organisation en matière de cybersécurité, et aux plans d'intervention en cas d'incident.

L'intégration d'activités exhaustives d'analyse des menaces et de renseignement sur les menaces aux offres des FSG/FSSG constitue un élément crucial pour que les organisations puissent garder une longueur d'avance sur les cybermenaces. Le rôle des FSG/FSSG va au-delà de la simple surveillance; il comprend des analyses approfondies, des apprentissages continus et l'intégration du renseignement au cadre de cybersécurité global de l'organisation.

Références

- Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137, Appendix D) (en anglais seulement)
- Évaluation des menaces de base : Cybercriminalité
- Évaluation des cybermenaces nationales

2.1.4 Documentation et procédures normales d'exploitation

Des PNE et une documentation exhaustive constituent des éléments cruciaux pour s'assurer que toutes les parties impliquées dans le COS s'entendent au sujet des méthodes et des pratiques. Ces documents représentent des points de

référence pour effectuer des opérations cohérentes et efficaces au sein du COS, et viennent faciliter la formation et favoriser la clarté opérationnelle.

Principaux éléments clés en matière de documentation

- **Diagrammes de l'installation de sécurité déployée :** fournissent une représentation visuelle de l'installation de sécurité déployée à des fins de référence et pour en assurer la compréhension.
- **Mises à jour régulières des PNE :** mise à jour des PNE en fonction des changements opérationnels, afin d'assurer le maintien de leur pertinence.
- **Production de rapports sur le rendement et le signalement des incidents :** ces rapports fournissent des informations sur les activités du COS, le traitement des incidents et l'efficacité opérationnelle.

Exemples de clauses contractuelles pour les PNE et la documentation

L'entrepreneur doit :

- créer et tenir à jour des diagrammes des nouvelles installations de sécurité déployées ou des installations de sécurité modifiées, en tenant compte de tous les systèmes et de toutes les applications liées au COS;
- élaborer et mettre à jour régulièrement les PNE du COS, particulièrement à la suite de changements touchant les opérations ou les technologies du COS, et produire sur une base régulière des rapports écrits, dont ce qui suit :
  - résumés quotidiens, hebdomadaires et mensuels des activités du COS;
  - mesures du rendement et état des incidents de sécurité;
  - actions menées à bien et jalons atteints pendant la période visée par le rapport;
- soumettre des rapports exhaustifs, dont ce qui suit :
  - mises à jour mensuelles sur les progrès et les développements;
  - activités prévues, problèmes/enjeux identifiés et solutions proposées;
  - retards anticipés et ressources utilisées durant la période.

Il est essentiel de définir des PNE claires et détaillées et des protocoles de documentation, de manière à maintenir l'efficacité opérationnelle dans l'environnement du COS. Ces documents, en plus de guider les opérations quotidiennes, constituent également des outils cruciaux pour la formation, le suivi du rendement et la planification stratégique.

2.1.5 Capacités supplémentaires : soutien avancé en matière de gestion des incidents, de criminalistique et d'analyse de maliciels

En plus du soutien habituel en matière de gestion des incidents, les organisations veulent ou souhaitent souvent obtenir des capacités avancées, notamment en matière de criminalistique et d'analyse de maliciels. Ces services sont essentiels pour effectuer des enquêtes approfondies et résoudre des cyberincidents sophistiqués, ainsi que pour comprendre les vecteurs d'attaque et améliorer les postures de sécurité.

Services de soutien avancés essentiels

- **Criminalistique et analyse de maliciels :** enquêtes approfondies sur les incidents afin de comprendre la nature et l'incidence des compromissions.
- **Rétroingénierie et analyse du trafic :** examen détaillé des logiciels malveillants et du trafic réseau pour mettre au jour les méthodologies utilisées par les menaces.

Exemples de clauses contractuelles pour le soutien avancé en matière de gestion des incidents

L'entrepreneur doit :

- fournir, selon les besoins, un soutien en matière de gestion, d'intervention et de reprise en cas d'incident de sécurité, à la fois sur place et à distance;
- effectuer des analyses techniques poussées d'activités potentiellement malveillantes à l'aide des données liées aux événements de sécurité que le COS détient;
- effectuer des analyses criminalistiques détaillées aux points terminaux/au niveau de l'hôte et des analyses des mémoires;
- mener à bien le tri et l'analyse approfondie de maliciels, y compris la rétro-ingénierie des logiciels Windows, des courriels d'hameçonnage et d'autres codes d'exploitation côté client.
- effectuer des analyses de criminalistique numérique sur des supports provenant d'hôtes compromis afin d'évaluer la portée et la nature de l'intrusion;
- effectuer la rétro-ingénierie de la séquence d'événements survenus lors d'intrusions ou d'attaques afin d'en tirer une compréhension approfondie;
- exécuter des analyses de fichier statiques et dynamiques afin d'identifier les caractéristiques, le but et la provenance du maliciel;
- recommander des contremesures pour déjouer les maliciels et autres codes malveillants exploitant les systèmes de l'organisation;
- proposer des modifications aux politiques et aux procédures en fonction des résultats obtenus lors des enquêtes, afin de renforcer les interventions en cas d'incidents liés à des maliciels;
- effectuer des analyses de trafic réseau poussées au niveau des paquets afin d'identifier des anomalies, des tendances et des schémas.

Le soutien avancé à la gestion des incidents, particulièrement en ce qui a trait à l'analyse criminalistique et à l'analyse de maliciels, constitue une composante essentielle d'une offre de services robuste d'un FSG/FSSG. Ces services, en plus d'aider à résoudre les incidents de sécurité du moment, jouent également un rôle de premier plan pour ce qui est de raffiner les politiques organisationnelles et de renforcer le cadre global de cybersécurité.

Veuillez consulter la publication Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003) pour plus d'information.

2.1.6 Entretien et exploitation des technologies de sécurité :

Dans le contexte d'un FSG/FSSG, la gestion des technologies clés, comme le système de GIES, les systèmes de détection et de prévention des intrusions (SDPI) et de prévention de la perte de données (PPD), est de toute première importance. Ces

technologies constituent la pierre angulaire de l'exécution d'opérations de cybersécurité efficaces. Les contrats devraient comporter des clauses précises pour s'assurer que ces outils sont exploités et entretenus de manière efficace, tout particulièrement quand l'organisation évolue et prend de l'expansion.

Principales responsabilités en matière de gestion des technologies

- **Maintenance et ajustement du système :** mettre à jour et ajuster les systèmes de sécurité sur une base régulière, afin d'assurer leur précision et leur efficacité.
- **Efficacité opérationnelle :** assurer le fonctionnement continu et le rendement optimal de toutes les technologies de sécurité.
- **Capacité d'adaptation au changement :** assurer la flexibilité voulue pour permettre d'adapter les outils et systèmes en fonction de l'évolution des besoins et de l'envergure de l'organisation.

Exemples de clauses contractuelles pour la gestion des technologies

L'entrepreneur doit :

- entretenir efficacement le GIES pour faire l'agrégation et l'analyse des données de diverses sources comme les capteurs réseau, les pare-feux, les systèmes antivirus et les scanneurs de vulnérabilité;
- gérer l'administration, la gestion et la configuration de tous les outils du COS, y compris le GIES, le SDI/SPI, le DLP et d'autres systèmes de sécurité spécialisés;
- élaborer et mettre à jour des signatures pour les dispositifs de sécurité, des rapports sur le rendement et des paramètres pertinents pour faire le suivi de l'efficacité du système;
- ajuster le GIES et le SDI/SPI pour réduire au minimum les faux positifs et améliorer la précision en matière de détection;
- de manière continue, exploiter, gérer et mettre à jour toutes les technologies de sécurité, et s'assurer qu'elles sont configurées adéquatement pour permettre un rendement optimal;
- veiller à ce que tous les flux de sécurité pertinents soient journalisés et corrélés de manière efficace dans le système GIES du COS;
- installer, mettre à jour ou modifier les composants et les outils de sécurité du réseau selon ce qui est nécessaire pour conserver une couverture exhaustive et un rendement optimal adaptés à la croissance organisationnelle;
- installer ou modifier les composants de sécurité du réseau, les outils et les autres systèmes selon ce qui est nécessaire pour conserver une couverture exhaustive et un rendement optimal adaptés à la croissance organisationnelle.

La gestion efficace des technologies clés à l'intérieur du cadre d'un FSG/FSSG constitue un élément essentiel pour le maintien d'une posture de cybersécurité robuste. Il s'agit non seulement d'effectuer la maintenance opérationnelle de ces outils, mais aussi de les améliorer et de les adapter pour suivre l'évolution des besoins de l'organisation.

3 État de préparation du fournisseur

Lors de la conclusion d'un contrat avec un FSG pour l'obtention de services de COS, il est essentiel de prévoir des clauses précises qui garantissent que le fournisseur peut offrir les services de l'envergure demandée et se conforme à certaines normes. Ces clauses servent à valider l'expérience du fournisseur, son respect des obligations légales et sa capacité à prendre en charge les besoins précis de votre organisation.

Clauses contractuelles clés relatives à l'état de préparation du fournisseur

- **Exigences :** L'entrepreneur devrait avoir un nombre minimum d'années d'expérience de la prestation de services de COS et d'engagements de même ampleur, de même envergure et de même complexité.
- **Respect des lois canadiennes :** L'entrepreneur devrait avoir une expérience de la prestation de services au Canada et de l'adhésion aux lois canadiennes qui touchent la protection de la vie privée et des données.
- **Droits en matière d'audits et de conformité :** L'organisation se réserve le droit d'effectuer des visites du COS à des fins d'audits, d'examen et de conformité.
- **Planification en matière de continuité des activités :** L'entrepreneur doit avoir un plan de continuité des activités (PCA) pour le COS, afin d'assurer la continuité du service.
- **Exigences en matière de certification :** L'entrepreneur doit respecter les exigences en matière de certification de l'industrie ou du secteur, comme les normes SOC 2 Type 2 et ISO 27001, les contrôles de sécurité critiques (CSC) du CIS, la certification de niveau 2 de la Cloud Security Alliance (CSA) ou la norme ISO 27017.
- **Habilitations de sécurité et vérification des antécédents du personnel :** Le personnel de l'entrepreneur devrait avoir fait l'objet des vérifications des antécédents et obtenu les habilitations requises, en fonction des besoins.
- **Conformité au cadre des contrôles de cybersécurité :** Des cadres des contrôles de cybersécurité doivent être mis en place dans les installations des COS (DRI International, NIST).
- **Responsabilité et dédommagement :** L'entrepreneur devrait fournir des précisions sur le partage des responsabilités en cas d'intrusion, et fournir des détails sur sa couverture-responsabilité aux fins de dédommagement.

Il est essentiel d'intégrer ces clauses cruciales à tout contrat avec un FSG visant l'obtention de services de COS, pour s'assurer que le fournisseur a toute la préparation requise et a la capacité de satisfaire aux exigences précises de votre organisation. Ces clauses couvrent un éventail de secteurs cruciaux allant de l'expérience acquise au respect des lois en passant par la continuité des activités et les cadres de cybersécurité, ce qui fournit une approche exhaustive pour évaluer l'état de préparation du fournisseur.

4 Conditions générales

Du point de vue de la sécurité, les éléments contractuels doivent être normatifs et conformes aux cadres et aux approches reconnus afin que le FSG/FSSG puisse établir la manière dont il aborde et maintient la posture de sécurité indiquée par l'organisation. Dans de nombreux cas, le recours aux modalités d'un fournisseur donné, telles qu'elles sont énoncées dans un contrat ou un contrat de licence utilisateur final (EULA pour *End User Licensing Agreement*), peut être considéré comme acceptable. Toutefois, pour certaines organisations ayant des besoins particuliers ou pour celles qui sont assujetties à des autorités réglementées, les équipes juridiques auront peut-être à négocier à l'aide de certaines des clauses types indiquées dans le présent guide. Si vous avez des préoccupations à l'égard de points particuliers, obtenez des conseils juridiques lorsque la chose est possible.

Les organisations devraient accorder une attention particulière aux points suivants lors de la négociation de contrats avec des fournisseurs de services et, au besoin, consulter leur conseillère ou conseiller juridique :

- **Protection des secrets commerciaux**
  - Renseignez-vous sur la manière dont le fournisseur de services séparera ou protégera les secrets commerciaux (p. ex. matériel breveté et image de marque légale) au sein de son système.
  - Assurez-vous que les modalités précisent que l'organisation conserve la propriété et le contrôle de ses secrets commerciaux, même lorsqu'ils sont confiés au fournisseur de services.
- **Propriété intellectuelle**
  - Discutez des mesures permettant d'étiqueter, d'identifier et de protéger la propriété intellectuelle qui pourrait ne pas être officiellement protégée, par exemple par des brevets, mais qui revêt une importance cruciale pour les opérations de l'organisation.
  - Établissez clairement, dans le contrat, que la propriété intellectuelle demeure la possession de l'organisation, indépendamment du fait qu'elle soit confiée au fournisseur de services.
- **Indemnisation/limitation de responsabilité :** Définissez le niveau de responsabilité applicable, songez aux difficultés qui pourraient se présenter, particulièrement lorsque plusieurs fournisseurs de services sont impliqués.
- **Considérations liées au modèle de soutien**
  - Si votre organisation est assujettie à des contraintes réglementaires concernant l'emplacement du soutien ou l'endroit où les ressources peuvent résider, discutez avec le fournisseur de services et convenez de modèles de soutien.
  - Vérifiez dans quelle mesure le modèle de soutien mondial du fournisseur, par exemple l'approche de « soutien continu ajusté aux fuseaux horaires » est compatible avec les exigences réglementaires.
- **Politiques en matière de migration de données :** Prévoyez les futurs besoins possibles en matière de migration de données, y compris :
  - les coûts liés aux données entrantes et sortantes;
  - les délais et les processus liés aux activités de migration;
  - les politiques de conservation post-migration.
- **Conformité aux cadres de sécurité :** Assurez-vous que les éléments du contrat se conforment aux cadres de cybersécurité établis et aux pratiques exemplaires.

- **Contrat de licence utilisateur final et contrat sur mesure :** Tandis que les clauses types d'un contrat de licence utilisateur final (EULA pour *End User Licensing Agreement*) peuvent convenir pour un usage général, elles pourraient ne pas suffire pour des organisations présentant des besoins particuliers en matière de sécurité ou pour celles qui doivent se conformer à des exigences réglementaires rigoureuses.
- **Négociations juridiques pour des besoins sur mesure**
  - Pour les organisations qui ont des exigences uniques ou des obligations réglementaires, les négociations entre équipes juridiques sont souvent nécessaires pour adapter le contrat de manière adéquate.
  - Les clauses données en exemple dans le présent document peuvent servir à guider ces négociations.
- **Obtention de conseils juridiques**
  - L'organisation devrait obtenir des conseils juridiques, surtout s'il y a des sujets particuliers de préoccupation ou si l'organisation est assujettie à des autorités réglementées.
  - L'expertise juridique peut permettre de s'assurer que les contrats sont exhaustifs, conformes et adaptés aux besoins uniques de l'organisation.

Lors de la conclusion d'un contrat avec un fournisseur, particulièrement lorsqu'il s'agit de FSG/FSSG, les organisations doivent s'assurer que les considérations d'ordre juridique et opérationnel sont traitées clairement dans le contrat. Parmi celles-ci, la conservation de la propriété intellectuelle et des secrets commerciaux, la définition claire des responsabilités, une compréhension approfondie des contraintes réglementaires et les préparatifs en prévision de la migration potentielle de données. Les organisations devraient consulter une conseillère ou un conseiller juridique pour s'assurer que le traitement de ces aspects protège bien les intérêts de l'organisation.

5 Résumé

Un COS combine des personnes, des processus et des technologies en vue d'améliorer la résilience d'une organisation contre les cybermenaces.

Que le service de COS soit assuré par une équipe interne dans un local prévu à cet effet au sein d'une organisation ou soit entièrement ou partiellement externalisé à une équipe de professionnelles et professionnels de la sécurité de l'information, il constitue une première ligne de défense, cruciale pour assurer la prévention et la détection des cyberattaques, de même que le rétablissement en cas d'incident.

Ceci est particulièrement vrai si l'on considère l'expansion des technologies opérationnelles, mobiles et infonuagiques, et des systèmes de contrôle industriels. Que le travail soit effectué à l'interne, en mode hybride ou entièrement à distance, votre organisation aura besoin d'échanger les mêmes intrants et extrants avec votre COS. Les conseils fournis dans le présent document devraient aider votre organisation à rédiger des clauses contractuelles qui vous permettront d'avoir l'assurance que vos fournisseurs répondent à vos besoins. Tel qu'indiqué, il ne s'agit pas d'un avis juridique.

Dans l'ensemble, le message à retenir est que votre organisation devrait collaborer avec le FSG/FSSG sélectionné en vue d'assurer une compréhension mutuelle et également de vérifier et d'établir ce qui peut être fait pour répondre aux besoins particuliers de votre organisation.