GoSec 25

Table Ronde CISO

Septembre 2025

ANGLES MORTS DU SAAS, LIMITES DE LA REPRISE APRÈS SINISTRE ET DÉFI DE L'IA

GoSec 25

Table ronde des CISO

Septembre 2025

RÉSUMÉ EXÉCUTIF

Lors du GoSec25 à Montréal, une quinzaine de CISO et dirigeants sécurité issus de secteurs variés (finance, énergie, logistique, divertissement, et industrie manufacturière) se sont réunis pour une discussion franche et confidentielle sur les défis les plus pressants de la cybersécurité moderne.

L'objectif : Échanger entre pairs sur des enjeux concrets qui redéfinissent la gouvernance technologique au Canada.

La conversation a révélé un paysage en pleine mutation, où trois forces convergent :

1

La prolifération du SaaS qui multiplie les angles morts de visibilité

Les participants ont reconnu que les applications SaaS critiques (comme Salesforce, Dayforce ou M365) fonctionnent souvent comme des zones d'ombre : même intégrées à des environnements sécurisés, elles demeurent partiellement opaques.

2

La pression des cadres de conformité, qui rassurent sans garantir la sécurité continue

Les certifications comme SOC 2 ne fournissent qu'une assurance limitée.

Les stratégies de reprise après sinistre (DR) dans ces environnements infonuagiques dévoilent elles aussi une réalité préoccupante : quelle que soit la rigueur des sauvegardes, la disponibilité finale des systèmes dépend toujours du fournisseur.

3

L'accélération de l'adoption de l'IA, porteuse d'efficacité mais aussi de nouveaux risques

Les outils d'intelligence artificielle s'intègrent à un rythme fulgurant dans les flux opérationnels : révision de code, détection des fraudes, conformité, automatisation.

Mais si les gains de productivité sont indéniables, la gouvernance et le ROI demeurent difficiles à mesurer, et les risques de fuite de données sensibles préoccupent.

| ***Thème transversal*** *: la gouvernance, la visibilité et la culture sécurité doivent évoluer au même rythme que la technologie.*

Les CISO ont convenu que la résilience ne se limite plus à la technique.

Elle repose désormais sur une gouvernance multicouche, un contrôle renforcé des fournisseurs, et une formation continue des utilisateurs pour transformer les angles morts en leviers de sécurité durable.

GoSec 25

Table ronde des CISO

Septembre 2025

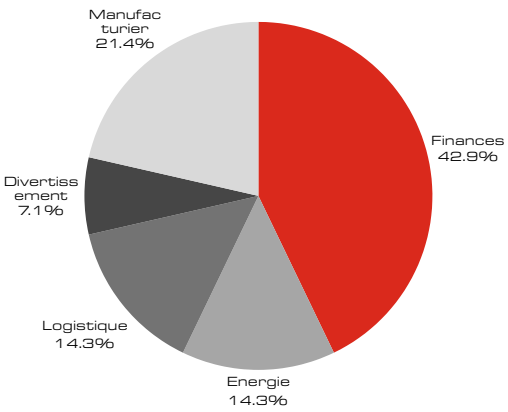
INTRODUCTION

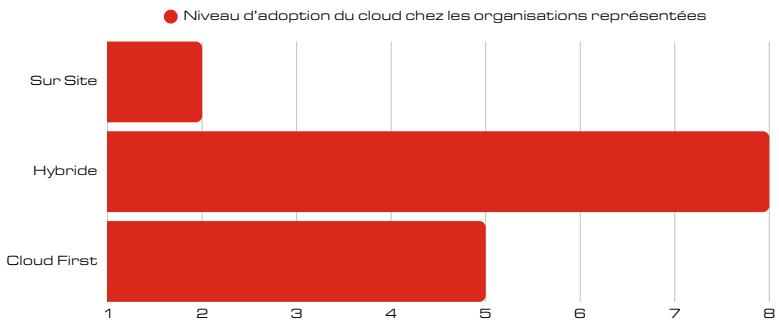
La cybersécurité gagne chaque année en complexité, alors que les organisations s'appuient de plus en plus sur des écosystèmes hybrides, distribués et interconnectés. Les CISO font face à un double impératif : accompagner l'innovation tout en préservant la confiance.

La rencontre a offert un espace d'échange libre entre pairs, sans influence fournisseur, centré sur la réalité terrain : les angles morts du SaaS, les limites de la conformité, la reprise après sinistre dans le cloud, et les implications de l'IA pour la gouvernance. De ces échanges est née une conviction commune : la résilience n'est plus une fonction, c'est une culture. Elle exige des organisations une adaptation constante à la vitesse même de la transformation numérique.

Ce livre blanc résume les principaux enseignements de cette table ronde, traduits en pistes concrètes pour les responsables sécurité d'aujourd'hui. Les quatre thèmes dominants ; Sécurité SaaS, conformité, reprise après sinistre et adoption de l'IA, illustrent l'équilibre fragile mais essentiel entre innovation, gouvernance et résilience organisationnelle.

PROFIL DES PARTICIPANTS





Parmi les 15 participants, certains mènent des organisations "cloud-first", gérant des dizaines de plateformes SaaS et une infrastructure presque entièrement dématérialisée. D'autres évoluent dans des environnements où le risque ne se tolère pas, comme l'énergie, où les systèmes opérationnels demeurent strictement sur site.

Mais tous partagent pourtant un même défi : protéger des environnements de plus en plus complexes, avec des ressources souvent limitées et une pression constante à innover. Autour de la table, l'expérience cumulée dépassait largement plus d'une centaine d'années de gestion du risque, entre sécurité technique, gouvernance organisationnelle et leadership stratégique.

Cette diversité de profils et d'appétits au risque a fait toute la richesse de la discussion. Les uns ont mis l'accent sur la vitesse d'adoption et la flexibilité nécessaires pour suivre le rythme de l'innovation. Les autres ont rappelé l'importance de la résilience, de la continuité et du contrôle, même au prix d'un déploiement plus lent.

FAITS SAILLANTS ET TENDANCES

- **Sécurité SaaS : Lacunes de visibilité et réalités opérationnelles**

Les CISO ont souligné que des plateformes telles que Salesforce et Dayforce représentent des angles morts potentiels. Même avec des intégrations SSO, ces systèmes fonctionnent souvent comme des boîtes noires où des erreurs de configuration peuvent entraîner des fuites de données. Les solutions émergentes de gestion de la posture de sécurité SaaS (SSPM) permettent une visibilité en temps réel, mais génèrent un volume d'alertes parfois ingérable. Des manuels et, dans certains cas, des partenaires externes sont nécessaires pour gérer cette charge. Le consensus était que la responsabilité est passée de la propriété de l'infrastructure à la supervision des fournisseurs, mais la responsabilité ultime des résultats incombe toujours à l'organisation, et les activités liées à la supervision ne peuvent être négligées.

- **Conformité : SOC 2 et le dilemme de la confiance**

Les cadres de conformité comme SOC 2 sont perçus comme des indicateurs de maturité, mais non comme des preuves de sécurité continue. Les contrôles évaluent un moment précis et n'assurent pas une protection permanente ; plusieurs entreprises certifiées ont tout de même subi des brèches. Les bonnes pratiques évoquées incluent la demande de rapports SOC 2, ISO ou TISAX, l'ajout de clauses de droit d'audit, l'exigence de plans correctifs et l'achèvement des certifications par des outils de surveillance externes fournis par les plateformes de notation de sécurité. Le groupe a convenu que la conformité fournit des aperçus utiles, mais qu'une confiance à plusieurs niveaux et une gouvernance active sont essentielles.

- **Reprise après sinistre : La réalité du SaaS**

Les sauvegardes seules ne peuvent pas garantir la continuité si un fournisseur subit une panne totale, car les clients ne peuvent pas exploiter les applications sans la plateforme elle-même. Certaines organisations effectuent désormais des tests de continuité d'affaires et établissent des procédures manuelles d'urgence. D'autres ont noté que ces plans échouent souvent lorsqu'ils ne sont pas testés. Les participants ont insisté sur la priorisation des systèmes critiques et la reconnaissance du coût de chaque mesure additionnelle ; la DR SaaS doit être vue comme une question de processus, de contrats et de procédures éprouvées, non simplement de copies de données.

FAITS SAILLANTS ET TENDANCES

- **Perspectives sectorielles : Appétit pour l'infonuage**

Le contexte sectoriel influence fortement la stratégie infonuagique. Les services publics et les secteurs à forte composante OT restent naturellement extrêmement réticents au risque, gardant les systèmes opérationnels strictement sur place et autorisant l'utilisation de l'infonuage uniquement pour les outils de productivité de fournisseurs de confiance. Certaines organisations adoptent une position « infonuage d'abord » pour les RH et la collaboration, mais conservent le contrôle sur place pour les systèmes industriels. Nombre d'entre eux exploitent des environnements hybrides, combinant des unités opérationnelles infonuagiques avec des équipes sur place, notamment dans les contextes industriels critiques où la séparation est considérée comme essentielle. Le point commun était clair : l'industrie dicte l'appétit, les secteurs OT étant ancrés sur place tandis que les fonctions d'affaires migrent progressivement vers l'infonuage.

- **L'IA en pratique : Avantages, risques et gouvernance**

L'adoption de l'IA est déjà visible dans de multiples fonctions, notamment pour les agents de conformité aux politiques, les questionnaires de sécurité préremplis, l'intégration des fournisseurs SaaS, les examens des demandes d'extraction, la validation des couvertures d'assurance, la corrélation des alertes et la détection des fraudes. Bien que ces applications offrent des gains d'efficacité notables, les participants ont reconnu la persistance de défis. La mesure du retour sur investissement demeure complexe par rapport aux coûts de licence, tandis qu'une « IA fantôme » non maîtrisée a déclenché des incidents de prévention des pertes de données (DLP) dans certaines organisations. Les dirigeants ont souligné la nécessité d'une éducation culturelle, d'un équilibre entre convivialité et sécurité, et d'encourager une utilisation sécuritaire de l'IA dans les contextes personnels et professionnels. La conclusion commune est que l'IA apporte des avantages tangibles, mais que la gouvernance, le suivi du retour sur investissement et la formation des utilisateurs sont essentiels à une adoption durable et sécurisée.

BONNES PRATIQUES ET STRATÉGIES D'AVENIR

Les tables rondes ont permis de dégager un ensemble de bonnes pratiques et de stratégies prospectives, reflétant à la fois les besoins immédiats et les priorités à long terme. Les participants ont souligné l'importance de renforcer la sécurité des SaaS grâce au déploiement de solutions SSPM et à l'élaboration de manuels clairs pour une gestion efficace des alertes. Pour les petites équipes, le recours à des partenaires externes de Fournisseurs de services de sécurité gérés (MSSP), de Détection et réponse gérées (MDR) ou de Détection et réponse gérées et étendues (MXDR) a été perçu comme un moyen pratique de faire évoluer les capacités sans surcharger le personnel interne. La gouvernance des fournisseurs est également apparue comme un thème récurrent, les dirigeants soulignant l'importance de la standardisation des contrats afin d'inclure des clauses de SLA et de reprise après sinistre, des droits d'audit et le partage obligatoire des rapports pour réduire les ambiguïtés et renforcer la responsabilisation.

La planification de la résilience a été soulignée comme une autre pratique essentielle, exigeant des organisations qu'elles dépassent les politiques théoriques et procèdent plutôt à des exercices manuels, testent régulièrement les flux de travail de sauvegarde et s'assurent que la direction comprend les limites inhérentes à la reprise après sinistre SaaS. Entre-temps, une stratégie robuste de gestion des données critiques a été recommandée, garantissant le stockage redondant des données essentielles à l'entreprise auprès de plusieurs fournisseurs de confiance afin de minimiser l'impact des interruptions de service. L'activation de l'IA a également été abordée, les CISO encourageant l'approbation et le suivi des outils d'IA approuvés, une formation complète des employés sur l'utilisation sécuritaire de l'IA dans les contextes personnels et professionnels, et le suivi des mesures d'adoption pour éclairer les décisions de licence.

À l'avenir, les CISO ont souligné l'importance de mettre en place des mécanismes de confiance fournisseurs à plusieurs niveaux, allant au-delà des certifications de conformité et offrant une vision plus fiable des pratiques de sécurité en vigueur. Ils ont souligné la nécessité de créer des tableaux de bord de retour sur investissement pour les initiatives d'IA afin de justifier les investissements en licences et de maintenir la confiance des organisations dans les nouvelles technologies. La planification de la continuité doit également être institutionnalisée, les manuels et les exercices de résilience étant considérés comme des documents et des exercices évolutifs plutôt que comme des actions ponctuelles. Enfin, les dirigeants ont recommandé d'aligner les stratégies d'adoption de la cybersécurité sur les appétences au risque propres à chaque secteur, tout en considérant l'IA à la fois comme un moteur de productivité et un défi de gouvernance nécessitant une surveillance et une formation constantes.

CONCLUSION

La table ronde des CISO GoSec25 a mis en lumière une réalité qui donne à réfléchir : la technologie déplace les responsabilités, mais pas l'obligation d'en répondre. Qu'il s'agisse d'adoption du SaaS, de cadres de conformité, de planification de la reprise après sinistre ou de gouvernance de l'IA, le poids des conséquences demeure sur les épaules des dirigeants de la sécurité.

Les angles morts, les lacunes en matière de conformité et les défis de gouvernance ne disparaîtront pas. Cependant, en mettant en œuvre les bonnes solutions, en négociant des contrats fournisseurs plus solides, en testant les plans de continuité et en adoptant l'IA de manière responsable, les organisations peuvent réduire l'incertitude et renforcer leur résilience.

La voie à suivre n'est pas d'éliminer complètement les risques, car une élimination complète ne sera jamais possible. Il s'agit plutôt de gérer les risques de manière transparente, de s'assurer que les dirigeants comprennent leurs choix et d'aligner les stratégies de résilience sur les priorités organisationnelles.

ANNEXE

QUESTIONS CLÉS ABORDÉES

1. Sécurité infonuagique et SaaS
L'infonuage renforce-t-il notre sécurité ou modifie-t-il simplement nos angles morts ? Face à l'expansion de l'infonuage dans les entreprises, êtes-vous préoccupé(e) par :

- La gouvernance de la sécurité multinuage (éviter la fragmentation) ?
- L'« IA fantôme » et la prolifération du SaaS : comment redonner de la visibilité ?
- La gouvernance SaaS est-elle le prochain angle mort majeur de la sécurité des entreprises ?

2. IA et cybersécurité
Face à la tendance mondiale à l'adoption de l'IA, comment l'utiliserez-vous pour renforcer votre cybersécurité ?

- Exploitez-vous l'IA pour la détection, la réponse et l'automatisation ?
- Laissez-vous cette responsabilité à vos fournisseurs de services ?
- Voyez-vous les avantages de l'IA de manière mesurable ?
- Avez-vous constaté les risques liés à l'IA générative (fuites de données, hypertrucages, attaques adverses) ?

ORGANISATEUR :
Julien Turcot, vice-président principal des ventes, GoSecure
L'auteur remercie GoSecure et les CISO participants pour leurs contributions sincères à la table ronde.