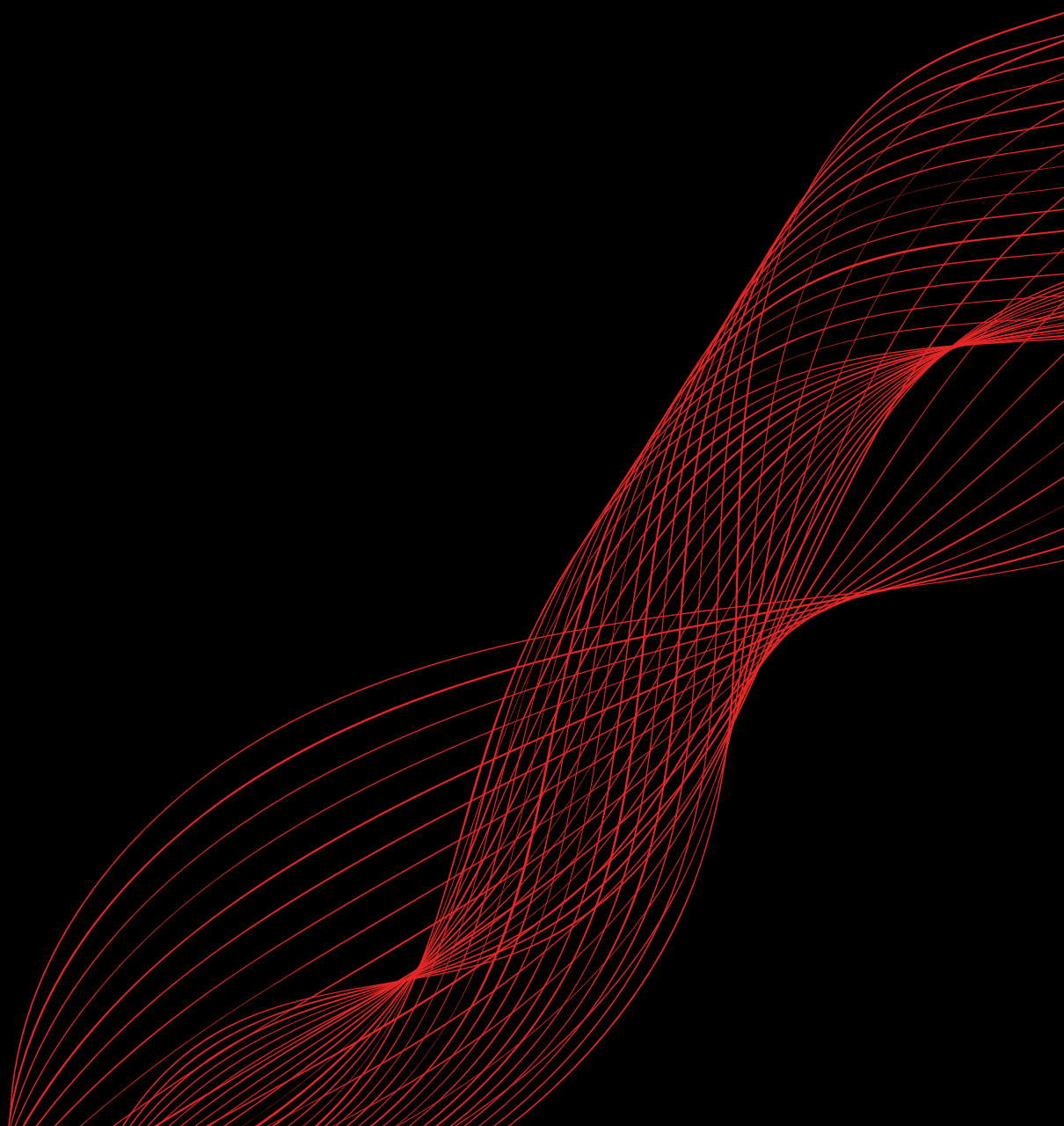
GoSec 23

TABLE RONDE CISO : MUTUALISATION DES RESSOURCES – UN DÉFI ET UNE OPPORTUNITÉ



GoSec 23

Table ronde CISO

Résumé Exécutif

Lors de la récente conférence GoSec 23 à Montréal, Canada, une session cruciale de table ronde a eu lieu, rassemblant 11 CISO distingués et anonymes de divers secteurs à travers le pays. Ce livre blanc se penche sur les défis, stratégies et meilleures pratiques discutés lors de cette session, avec un accent particulier sur la navigation dans le paysage de la cybersécurité avec des contraintes budgétaires dans le contexte économique canadien. S'appuyant sur diverses expériences et perspectives, ce livre blanc vise à fournir des informations complètes pour les professionnels et les organisations dans le domaine de la cybersécurité, soulignant l'approche transformative de la mutualisation.

Introduction

Dans une ère où les menaces cybernétiques sont omniprésentes et en constante évolution, comprendre les défis et stratégies essentiels à une gestion efficace de la cybersécurité est primordial. Une table ronde modérée à Montréal a offert une plateforme aux CISOs de divers secteurs, notamment bancaire, aérospatiale, agriculture et divertissement, pour partager des perspectives candides, des défis et des meilleures pratiques. Cette session d'une heure a eu lieu lors de GoSec à Montréal le 14 septembre 2023, sur place dans une salle de conférence du Crew Collective & Café. Les délibérations étaient orientées par dix questions principales, abordant des aspects allant des contraintes budgétaires, la prise de décision, l'adoption de la technologie, à la mesure de l'efficacité des initiatives de cybersécurité. Les questions clés qui ont contribué à orienter les discussions se trouvent en annexe.

Participants / Contexte des Participants

La table ronde a vu la participation de 11 CISOs anonymes. Les industries représentées comprennent : recherche, fabrication, vente au détail, militaire, organisations à but non lucratif, aérospatiale, agriculture, bancaire et divertissement. Leur expérience en tant que CISOs variait de 2 à 15 ans. La table ronde était une riche combinaison de perspectives, rassemblant des participants de divers horizons et expériences. Ces considérations lors de la planification de la table ronde ont garanti que diverses perceptions et points de vue étaient mis en avant dans la discussion.

GoSec 23

Table ronde CISO

Points Saillants / Tendances de la Discussion

Les discussions ont mis en lumière divers thèmes :

- Défi du talent - La difficulté croissante à attirer de nouveaux talents, notamment avec les pertes en faveur de grandes entreprises renommées et la commercialisation de l'éducation.
- Défi de la portée - La vaste portée de la sécurité peut s'étendre au-delà de la cybersécurité, incorporant des aspects tels que la sécurité physique.
- Problèmes de budgétisation - Des divergences dans les allocations budgétaires, surtout dans le contexte des projets par rapport aux besoins opérationnels.
- Impact de l'état économique - Les récessions économiques entraînent des coupes dans les opérations, indépendamment de leurs performances.
- Défis des nouvelles technologies et réglementations - Adopter de nouvelles technologies introduit de nouveaux points d'extrémité de risque et les cadres réglementaires peuvent entraver la progression des projets.
- Silos organisationnels - La hiérarchie et la structure filière des CISOs varient selon les organisations, conduisant à d'éventuels conflits, angles morts et défis.
- Budgétisation des projets - Les phases initiales des projets voient souvent des budgets conséquents, mais à mesure qu'ils passent à l'exploitation, les fonds diminuent.
- Qualité vs quantité - L'accent mis sur la qualité pourrait conduire à négliger d'autres contrôles de sécurité cruciaux.
- Lacunes de connaissance - L'organisation dans son ensemble manque souvent de compréhension approfondie de la cybersécurité.

Meilleures Pratiques, Recommandations et Stratégies de Cybersécurité pour l'Avenir

Pour les CISO, la voie à suivre exige un leadership audacieux. Comprendre la vaste étendue de la sécurité est essentiel ; il est crucial de reconnaître que son champ d'application ne se limite pas uniquement à la cybersécurité. Il intègre des aspects plus larges, tels que la sécurité physique. De plus, le paysage dynamique des menaces cybernétiques nécessite un apprentissage continu. Les CISO doivent rester à la pointe des menaces émergentes, en exploitant un éventail de sources d'information, pour affiner et ajuster constamment leurs stratégies. Décomposer les silos organisationnels est aussi essentiel. Assurer une structure organisationnelle cohérente et un cadre de rapport pour les CISO atténue non seulement les conflits potentiels mais encourage aussi une meilleure coopération entre les départements. L'avenir exige des efforts actifs de la part des CISO pour briser ces silos et optimiser les coûts grâce à des ressources partagées. Adopter la mutualisation comme effort pour briser les silos nécessite de prendre des risques calculés pour obtenir des avantages à long terme.

GoSec 23

Table ronde CISO

La mutualisation est une approche transformatrice dans le paysage de la cybersécurité. Elle permet aux CIO et aux CISO d'optimiser leur portée, répartissant les budgets sur un plus grand nombre de priorités et de projets. Au-delà des aspects purement financiers, la mutualisation englobe la mise en commun de ressources essentielles, de connaissances et de talents. Il s'agit de la convergence des moyens, compétences et talents, tous dirigés vers des objectifs partagés. Une telle stratégie comble non seulement les lacunes en matière de talents, permettant aux équipes de croître exponentiellement, mais garantit également des avantages financiers, offrant des améliorations de revenus pour les petites équipes et des économies pour les plus grandes.

La pénurie de talents n'est pas un problème nouveau ou limité à l'industrie de la cybersécurité. L'apprentissage continu est essentiel pour aborder ce problème, et son intégration à un cadre de mutualisation amplifie son efficacité. Le partage de ressources permet aux professionnels expérimentés d'élever le niveau de compétence de toute l'équipe. Une telle approche collaborative permet aux équipes d'accéder à des opportunités d'apprentissage qui pourraient être financièrement inaccessibles individuellement ou difficilement budgétisées par les CISO. En abordant le déficit de talents, les organisations devraient privilégier le recrutement interne, complété par des descriptions de poste standardisées, pour retenir et attirer les meilleurs dans le domaine, les éloignant des noms les plus en vue.

L'intégration de nouvelles technologies, surtout dans le domaine de la cybersécurité, est cruciale pour les organisations cherchant à anticiper les menaces potentielles. Grâce à la mutualisation, les équipes peuvent regrouper leurs ressources pour adopter collectivement les outils et solutions de cybersécurité les plus avancés, comme l'IA et l'automatisation, à un rythme accéléré. La rapidité est essentielle, car le potentiel de ces nouvelles technologies peut être utilisé pour contrer les défis croissants de la cybersécurité, surtout lorsque les ressources sont limitées.

La force de la mutualisation réside également dans la réduction des dépenses redondantes, notamment entre les départements similaires. En exploitant ce qui est déjà disponible et en évitant d'empiler constamment des produits ou solutions, les entreprises peuvent s'assurer qu'elles demeurent à la fois protégées et financièrement efficientes. Cela, associé à une formation adéquate pour les décideurs et à une vision synchronisée de la sécurité cybernétique et matérielle, garantit une approche globale et robuste de la cybersécurité.

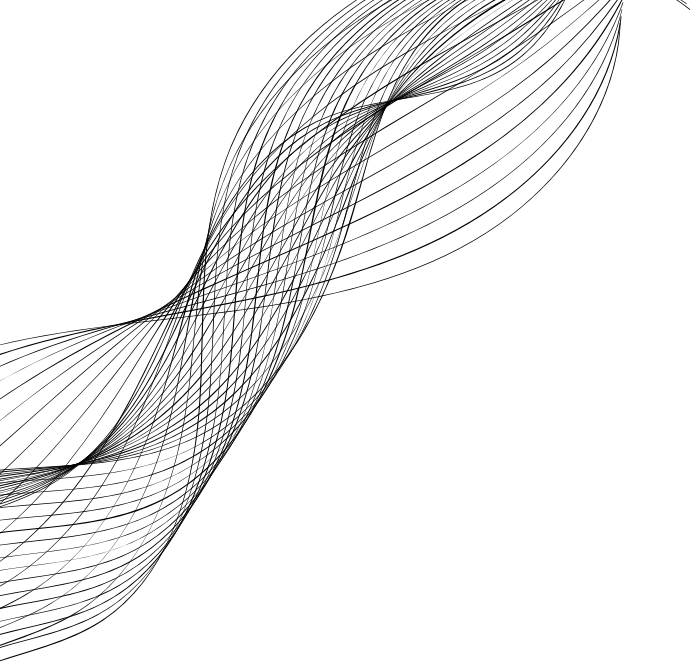
Conclusion

Lors de la table ronde des CISO, il devient évident qu'une approche holistique et intégrée, caractérisée par la mutualisation, qui permet un apprentissage continu et une adoption plus rapide des avancées technologiques, est la voie à suivre vers un avenir plus collaboratif et efficace pour la cybersécurité. À mesure que les menaces évoluent, nos stratégies et pratiques doivent également s'adapter. Ce livre blanc souligne la sagesse collective des vétérans de l'industrie et sert de phare pour les organisations cherchant à renforcer leurs cadres de cybersécurité.

Annexe

Les questions clés qui ont aidé à orienter la discussion étaient :

- Quels sont les principaux défis que vous avez rencontrés en matière de cybersécurité depuis que les contraintes budgétaires sont devenues plus prononcées? Comment avez-vous abordé ces défis?
- Lorsque les budgets sont restreints, comment décidez-vous des priorités en matière de sécurité? Quelles sont les considérations clés qui guident vos choix?
- La consolidation des solutions de cybersécurité peut offrir des avantages en termes d'efficacité et de coûts. Pouvez-vous partager des exemples concrets de la manière dont vous avez réussi à consolider vos solutions tout en maintenant un niveau élevé de protection?
- En situation de contraintes budgétaires, comment parvenez-vous à convaincre la direction de l'importance de l'investissement dans la cybersécurité? Quelles stratégies de communication avez-vous trouvées efficaces?
- La collaboration interne est cruciale pour renforcer la posture de cybersécurité. Comment avez-vous réussi à favoriser une meilleure coopération entre les équipes IT, les départements métier et la direction, malgré les pressions budgétaires?
- Face à des ressources limitées, comment gérez-vous les compromis entre la sécurité et l'innovation? Pouvez-vous partager des exemples où vous avez trouvé un équilibre entre ces deux impératifs?
- Les nouvelles technologies telles que l'IA et l'automatisation peuvent potentiellement aider à relever les défis en matière de cybersécurité. Avez-vous exploré ces solutions pour optimiser la sécurité avec des ressources limitées?
- Comment mesurez-vous l'efficacité de vos initiatives de cybersécurité malgré les contraintes budgétaires? Quels indicateurs ou métriques utilisez-vous pour évaluer la réussite de votre stratégie?
- Dans un environnement de contraintes budgétaires, comment maintenez-vous la veille sur les nouvelles menaces et les évolutions de la cybercriminalité? Quelles sont vos sources d'information et comment ajustez-vous votre stratégie en conséquence?
- Pouvez-vous partager des leçons apprises ou des erreurs à éviter lors de la consolidation des solutions de cybersécurité? Quels sont vos conseils pour d'autres CISO qui font face aux mêmes défis?



Organisateur :

Julien Turcot est le vice-président principal des ventes chez GoSecure et il est basé à Québec.

L’auteur souhaite remercier Cyber Eco et les CISO pour leurs contributions à la table ronde.