5 façons concrètes

pour les RSSI de soutenir la stratégie d'entreprise

splunk> turn data into doing™

Table des matières

5 façons concrètes pour les RSSI de soutenir la stratégie d'entreprise

Plus que jamais, le Responsable de la Sécurité du Système d'Information (RSSI) est tenu d'intervenir dans les décisions du conseil de direction. Dans un paysage économique toujours plus compétitif, l'intuition commerciale devient aussi importante que le savoir-faire technique, et les dirigeants attendent de leur RSSI qu'il aligne les programmes de sécurité sur les objectifs de l'entreprise pour favoriser sa croissance et l'augmentation de ses revenus.

Selon un rapport dirigé par Forrester, les RSSI sont encouragés à aligner la sécurité sur la stratégie de l'entreprise, mais doivent également implémenter des innovations clés et gérer la rareté des compétences. Voici cinq bonnes pratiques pour contribuer à l'entreprise et donner au conseil de direction exactement ce qu'il espère : une star de RSSI !.

01

Comprendre l'évolution du rôle du RSSI

Jusqu'à présent, le rôle des RSSI consistait à diriger la stratégie de sécurité de l'entreprise. Il n'avait pas à se préoccuper des marges de profit et, en cas de faille ou de vulnérabilité, sa mission était de réparer le système, pas les opérations. Mais les temps ont changé et le RSSI est aujourd'hui un rôle métier autant que technique, qui ne se préoccupe plus seulement de mettre en œuvre des mesures de sécurité et des technologies réactives mais intègre désormais l'analyse des coûts et bénéfices et la gestion des risques.

Aujourd'hui, les RSSI doivent créer de la valeur, augmenter les revenus, échanger avec les clients et favoriser une croissance à deux chiffres. On attend d'eux qu'ils accroissent la vélocité de l'activité des fonctions métier (en accélérant la mise sur le marché des produits et des expériences) pour acquérir un avantage compétitif et augmenter les profits, tout en minimisant les risques et les pertes financières – ou pire, les dommages à la réputation – qui les accompagnent.

Enfin, le conseil de direction a besoin d'un RSSI capable d'envisager la sécurité de leur point de vue, de communiquer et gérer la cybersécurité parallèlement à une longue liste de demandes annexes (voir transformation numérique). Selon Forrester, « les directeurs de la sécurité doivent également ajouter la personnalisation, les assistants virtuels, l'edge computing, les services d'API externes et l'automatisation des processus numériques à la liste des technologies maîtrisées par leurs équipes. » Pour résumer, le RSSI doit jouer le rôle de conseiller de confiance sur plusieurs canaux et communiquer efficacement les risques dans des termes intelligibles par l'équipe dirigeante pour qu'elle puisse mettre en œuvre rapidement et en toute sécurité les meilleures décisions pour l'entreprise.

02

Connaître les besoins fonctionnels de votre comité de direction

La cybersécurité appartenait traditionnellement au domaine de l'IT, et était de fait trop technique pour les cadres dirigeants. En contrepartie, les RSSI avaient une maigre connaissance des risques financiers et pouvaient rarement répondre à des questions touchant les revenus de l'entreprise. Mais aujourd'hui, le comité de direction demande aux RSSI de prendre part à ces discussions et d'avoir voix au chapitre. Ils doivent donc comprendre quels sont les moteurs de croissance et comment parler de sécurité dans des termes concrets, pratiques et intelligibles par les autres directeurs.

La plupart des cadres dirigeants n'ont pas de formation technique. Ils ne comprennent pas la différence entre « commande et contrôle » et « déplacement latéral dans le réseau », et peuvent être intimidés par les implications de la cybersécurité, surtout face à des conversations pleines de jargon et des présentations de sécurité formatées.

C'est pour cela que le RSSI doit impérativement trouver un terrain d'entente avec le reste de la direction. Pour cela, il doit comprendre le fond des préoccupations du comité de direction et traduire la valeur de la cybersécurité à l'aide d'indicateurs parlants tels que les gains de temps, les réductions de coûts et les incidents évités. Inutile de s'étendre sur les outils déployés et les applications testées. Les autres directeurs veulent visualiser l'impact que la sécurité exerce sur les activités à proprement parler, et pas seulement au niveau opérationnel.

Enfin, pour mieux hiérarchiser les objectifs de la direction, vous devrez comprendre les flux de revenus entrants et sortants de l'entreprise et les facteurs qui peuvent potentiellement les mettre en danger (par exemple, une interruption du site web pour un grand détaillant). Lorsque vous commencez réfléchir sous cet angle, vous pouvez élaborer des initiatives alignées sur les priorités.

03

Intégrer la sécurité dans votre stratégie métier

Face à un nouveau projet, les RSSI doivent prendre en compte la sécurité dès le départ et la tester tout au long du développement. Intégrer la sécurité dans le processus de développement permet d'établir une relation de confiance avec le client, favorise les ventes et accélère la commercialisation des produits, ce qui accroît les revenus en bout de ligne. L'intégration de la sécurité dans la planification des projets et de l'entreprise contribue également à réduire les risques, en particulier dans les environnements agiles aux cycles de publication courts.

Selon Forrester, **« Les stratégies de sécurité qui ne sont pas alignées se privent de l'opportunité d'intégrer la sécurité dès la conception aux premières étapes du cycle d'innovation, ce qui ralentit l'entreprise dans son effort de disruption à grande échelle. »** La sécurité dès la conception (ou SbD pour Security by Design) adopte une approche holistique et proactive de la sécurité, plutôt qu'une approche rétroactive qui se contente d'appliquer des politiques de sécurité lorsque les incidents se produisent (risquant ainsi des interruptions de service et des pertes financières).

Grâce à la SbD, les professionnels de sécurité peuvent incorporer des exigences de sécurité à toutes les étapes du processus de développement et ainsi bâtir et concevoir l'intégralité de l'infrastructure dans cette optique tout en automatisant les contrôles de sécurité. Avec une telle organisation, les RSSI n'ont plus à être consultés à chaque modification de l'infrastructure, les tâches répétitives et fastidieuses sont réduites et les équipes ont plus de temps à consacrer aux problématiques de haut niveau.

04

Créer une feuille de route stratégique

Les feuilles de route s'avèrent très utiles pour faire de la planification à long terme. Elles offrent un cadre pour prédire et coordonner les développements techniques, en alignant efficacement les initiatives et les solutions de sécurité sur les objectifs à long terme de l'entreprise.

Dans un premier temps, un plan stratégique doit évaluer l'état actuel de la sécurité et définir des objectifs pour les 12 prochains mois, des objectifs à moyen terme sur 18 à 24 mois et, enfin, des visées sur un horizon de 36 mois. Au niveau le plus haut, le programme doit confirmer la mission, la vision et les objectifs de l'entreprise pour permettre au RSSI de cibler ses efforts. Non seulement cela va consolider l'exécution en aval, mais cela va aussi améliorer la gestion des risques et éviter des écueils et retards potentiels dans les technologies.

Une fois que cette vision de haut niveau a été établie, le RSSI peut examiner les questions de sécurité à une échelle plus granulaire, en abordant notamment l'approche des menaces internes et externes, de la confidentialité des données et de l'intégration de la cybersécurité comme bonne pratique dans les opérations quotidiennes.

Il faudra enfin actualiser ces objectifs en continu au fil de l'exécution des projets, et le RSSI devra réévaluer les initiatives en fonction des besoins de l'entreprise et de l'évolution de la pile technologique.

05

Déterminer le rôle des solutions de sécurité

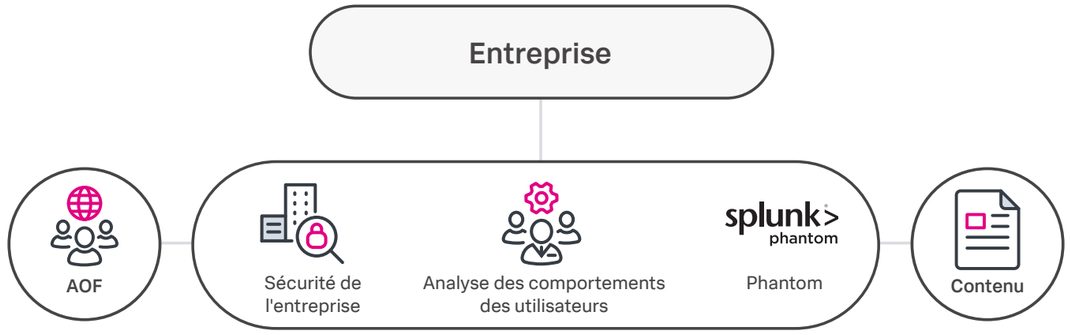
Comment un RSSI peut-il concrètement aligner la sécurité sur les objectifs de son entreprise ? Surtout quand on sait tout toutes les reponsabilités qu'il a déjà ? Il chapeaute toute la hiérarchie de sa fonction jusqu'au conseil de direction, et exerce une mission de gestion qui s'étend à toute l'entreprise en délivrant des solutions, en préservant le statu quo et en donnant de nouveaux outils au personnel si possible. Il est déjà difficile pour le RSSI de tout faire, d'autant plus que les talents sont rares et l'appui, souvent insuffisant. La réalité est simple : il n'y a pas assez de professionnels qualifiés pour analyser le volume d'incidents que la plupart des entreprises reçoivent tous les jours.

Le RSSI a besoin d'une plateforme puissante qui garantit la protection de la sécurité et la réputation de l'entreprise : une solution de sécurité évolutive et englobante. Une solution qui aide les équipes de sécurité et les RSSI à mieux identifier les actifs et données stratégiques de l'entreprise, à abattre les silos, à standardiser les workflows et à produire une image globale des écosystèmes IT et de sécurité. Vous pouvez maintenant automatiser les tâches répétitives pour permettre à votre équipe de sécurité de démultiplier ses efforts, et vous concentrer sur les décisions critiques.

Le secret, c'est SOS : la suite Splunk pour les Opérations de sécurité.

La suite Splunk pour les Opérations de sécurité modernise les opérations de sécurité et réduit l'exposition au risque. Notre suite de sécurité, qui englobe des solutions SIEM, UEBA et SOAR de premier plan, peut renforcer vos cyber-défenses tout en accélérant la gestion des menaces et en facilitant l'expansion de vos opérations de sécurité.

Découvrez comment notre solution de sécurité peut vous aider à renforcer et optimiser vos opérations et notamment la position de sécurité de votre entreprise.



Pour commencer.

Découvrez comment la suite Splunk pour les Opérations de sécurité peut vous aider dans votre parcours de sécurité.

2020-Splunk-SEC-5-Key-Ways-CISOs-Can-Accelerate-the-Business-106-EB

splunk> turn data into doing™