NOTE DE SYNTHÈSE

Mieux se préparer à la cybersécurité : le point de vue des RSSI

Enquête 2024 sur la Sécurité du cloud hybride

Le paysage actuel des cybermenaces, en constante évolution, est redoutable. Avec des dépenses mondiales pour la sécurité de l'information qui devraient atteindre 215 milliards de dollars en 2024, les organisations n'en perdent pas moins du terrain dans la course à l'armement face aux acteurs malveillants. Plus de la moitié (54 %) des responsables IT et sécurité affirment être bien préparés à identifier les menaces dans leur infrastructure de cloud hybride, mais échouent toujours à détecter certaines failles.

Au cours des 12 derniers mois, **plus d'une organisation sur trois (37 %)** n'a pas réussi à détecter une faille à l'aide de ses outils de sécurité existants, contre **31 %** en 2023. Les environnements de cloud hybride, toujours plus complexes, amplifient les risques de cybersécurité en élargissant la surface d'attaque et en générant des problèmes de visibilité. Et à mesure que l'infrastructure de cloud hybride évolue, qu'elle s'adapte pour faciliter les déploiements d'IA, le danger ne fera que croître. **À cette époque charnière pour l'infrastructure IT des entreprises, quelle est la meilleure façon pour les RSSI de combler leur retard en matière de préparation à la cybersécurité ?**

Nous avons interrogé plus de 1 000 professionnels de la sécurité et de l'IT en Australie, en France, en Allemagne, à Singapour, au Royaume-Uni et aux États-Unis pour publier notre rapport 2024 « La sécurité du cloud hybride : mieux se préparer à la cybersécurité ». Vous pouvez consulter le rapport dans son intégralité [ici], mais cette note de synthèse s'intéresse spécifiquement aux points de vue de plus de 230 RSSI dans le monde pour comprendre les principaux enjeux et priorités auxquels cette fonction essentielle dans l'entreprise doit faire face. Voici ce que les conclusions révèlent :

Les réglementations ajoutent de la pression

Alors que la posture de cybersécurité est dans la ligne de mire des législateurs, le rôle du RSSI évolue pour englober la conformité et même le risque juridique. La cybersécurité a donc attiré l'attention des Conseils d'administration

du monde entier, apportant aux RSSI un soutien bien nécessaire. Mais les dirigeants comprennent-ils vraiment ce dont les RSSI ont besoin pour garantir la sécurité ?

Les RSSI sont très conscients des manques en matière de visibilité

Aujourd'hui, près de la moitié **(46 %)** des RSSI ne se sentent pas suffisamment préparés pour identifier les menaces dans leur infrastructure de cloud hybride. Ils se montrent particulièrement préoccupés par le trafic est-ouest et le trafic chiffré, qui permettent aux acteurs malveillants de ne pas être détectés dans l'infrastructure de l'entreprise. Par conséquent, **7 RSSI sur 10** ne pensent pas pouvoir détecter les failles avec leurs outils de sécurité existants.

Les stratégies en matière d'outils sont une préoccupation majeure

La consolidation des outils est toujours une des principales priorités des organisations, l'optimisation et l'investissement dans de nouveaux outils **étant classés respectivement en première et deuxième position** par les RSSI pour l'identification et la correction des manque de visibilité.

Le Zero Trust est désormais un impératif

Longtemps considéré comme important, le Zero Trust est devenu une réalité pour les organisations dans le monde entier, avec les États-Unis en tête. Les RSSI doivent maintenant s'atteler à la mise en œuvre pratique, **44 %** d'entre eux citant la « pression du Conseil d'administration pour atteindre le Zero Trust » comme l'une de leurs trois principales préoccupations.

Définition de l'observabilité avancée : il s'agit de la capacité à fournir efficacement des informations provenant du réseau aux outils de cloud, de sécurité et d'observabilité. Cela permet d'éliminer les angles morts en matière de sécurité, de réduire le coût des outils et d'améliorer ainsi la sécurité et la gestion de l'infrastructure de cloud hybride.

Mobiliser le Conseil d'administration

Alors que les cyberattaques font régulièrement la une des journaux, les dirigeants et les gouvernements du monde entier affirment clairement que les risques de cybersécurité représentent une menace pour l'entreprise. Du règlement DORA de l'UE aux nouvelles règles de la Commission des opérations de bourse (SEC) sur la publication d'informations, les réglementations en matière de responsabilité des risques et de détection des menaces font fermement peser la charge des défaillances de sécurité sur les épaules des dirigeants d'entreprise. Et cela semble fonctionner – **85 %** des RSSI indiquent que la sécurité du cloud est désormais une priorité pour le Conseil d'administration, les dirigeants travaillant avec les RSSI pour identifier et gérer les risques induits par la cybersécurité de leur organisation. À première vue, il s'agit d'une excellente nouvelle pour les RSSI, puisqu'ils sont **6 sur 10** à déclarer être plus valorisés dans leur travail depuis que les cyber-risques sont devenus une véritable priorité pour le Conseil d'administration.

Mais qui dit plus d'attention, dit aussi plus de pression. Interrogés sur leurs principaux problèmes, près de la moitié des RSSI **(44 %)** ont indiqué que la pression exercée par le Conseil d'administration pour atteindre le Zero Trust était l'une de leurs principales préoccupations. Cette pression est vivement ressentie par les RSSI, alors que seulement **29 %** de toutes les personnes interrogées au niveau mondial sont d'accord avec cette affirmation.

Quelles sont vos principales préoccupations ?

CLASSEMENT DU TOP 5 DES RÉPONSES DES RSSI

1. **La pression exercée par le Conseil d'administration pour atteindre une architecture Zero Trust, sans disposer des ressources/compétences nécessaires pour y parvenir**
2. **Disposer d'un trop grand nombre d'outils mal intégrés, ce qui entraîne des failles**
3. **Une nouvelle législation plus précise et plus contraignante en matière de cybersécurité et des obligations de mise en conformité**
4. **Sécuriser la croissance exponentielle des dispositifs IoT/OT**
5. **L'exploitation d'angles morts dont vous ignorez l'existence**

En tant que RSSI aujourd'hui, votre rôle évolue. Vous devez parler au nom de l'entreprise et la protéger contre les répercussions négatives, en particulier en ce qui concerne les risques juridiques et de conformité. En termes de risques, on peut distinguer ceux qui sont acceptables de ceux qui sont inacceptables. Les réglementations gouvernementales poussent les dirigeants à assumer la responsabilité juridique du niveau de risque accepté, ce qui oblige les entreprises à définir précisément leur tolérance au risque. La possibilité d'accepter des risques sans en craindre les conséquences appartient au passé.

CHAIM MAZAL
Directeur de la Sécurité de Gigamon

Les résultats de l'enquête mettent en évidence un éternel dilemme : les RSSI ont besoin que leur Conseil d'administration comprenne et hiérarchise les cyber-risques, mais les réglementations ne suffiront pas à résoudre leurs plus grands défis. Les RSSI d'aujourd'hui sont de plus en plus chargés de gérer les risques économiques et juridiques en plus des besoins techniques, mais ils n'ont tout simplement pas les ressources nécessaires pour préparer et protéger leurs organisations contre la prochaine génération de cybermenaces. Sans soutien technique, la pression exercée par le Conseil d'administration risque d'accroître le stress des RSSI sans pour autant améliorer la posture de sécurité.

Comprendre les risques

Les RSSI interrogés font preuve d'un manque de confiance généralisé dans les capacités de leur organisation à détecter des menaces. Un peu moins de la moitié d'entre eux **(46 %)** ne se sentent que peu ou pas du tout préparés à détecter les menaces dans l'infrastructure de cloud hybride, et **48 %** ont des doutes similaires quant à leur capacité à réagir rapidement en cas d'accès non autorisé au cloud hybride. Bien que les chiffres ne soient pas optimistes, ils suggèrent néanmoins une certaine surestimation des capacités : 1 CISO sur 5 **(20 %)** déclare être en mesure de détecter et d'atténuer les dommages d'une violation en temps réel à l'aide de ses outils de sécurité existants. La migration vers le cloud continuant à s'accélérer – et les déploiements de l'IA promettant encore plus d'investissements dans le cloud – l'amélioration de la visibilité est une priorité absolue pour les RSSI afin qu'ils puissent avoir réellement confiance dans leurs capacités de détection des menaces.

La détection et la prévention des attaques ne sont pas les seuls éléments de la préparation à la sécurité à être mis sur le devant de la scène. Les organisations sont confrontées aux conséquences de leur incapacité à comprendre et à divulguer rapidement l'étendue d'une brèche. C'est un point faible pour de nombreuses organisations. Au cours des 12 derniers mois, plus de la moitié des RSSI **(53 %)** admettent qu'ils n'ont été alertés d'une violation que lorsqu'ils ont appris que les utilisateurs ne pouvaient pas accéder aux applications, et **1 RSSI sur 3** indique ne pas avoir été en mesure de déterminer la cause première de la brèche. Le manque d'information après une violation a de graves conséquences : **39 %** des RSSI citent une demande de rançon comme premier indicateur d'une faille

Comment avez-vous pu détecter la violation de données ?

56 % **Notre équipe IT a détecté la menace à l'aide d'outils de sécurité et d'observabilité**

53 % **Les utilisateurs ne pouvaient pas accéder aux applications et aux ressources numériques**

43 % **Les utilisateurs ont constaté des lenteurs dans l'utilisation des applications**

39 % **Nous avons reçu une demande de rançon de l'attaquant**

36 % **Des informations confidentielles de notre organisation ont été divulguées sur le dark web**

Les personnes interrogées avaient la possibilité de choisir plusieurs réponses.

de sécurité grave, tandis que **36 %** n'ont découvert l'attaque que lorsque des données ont été divulguées sur le dark web.

Le nombre impressionnant d'attaques qui passent sous le radar des équipes de sécurité indique que les acteurs malveillants connaissent et exploitent les angles morts des organisations. C'est aussi ce qu'on a récemment pu lire dans la presse, les agences de renseignement mettant en garde contre une augmentation des attaques de type "Living off the Land" soutenues par des États-nations, dans lesquelles les acteurs de la menace se cachent ou s'installent pendant de longues périodes dans les réseaux pénétrés, se déplaçant latéralement pour collecter des informations et augmenter les dommages de leur attaque éventuelle.

La faible visibilité est-ouest et la dépendance à une surveillance basée sur des historiques d'activité jouent en la faveur de ces pirates. Les logs sont des enregistrements modifiables que les acteurs malveillants peuvent manipuler pour échapper à la détection. De même, les cybercriminels utilisent de plus en plus le chiffrement comme mesure de sécurité – dissimulant les logiciels malveillants, les mouvements et l'exfiltration de données dans le trafic chiffré. Pour venir à bout de ces tactiques, les RSSI doivent s'attaquer à la confiance implicite et disposer d'une visibilité totale sur le trafic est-ouest et le trafic chiffré. À l'heure actuelle, 7 RSSI sur 10 déclarent avoir du mal à obtenir une visibilité sur le trafic chiffré, et pourtant 8 RSSI sur 10 pensent toujours qu'il est sécurisé. Tant que les organisations ne résoudront pas le risque posé par cet angle mort persistant avec des ressources suffisantes, elles ne pourront pas être confiantes dans leur posture de sécurité globale.

Gérer les risques / Les avantages de l'IA

Les outils existants ne semblent pas être à la hauteur, mais les RSSI sont divisés sur la façon d'avancer. **Quatre RSSI sur cinq** décrivent leurs équipes de sécurité comme étant submergées par la multiplication des outils, et la refonte des outils figure en tête des priorités des RSSI pour remédier aux angles morts au cours des 12 prochains mois. Près des deux tiers des RSSI citent la consolidation et l'optimisation des outils comme leur priorité numéro un **(62 %)**, suivie de près par l'investissement dans des outils supplémentaires **(54 %)**. Alors que les personnes interrogées dans leur ensemble placent leurs espoirs dans l'automatisation de la sécurité et l'IA, **54 %** d'entre elles les plaçant en première position, les RSSI sont plus sceptiques. Pour cette catégorie de répondants, l'IA arrive en quatrième position avec **46 %**.

Bien que l'IA ait été désignée par Gartner comme la principale tendance de cybersécurité pour 2024, les personnes les plus proches de la sécurité se concentrent davantage sur la mise en ordre de leurs fondamentaux : remédier aux angles morts, optimiser les outils et se préparer aux réglementations à venir. Les menaces générées par l'IA occupent également une place importante dans leur surveillance des menaces, **83 %** des RSSI s'attendant à ce que la technologie favorise la croissance mondiale des ransomwares. L'avènement de l'IA présente autant de risques que d'opportunités pour les organisations, et il existe une nette disparité entre la façon dont les RSSI et leur dirigeants évaluent son potentiel de réduction des risques. Cela s'explique peut-être par le fait que les RSSI sont bien conscients qu'ils jouent un rôle essentiel dans la sécurisation de tous les déploiements de l'IA, ainsi que dans l'atténuation des violations provoquées par l'IA..

Ceci est révélateur d'une tendance plus large : le rôle du RSSI s'étend pour couvrir plus que la cybersécurité, touchant aux stratégies d'IA, à la sécurité physique et aux décisions générales en matière de technologie de

Pour **85 %** des RSSI, une observabilité avancée de l'infrastructure de cloud hybride est essentielle pour passer à un état d'esprit proactif et prévenir les attaques.

l'information. Et pourtant, alors que le champ d'action de cette fonction déjà très étendue s'élargit, les RSSI ne disposent pas actuellement des outils et du soutien nécessaires pour protéger pleinement leur organisation.

Mieux se préparer

L'insatisfaction des RSSI à l'égard des outils existants est partagée par les Conseils d'administration, qui prônent souvent la consolidation des outils et les offres de plateformes pour réduire les dépenses informatiques. Mais si la consolidation et l'investissement dans de nouveaux outils font partie des priorités des organisations, il semble qu'une stratégie consistant à tout remplacer ne soit pas la voie à suivre, pas plus qu'une consolidation totale derrière un seul fournisseur.

Les organisations devraient plutôt s'assurer que les outils existants fonctionnent efficacement et sont bien intégrés afin d'éliminer les angles morts en matière de sécurité. Cela nécessite une observabilité avancée, alimentée par des données très fiables et la télémétrie du réseau, qui va au-delà des données MELT ("metrics, events, logs, and traces" – métriques, événements, logs et traces). Les RSSI en sont bien conscients, puisque **83 %** d'entre eux reconnaissent que l'observabilité avancée est un élément fondamental de la sécurité du cloud.

Atteindre ce niveau d'observabilité avancée va permettre aux RSSI et à leurs organisations de se préparer aux stratégies IT du futur. Pour réussir, les déploiements d'IA doivent être alimentés par des données très fiables, et **65 %** des RSSI reconnaissent que la visibilité sur toutes les données est la priorité numéro un pour garantir des investissements sécurisés et fructueux en matière d'IA. La complexité de l'infrastructure de cloud hybride ne cessera de croître à mesure que les organisations adopteront, à juste titre, les avantages des nouvelles technologies et feront évoluer leurs opérations. Les RSSI proactifs doivent chercher à employer des technologies d'infrastructure capables de fournir efficacement la télémétrie réseau à leurs outils existants et d'informer les équipes de sécurité en temps réel, en garantissant une observabilité avancée et continue de l'infrastructure de cloud hybride.

À propos de Gigamon

Gigamon® offre un flux d'observabilité avancée qui fournit efficacement des informations provenant du réseau aux outils de cloud, de sécurité et d'observabilité. Cela permet d'éliminer les angles morts de la sécurité et de réduire le coût des outils, vous permettant de mieux sécuriser et gérer votre infrastructure de cloud hybride. Gigamon compte plus de 4 000 clients dans le monde, dont plus de 80 % des entreprises du classement Fortune 100, 9 des 10 plus grands fournisseurs de réseaux mobiles et des centaines de gouvernements et d'établissements d'enseignement dans le monde. Pour en savoir plus, rendez-vous sur gigamon.com.

Téléchargez le rapport dans son intégralité pour découvrir les données de votre pays. gigamon.com/enquete-cloud-securite

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

05.24_01