Gigamon®

Renforcer le rôle des RSSI à l'ère des risques liés à l'IA

LE POINT DE VUE DES RSSI

Enquête 2026 sur la sécurité du cloud hybride

Introduction

L'IA est en train de rapidement transformer la manière dont les organisations fonctionnent, sont mises en concurrence et innovent. À mesure que son adoption s'accélère, les risques augmentent tout aussi vite. Dans de nombreux cas, ils dépassent les capacités à les mesurer, les vérifier et les atténuer.

Pour les RSSI, cela pose un défi de taille. Ils sont responsables de la sécurisation d'environnements plus distribués, plus dynamiques et plus difficiles à observer. Les architectures de cloud hybride, l'usage décentralisé de l'IA et les flux de données chiffrés ont transformé la manière dont les risques se développent et doivent être gérés.

Il ne s'agit pas seulement d'une question technique. C'est aussi une question de visibilité et de preuve.

L'ampleur de ce défi est évidente. Au cours des 12 derniers mois, **83 %** des organisations mondiales ont signalé des incidents de sécurité liés à l'IA. Parmi eux, **41 %** concernaient des attaques externes impliquant l'IA, **30 %** des fuites internes, **30 %** une utilisation non autorisée de l'IA et **33 %** des attaques directes contre des systèmes d'IA ou des modèles de langage (LLM).

Dans le même temps, de nombreux RSSI manquent encore de la visibilité nécessaire pour réagir avec confiance. **Près de la moitié** déclarent qu'il faut plus de temps pour détecter les violations, tandis que **46 %** indiquent que le trafic piloté par l'IA les rend plus difficiles à identifier et à analyser.

Les RSSI sont tenus responsables de risques qu'ils ne peuvent ni cerner pleinement, ni justifier complètement. Dans ce contexte, la visibilité renforce la capacité d'action des RSSI. Elle leur apporte la clarté nécessaire pour agir avec discernement, les éléments probants pour communiquer de façon crédible et la confiance pour diriger avec autorité.

Ce point de vue est basé sur les réponses de **307 RSSI** ayant participé à l'Enquête **2026 sur la sécurité du cloud hybride,** et reflète l'expérience de responsables de la sécurité du monde entier qui sont en première ligne face aux risques liés à l'intelligence artificielle.

Responsabilité sans preuve

L'adoption de l'IA et du cloud hybride a profondément changé la manière dont les données circulent. Les applications couvrent désormais plusieurs environnements. Les workloads se déplacent constamment. Le trafic est chiffré par défaut. Les systèmes interagissent de façons difficiles à retracer avec les approches traditionnelles.

Le manque de visibilité lié à la complexité du cloud est désormais le **principal défi** auquel les RSSI sont confrontés. Ils voient comment les risques se développent dans le trafic Est-Ouest, dans les environnements de cloud hybride et au sein des processus pilotés par l'IA. Ils savent que les modèles de gouvernance, les contrôles de sécurité des données et les compétences spécifiques à l'IA ne suivent pas le rythme auquel ces environnements évoluent.

Mais avoir conscience du problème ne suffit pas à le prouver.

Sans une vue cohérente des données en mouvement, les équipes de sécurité n'ont pas la capacité de vérifier ce qui se passe dans leur environnement. Elles ne peuvent pas détecter de manière fiable les menaces dans le trafic chiffré ou latéral. Elles ne peuvent pas toujours établir clairement la cause première. Et elles ne sont pas en mesure de fournir systématiquement des preuves pour étayer leurs rapports et leurs prises de décision.

Cela crée un déséquilibre structurel. On attend des RSSI qu'ils répondent à des questions cruciales sans toujours disposer des données nécessaires pour le faire en toute confiance.

Les RSSI ont une vision différente des défis à relever, s'intéressant davantage aux faiblesses structurelles et opérationnelles

RSSI	DÉFIS	TOUS LES AUTRES RÉPONDANTS
1	Manque de visibilité dû à la complexité du cloud	2
2	Pénurie d'expertise en sécurité du cloud	3
3	Outils de sécurité disparates	5
4	Complexité liée à l'adoption de l'IA	4
5	Augmentation des attaques basées sur l'IA	1

Un écart de perception qui accentue les risques

Si les RSSI reconnaissent ces limites, l'entreprise dans son ensemble perçoit souvent une réalité différente. **Près de 40 %** des organisations déclarent fonctionner à un niveau intégré de maturité en matière de sécurité de l'IA. **60 %** estiment que leurs cadres de gouvernance des données sont robustes et bien établis. En apparence, cela suggère confiance et contrôle.

Les données sous-jacentes racontent une autre histoire.

Le pourcentage d'organisations ayant subi une violation de données est passé de **47 %** en 2024[1] à **65 %** en 2026. Les menaces internes augmentent. L'IA est désormais impliquée dans la plupart des incidents. Le manque de visibilité persiste dans les environnements hybrides.

Ce décalage entre perception et réalité se creuse.

Près de la moitié des cadres supérieurs interrogés estiment que la cause première des incidents de sécurité peut être identifiée en 72 heures. À l'inverse, seul **environ un quart** (27 %) des RSSI partagent cet avis, près de la moitié indiquant que l'identification prend en réalité jusqu'à sept jours. Les RSSI décrivent une réalité plus lente et plus complexe, **23 %** d'entre eux indiquant même qu'il faut parfois jusqu'à 30 jours pour déterminer la cause première ou rétablir les opérations, contre seulement **8 %** des autres cadres supérieurs.

Les RSSI, qui travaillent directement avec les données d'incident, comprennent le temps et la complexité nécessaires pour retracer l'activité à travers les systèmes. Les autres dirigeants s'appuient souvent sur un reporting synthétique qui ne reflète pas le même niveau de détail. Il en résulte une vision plus optimiste de la performance que ne le justifie la réalité des faits.

Cette divergence a des conséquences. Lorsque les organisations estiment qu'elles se remettent plus rapidement et plus complètement qu'elles ne le font réellement, elles ont davantage tendance à renforcer les approches existantes plutôt qu'à s'attaquer aux causes profondes.

Les défis de visibilité aggravent cette situation. Plus d'**un tiers** des RSSI identifient le trafic Est-Ouest comme la zone de plus grand risque. Chez les autres cadres supérieurs, ce chiffre tombe à **26 %**, ce qui accentue le fossé entre ceux qui sont au plus près des données et ceux qui se fient à des synthèses. Ce trafic reste souvent chiffré et insuffisamment surveillé. C'est aussi là que les attaquants peuvent s'implanter durablement et que les menaces internes peuvent se propager.

Principaux risques de violation dans l'infrastructure

CLASSÉS PAR ORDRE D'IMPORTANCE DES PRÉOCCUPATIONS DES RSSI

1. **Cloud public**
2. **Trafic latéral (Est-Ouest)**
3. **Environnements privés d'IA/LLM**
4. **Trafic chiffré**
5. **Cloud privé / workloads virtualisés et data lakes SaaS**

Le même problème s'applique à l'IA. **Trois RSSI sur quatre** (76 %) affirment qu'une visibilité limitée sur le trafic piloté par l'IA constitue un obstacle majeur, permettant à l'adoption de l'IA de dépasser la capacité de leur organisation à sécuriser les données. À mesure que l'IA s'intègre davantage aux opérations, l'incapacité à observer la manière dont elle interagit avec les données crée une incertitude supplémentaire.

Pourquoi multiplier les outils ne résout pas le problème

Dans l'enquête 2025[2], **près de la moitié** (46 %) des RSSI identifiaient la fragmentation des outils et les défis d'intégration comme leur principale zone de compromis. En réponse, les organisations continuent d'investir dans des technologies de sécurité pour faire face à la hausse des menaces, **9 RSSI sur 10** (93 %) déclarant avoir déployé de nouveaux outils afin d'améliorer la détection et la visibilité au cours de l'année écoulée. Pourtant, les violations ont augmenté de **18 %** d'une année sur l'autre.

Cela reflète un problème plus profond. Les outils de sécurité dépendent de la qualité et de l'exhaustivité des données qu'ils exploitent. Lorsque la télémétrie est fragmentée entre les environnements, lorsque la visibilité sur le trafic chiffré est limitée et lorsque les sources de données manquent de cohérence, même les outils avancés ne peuvent pas produire des résultats fiables.

De nombreuses organisations tombent dans un schéma récurrent. Une faille de sécurité met en évidence une vulnérabilité. De nouveaux outils sont déployés. La visibilité reste toutefois incomplète. Et les mêmes problèmes réapparaissent lors d'incidents ultérieurs.

Briser ce schéma exige un changement de priorité. L'objectif n'est pas d'ajouter davantage d'outils. Il est d'améliorer la visibilité et l'intégrité des données qui les alimentent.

Des enjeux croissants pour les RSSI

À mesure que le risque augmente, la responsabilité augmente elle aussi. Elle devient également plus personnelle.

Plus d'**un RSSI sur quatre** craint de perdre son emploi à la suite d'un incident grave. Cela reflète l'attente croissante selon laquelle les responsables sécurité doivent être capables d'expliquer ce qui s'est passé, pourquoi cela s'est produit et comment éviter que cela ne se reproduise.

La pression réglementaire s'intensifie également. Aux États-Unis, les règles de la SEC relatives à la divulgation des incidents de cybersécurité ont renforcé les attentes quant à la rapidité et à l'exactitude des rapports. En Europe, la directive NIS2 étend la responsabilité aux instances de direction, y compris aux RSSI. Des tendances similaires se dessinent dans toute la région Asie-Pacifique, où les cadres réglementaires mettent l'accent sur le devoir de diligence et la responsabilité au niveau du conseil d'administration.

La cybersécurité est désormais considérée comme un enjeu de gouvernance, et non plus seulement comme un sujet technique.

80 % des RSSI déclarent qu'une gouvernance d'entreprise insuffisante autour de l'utilisation non autorisée de l'IA constitue le principal défi pour sécuriser les données aujourd'hui. Pour répondre à cette préoccupation, **41 %** placent la gouvernance d'entreprise en tête de leurs priorités de sécurité.

Les RSSI sont également confrontés à un ensemble de défis persistants, notamment sécuriser les données dans les environnements de cloud public, combler les manques de compétences liées à l'IA, gérer l'utilisation non autorisée de l'IA, gagner en visibilité sur le trafic Est-Ouest et soutenir des équipes soumises à une pression croissante.

EChacun de ces défis renvoie à un problème commun. Les organisations ne comprennent pas clairement comment les données circulent, comment l'IA est utilisée et où les risques se développent.

Ce dont les RSSI ont réellement besoin pour renforcer leur rôle

Si la responsabilité des RSSI continue d'augmenter, leur capacité d'action doit être renforcée dans la même mesure. Cela signifie qu'ils doivent pouvoir disposer d'une visibilité claire et fiable sur la manière dont les données circulent, dont l'IA est utilisée et dont les risques se développent, ainsi que de l'autorité et des ressources nécessaires pour agir sur la base de ces informations.

Les RSSI identifient trois capacités comme les plus essentielles à leur réussite :

- L'accès à une télémétrie précise issue du réseau
- Une visibilité complète sur toutes les données en mouvement
- Des ressources suffisantes pour faire évoluer les équipes et les opérations

Les RSSI agissent déjà. **Près de la moitié** (47 %) prévoient d'utiliser des outils basés sur l'IA pour épauler leurs équipes et optimiser leurs workflows, tandis que **43 %** renforcent la gouvernance afin de garantir une utilisation sûre et appropriée de l'IA. Dans le même temps, **45 %** accordent la priorité à l'amélioration de la visibilité sur les flux de données générés par l'IA dans les environnements de cloud hybride.

Ensemble, ces priorités vont dans le sens d'une évolution vers l'observabilité avancée.

L'observabilité avancée combine la télémétrie issue du réseau, notamment les métadonnées, les paquets et les flux, avec les données MELT (métriques, événements, logs et traces). Cela permet d'obtenir une vue unifiée des données en mouvement dans les environnements de cloud hybride et fournit le contexte nécessaire pour comprendre comment les systèmes interagissent et comment les risques évoluent. Cela permet également aux RSSI d'aligner leurs décisions en matière de sécurité sur les résultats de l'entreprise, améliorant ainsi la rapidité, la précision et la crédibilité des rapports sur les risques destinés à la direction.

Avec ce niveau de visibilité, les RSSI peuvent aller au-delà d'une vision fragmentée pour acquérir une compréhension plus complète de leur environnement.

Ils peuvent détecter les menaces plus tôt et avec une plus grande précision. Ils peuvent retracer l'activité sur l'ensemble des systèmes afin d'en déterminer la cause première. Ils peuvent vérifier l'efficacité des contrôles et identifier les failles avant qu'elles ne conduisent à des incidents. Et ils peuvent étayer les rapports avec des preuves claires et solides.

Cela transforme le fonctionnement de la sécurité. Les hypothèses sont remplacées par des données observables. Cela permet de fonder les décisions sur des données factuelles plutôt que sur des déductions.

Cela renforce également le rôle de l'IA. Lorsque la visibilité est insuffisante, l'IA peut renforcer les failles et créer un faux sentiment de confiance. Lorsque la visibilité est solide, l'IA peut améliorer la détection, accélérer l'analyse et optimiser la prise de décision.

Dans ce contexte, la capacité d'action des RSSI repose sur la clarté.

Redéfinir le rôle du RSSI

Une meilleure visibilité ne se contente pas d'améliorer les opérations. Elle transforme la manière dont les RSSI conduisent leurs activités.

Sept RSSI sur dix affirment que le manque de compréhension au niveau du conseil d'administration constitue un obstacle majeur à une adoption sécurisée de l'IA. Pour y remédier, l'expertise technique ne suffit pas. Il faut aussi savoir communiquer les risques d'une manière alignée sur les priorités de l'entreprise.

Lorsque les RSSI disposent de données claires et fiables, ils sont mieux à même d'aligner la sécurité sur les objectifs de l'entreprise. Les RSSI soulignent également que l'amélioration du reporting constitue l'étape la plus importante pour renforcer l'alignement avec le conseil d'administration, car elle permet de traduire les risques techniques en impacts business clairs. En expliquant les risques en termes concrets, les RSSI peuvent démontrer la valeur des investissements en sécurité et instaurer un climat de confiance en tant que conseillers stratégiques.

À mesure que l'IA occupe une place de plus en plus centrale dans le fonctionnement des organisations, cette évolution est indispensable. La sécurité doit être intégrée dans le processus décisionnel global de l'entreprise, et non plus considérée comme une fonction distincte.

De la visibilité à la confiance

Le défi auquel sont confrontés les RSSI ne tient pas à un manque d'investissement, mais à un manque de clarté.

Alors que l'IA accentue les risques, les écarts de perception continuent de se creuser et la responsabilité s'accroît. Pourtant, sans méthode cohérente pour observer et vérifier ce qui se passe dans les environnements de cloud hybride, les entreprises restent exposées.

Le progrès ne viendra pas du déploiement de nouveaux outils. Il viendra de la mise en place d'une observabilité avancée, permettant d'obtenir une vue cohérente et complète des données en mouvement dans l'ensemble de leur environnement.

Comment les RSSI peuvent renforcer la relation entre RSSI et conseil d'administration

1. **Améliorer les rapports destinés au conseil d'administration en démontrant l'alignement de la sécurité sur les résultats de l'entreprise**
2. **Veiller à ce que la cybersécurité figure parmi les priorités du conseil d'administration en matière de gestion des risques**
3. **Soutenir les RSSI dans leurs responsabilités et leur obligation de rendre compte en matière de posture de sécurité**
4. **Définir des critères communs de communication et de responsabilité en cas de violation**
5. **Mettre en place des réunions régulières entre le RSSI et le conseil d'administration pour discuter des risques et de la stratégie**

Lorsque les RSSI peuvent voir comment les données circulent, comment les systèmes interagissent et où les risques se développent, ils gagnent plus que de la visibilité. Ils disposent de preuves.

Et avec ces preuves vient la confiance, non seulement pour répondre aux risques, mais aussi pour les expliquer, guider l'entreprise et diriger avec autorité. C'est ce qui permet aux RSSI de répondre aux exigences d'un monde guidé par l'IA.

À propos de Gigamon

Gigamon® protège les réseaux et les données de cloud hybride des organisations les plus complexes au monde. La plateforme Gigamon Deep Observability Pipeline, alimentée par l'IA, offre une visibilité complète sur l'ensemble des données en mouvement en fournissant une télémétrie fiable issue du réseau directement aux outils cloud, de sécurité et d'observabilité. Grâce à des analyses générées par l'IA sur les paquets, les flux et les métadonnées applicatives, les organisations peuvent détecter les menaces dissimulées dans le trafic chiffré et latéral, résoudre les problèmes de performance des réseaux et des applications, et valider leur conformité tout en réduisant les coûts et la complexité. Gigamon est une entreprise de confiance pour plus de 4 000 organisations dans le monde, dont 83 du Fortune 100, de grands opérateurs de réseaux mobiles et des organismes du secteur public à tous les niveaux.

Plus d'informations sur **gigamon.com**.

Téléchargez le rapport sur gigamon.com/enquete-cloud-securite

1 Gigamon, 2024, Enquête sur la Sécurité du cloud hybride : Mieux se préparer à la cybersécurité

2 Gigamon, 2025, Enquête sur la Sécurité du cloud hybride : L'évolution de la sécurité du cloud hybride à l'ère de l'IA

Gigamon®

Siège social mondial
3300 Olcott Street, Santa Clara, CA 95054 États-Unis
+1 (408) 831-4000 | gigamon.com

04.26_01