Gartner

Neuf principales tendances dans le domaine de la cybersécurité à l'horizon 2025

Favoriser la transformation

1 L'IA générative au service des programmes de sécurité des données

2 Gestion collaborative des cyberrisques

3 La gestion des identités des machines

Intégrer la notion de résilience

4 Une transition au service de la cyberrésilience

5 Optimisation des technologies relatives à la cybersécurité

6 Bien-être des RSSI et des équipes de sécurité

Faciliter la transformation et renforcer la résilience

7 Intégrer l'IA de manière tactique

8 Renforcer et développer l'efficacité des programmes axés sur des comportements et une culture sécuritaires

9 Gérer les risques de cybersécurité liés aux tiers

Favoriser la transformation

1 L'IA générative au service des programmes de sécurité des données

Qu'il s'agisse de services tiers, d'applications métiers ou d'architectures sur mesure, le recours à l'IA générative s'intensifie à mesure que les entreprises cherchent à en tirer pleinement parti. Cela dit, les inquiétudes soulevées par le manque d'exactitude des données, les problématiques en matière de confidentialité et de conformité réglementaire constituent des freins majeurs à son déploiement.

2 Gestion collaborative des cyberrisques

À mesure que les experts métiers prennent eux-mêmes l'initiative des investissements technologiques, les modèles traditionnels de gestion centralisée des cyberrisques peinent à suivre, générant des tensions et limitant l'agilité de l'organisation. L'adoption par les entreprises de technologies émergentes, telles que l'IA générative accélère la mutation des environnements de gestion des cyberrisques, en introduisant de nouveaux vecteurs de vulnérabilité.

3 La gestion des identités des machines

La gestion des identités et des accès pour les entités non humaines (telles que les systèmes, applications ou processus automatisés) devient un enjeu stratégique face à l'essor des services cloud, de l'automatisation, du DevOps et de l'IA, qui multiplient l'utilisation d'identifiants machine dans les environnements physiques comme logiciels

Intégrer la notion de résilience

4 Une transition au service de la cyberrésilience

Les responsables de la sécurité et de la gestion des risques délaissent progressivement une approche strictement préventive au profit de la cyberrésilience, qui vise à limiter l'impact des incidents et à renforcer les capacités d'adaptation, en adoptant une posture du type « quand, et non si », en partant du principe que les incidents ne sont pas une éventualité, mais une certitude.

5 Optimisation des technologies relatives à la cybersécurité

Les responsables de la sécurité et de la gestion des risques doivent composer avec de nombreuses sources de tension : les options technologiques en cybersécurité se multiplient, tandis que les plus grands fournisseurs encouragent la consolidation au profit de plateformes plus étendues. Bien que ces plateformes visent à réduire la complexité et à couvrir un éventail plus large de menaces, elles entrent souvent en redondance avec des solutions ponctuelles existantes, ce qui peut générer des pertes d'efficacité et nécessiter le recours à des outils supplémentaires pour pallier certaines insuffisances.

6 Bien-être des RSSI et des équipes de sécurité

L'épuisement professionnel des responsables de la gestion des risques et des équipes de sécurité est une préoccupation majeure dans un secteur confronté à une pénurie de main-d'œuvre qualifiée. Les responsables de la sécurité et de la gestion des risques les plus avisés accordent une attention particulière à la santé mentale : ils donnent la priorité à la gestion de leur propre stress et investissent dans des mesures destinées à améliorer le bien-être de leurs équipes, afin de renforcer leur résilience.

Faciliter la transformation et renforcer la résilience

7 Intégrer l'IA de manière tactique

Les responsables de la gestion des risques ont d'abord été déçus par l'IA, en partie à cause du battage médiatique autour de l'IA générative. Ils se tournent désormais vers des applications plus ciblées et quantifiables. Ces approches plus tactiques permettent aux outils d'IA de s'intégrer plus harmonieusement aux indicateurs et projets existants, facilitant ainsi la démonstration de la valeur réelle des investissements en IA.

8 Renforcer et développer l'efficacité des programmes axés sur des comportements et une culture sécuritaires

Les programmes de gestion des comportements et de la culture de sécurité (Security Behavior and Culture Programs, SBCP) sont désormais au centre des préoccupations des entreprises. Les responsables de la gestion des risques d'entreprise apprécient ces programmes pour leur capacité à renforcer la cybersécurité. Ils marquent un tournant stratégique en faveur d'une intégration plus profonde de la sécurité dans la culture de l'entreprise, tout en promettant une meilleure compréhension et appropriation des risques liés au facteur humain.

9 Gérer les risques de cybersécurité liés aux tiers

La dépendance accrue à l'égard de tiers faisant appel à des outils d'IA générative met en évidence à quel point il est nécessaire de mettre en place des stratégies de gestion des réponses et de reprise après sinistre rigoureuses. Les responsables de la sécurité et de la gestion des risques proactifs se concentrent sur des politiques de suspension ou d'abandon des relations avec les tiers et se concertent avec les partenaires commerciaux pour gérer les risques et guider la mise en œuvre des mesures de contrôle.

Remarque : ces tendances ne sont pas classées par ordre d'importance.

Des connaissances à la fois exploitables et objectives

Donnez à votre entreprise les moyens de réussir. Consultez ces ressources connexes et outils gratuits dédiés aux responsables de la cybersécurité

eBook

Vision de leadership destinée aux responsables de la sécurité et de la gestion des risques

Découvrez les trois principales priorités stratégiques de cette année.

Télécharger maintenant

Des informations pertinentes

Cybersécurité et IA : faciliter la sécurité tout en maîtrisant les risques

L'engouement pour l'IA et ses promesses en matière de cybersécurité sont tempérés par certaines appréhensions et divers risques. Vous trouverez ci-dessous les points sur lesquels vous devez vous concentrer.

En savoir plus

Comment nous vous assistons

Comment Gartner accompagne les RSSI

Découvrez comment nous vous fournissons les analyses, les conseils et les outils nécessaires pour répondre à vos priorités stratégiques décisives.

En savoir plus

Feuille de route

Élaborer une stratégie de cybersécurité résiliente et adaptée aux enjeux de votre organisation

Créer une stratégie en matière de cybersécurité résiliente, évolutive et agile.

En savoir plus

Déjà client ?
Accédez à d'autres ressources sur votre portail client. Se connecter

En savoir plus sur Gartner pour les responsables de la cybersécurité

Suivez-nous sur LinkedIn

Devenez client

Source : Gartner