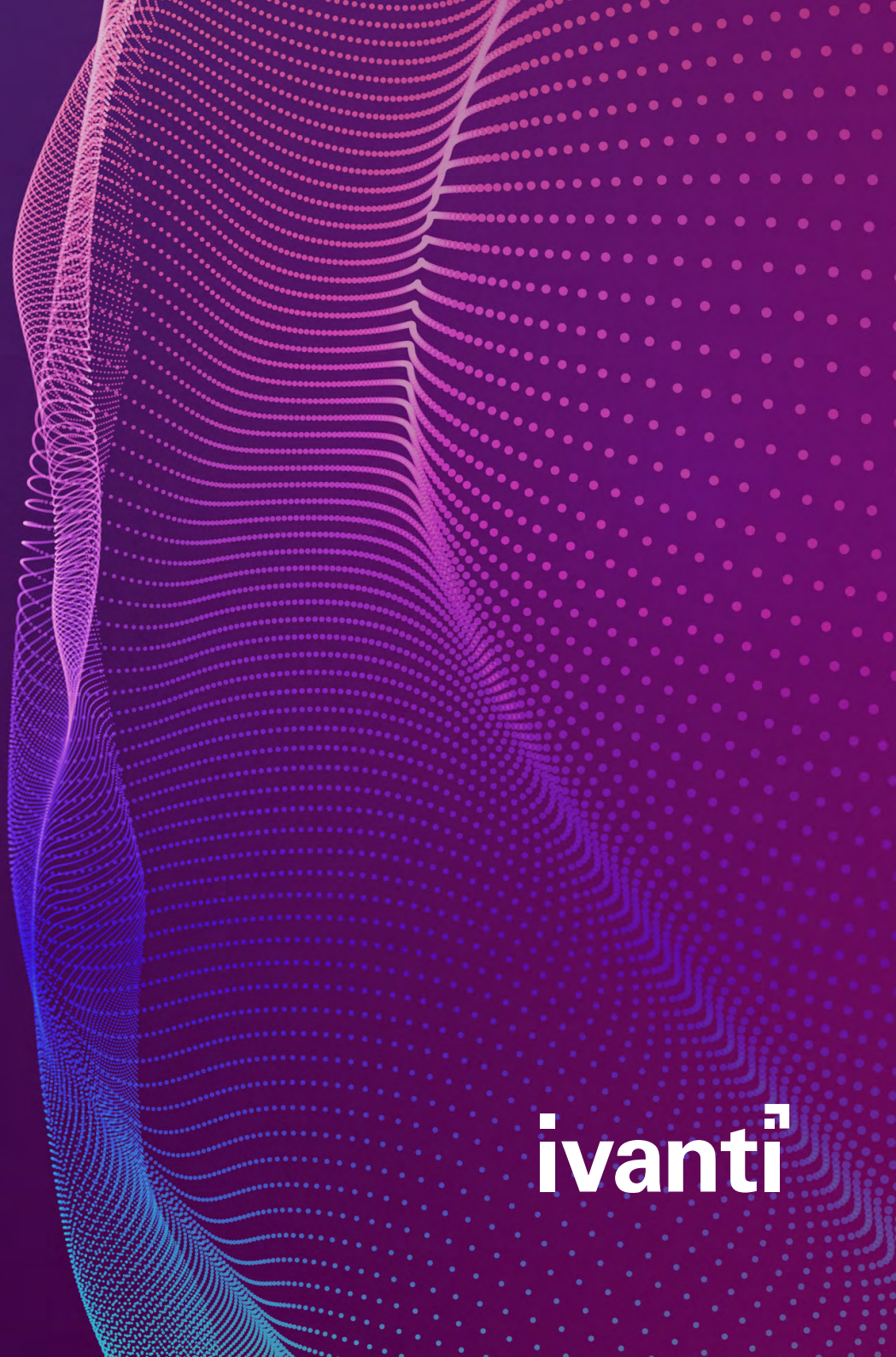
Comment la gestion de l'exposition va transformer la cybersécurité

5 virages stratégiques pour repenser votre approche



ivanti

Le concept de gestion de l'exposition devient une **force de transformation de la cybersécurité.**

À la différence des méthodes conventionnelles qui considèrent souvent le risque de façon isolée, la gestion de l'exposition encourage une compréhension contextuelle des menaces, en les situant par rapport au cadre plus large des objectifs de l'entreprise. Cette évolution dépasse le simple changement de perspective ; il s'agit de totalement réinventer la façon dont les entreprises envisagent la sécurité.

Les menaces auxquelles les entreprises sont confrontées aujourd'hui vont continuer à se multiplier et à se complexifier, imposant une évolution proportionnelle de la manière dont elles appréhendent les cyber-risques. La sécurité ne doit plus être uniquement l'affaire du département IT. Elle doit plutôt être une responsabilité partagée, chaque facette de l'entreprise jouant un rôle dans l'identification, l'atténuation et la gestion des risques. Cette approche collaborative renforce la résilience, tout en stimulant l'innovation et en générant un avantage concurrentiel.

L'émergence continue de la gestion de l'exposition peut fondamentalement transformer le secteur de la cybersécurité et la façon dont cette dernière est perçue dans l'entreprise. Nous sommes convaincus que les 5 prévisions suivantes sont des conséquences non seulement possibles mais probables de cette émergence.

Les **5 virages stratégiques** de la gestion de l'exposition

01

Les entreprises vont obtenir une vision globale des cyber-risques.

02

Le concept de « surface d'attaque » va s'élargir de façon significative.

03

Les entreprises vont passer d'une évaluation subjective des cyber-risques à une évaluation objective.

04

La stratégie de cybersécurité va guider les investissements opérationnels.

05

Les hauts dirigeants vont privilégier une gestion éclairée de la cybersécurité.

01

Les entreprises vont obtenir une vision globale des **cyber-risques.**

Aujourd'hui, la gestion des risques incombe principalement (si ce n'est entièrement) à votre équipe IT. C'est une discipline cloisonnée, sans impact global à l'échelle de l'entreprise.

En outre, elle repose souvent sur des solutions ponctuelles : des produits conçus pour répondre à des menaces spécifiques à mesure qu'elles apparaissent. Vous obtenez ainsi une boucle de rétroaction fragmentée qui ne permet pas d'avoir une vision globale des cyber-risques. Le manque d'interopérabilité entre ces solutions ponctuelles peut créer des failles dans votre couverture de sécurité.

Pour s’écarter de cette méthodologie déficiente, il convient de consolider les données de risque afin d’obtenir une vue contextuelle et complète de vos cyber-risques. Voici quelques étapes pratiques à suivre pour mettre en oeuvre une gestion globale des risques.

Collecte et intégration des données

Créez un inventaire exhaustif des outils et plateformes de cybersécurité utilisés dans l’entreprise, et implémentez une plateforme centralisée pour consolider les données de risque recueillies par tous ces outils.

Évaluation contextuelle des risques

Développez un cadre d’évaluation des risques à l’échelle de l’entreprise pour évaluer l’impact potentiel des risques et les prioriser en conséquence.

Gestion intégrée du risque

Obtenez une vue unifiée de votre posture de risque à l’aide d’une plateforme intégrée de gestion des risques. Grâce à des capacités de surveillance en temps réel et à l’automatisation des workflows, vous optimisez la gestion des risques avec une réponse rationalisée et des actions de remédiation.

Alignement stratégique

Élaborez des rapports exécutifs fournissant une image claire et synthétique de la posture de risque de l’entreprise, tout en facilitant l’intégration de la cybersécurité dans la planification stratégique

En adoptant cette approche, les entreprises obtiennent une vue plus complète et contextuelle des risques de cybersécurité. Il est alors possible d’intégrer les cyber-risques dans les principaux objectifs de l’entreprise. Vous renforcez en retour la résilience globale et créez un avantage compétitif.

La surface d'attaque de votre organisation n'est pas statique, loin de là. Elle évolue rapidement et les paramètres traditionnels qui jadis la définissaient (logiciels et matériel) sont insuffisants pour mettre en place une stratégie de sécurité moderne.

L'interconnexion des technologies utilisées dans l'entreprise contribue à une extension correlative de la surface d'attaque. De nouveaux éléments, comme les environnements Cloud, les fournisseurs tiers et des facteurs humains de plus en plus nombreux, introduisent des vulnérabilités spécifiques, que les entreprises ne peuvent pas se permettre d'ignorer.

Voici quelques-uns des facteurs qui constituent votre surface d'attaque.

Au-delà du matériel et des logiciels

Gardez à l'esprit que la surface d'attaque s'étend au-delà des actifs IT traditionnels. Incluez les environnements Cloud, les périphériques IoT, les fournisseurs tiers, les partenaires de supply chain, les facteurs humains et d'autres éléments critiques.

Sécurité Cloud

Intégrez les données issues des outils CSPM (gestion de la posture de sécurité Cloud) pour surveiller et gérer les risques associés aux services Cloud. Assurez-vous que les environnements Cloud sont contrôlés en continu pour respecter les meilleures pratiques de conformité et de sécurité.

Périphériques IoT

Incorporez les données provenant des solutions de sécurité IoT pour traiter les vulnérabilités spécifiques des périphériques connectés. Implémentez des pratiques solides de surveillance et de gestion pour sécuriser les périphériques IoT et limiter les risques potentiels.

Risques liés aux tiers

Collectez et analysez les données des outils TPRM (gestion des risques liés aux tiers) pour évaluer la posture de sécurité des fournisseurs et des partenaires. Évaluez régulièrement les tiers avec qui vous êtes en relation pour vous assurer qu'ils respectent les normes de sécurité et les exigences de conformité de votre entreprise.

Facteurs humains

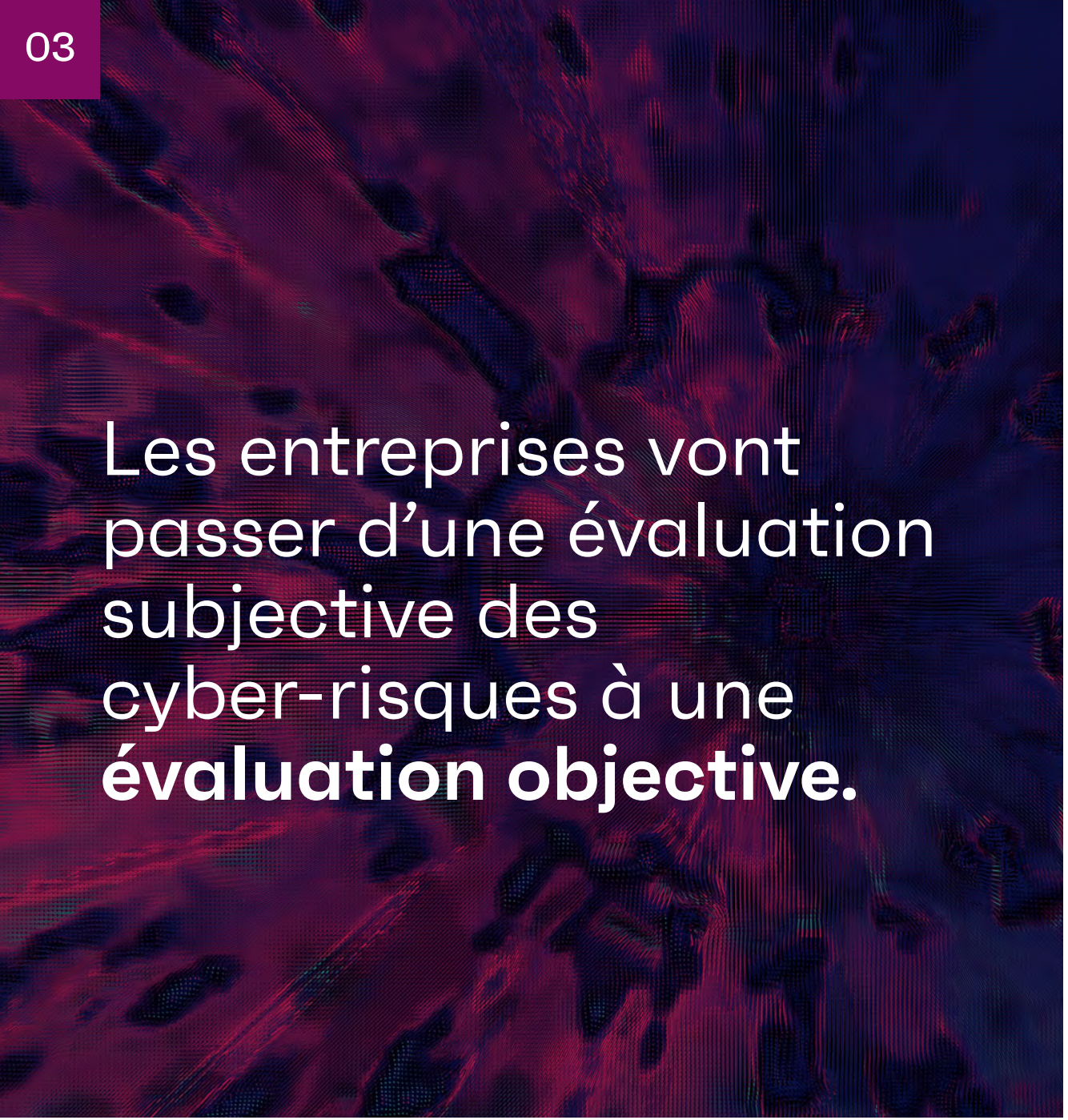
Incluez les données des programmes de sensibilisation à la sécurité et de simulation d'hameçonnage afin de comprendre et de limiter les risques associés aux comportements humains. Développez une culture de sensibilisation aux cyber-risques et renforcez la formation continue pour

Protection contre les risques numériques

Intégrez les données des systèmes de protection contre les risques numériques afin de surveiller les risques sur tous les canaux numériques, y compris les réseaux sociaux, le Dark Web et autres plateformes en ligne. Vous pourrez ainsi identifier et éliminer les menaces comme l'usurpation d'une identité de marque ou les fuites de données.

En étendant leur surface d'attaque à ces domaines, les entreprises obtiennent une image plus complète et contextuelle des risques de cybersécurité et améliorent en retour leur résilience globale.

03



Les entreprises vont passer d’une évaluation subjective des cyber-risques à une **évaluation objective.**

En l’absence de normes universellement acceptées, les métriques utilisées aujourd’hui par les équipes opérationnelles de sécurité ne sont pas prises en compte dans la planification stratégique. Bien que les normes et les cadres de sécurité fournissent des lignes directrices, ils se concentrent souvent sur ce qu’il faut faire, plutôt que sur la façon de le faire.

La gestion de l’exposition va obliger les entreprises à être plus rigoureuses dans la mesure des informations décisionnelles, tout en rationalisant les résultats présentés aux dirigeants : des informations actionables et objectives pourront guider les entreprises vers la posture de sécurité idoine.

Voici les étapes à suivre pour y parvenir.

Analyser la valeur de chaque actif

Pour gérer efficacement les risques associés à vos actifs, commencez par bien comprendre la valeur de chaque actif. Dans le cadre de cette analyse, utilisez les informations (données internes, goût du risque, vulnérabilités particulières) propres à votre entreprise,

Évaluer la probabilité des risques

Évaluez ensuite la fréquence et la gravité des risques afin de créer des scénarios pertinents pour votre entreprise. Ils permettront de mieux comprendre la probabilité et l'impact potentiel des différents événements de risque.

Catégoriser les risques d'après leur impact

Catégorisez les actifs en fonction de leur profil de risque, à l'aide de méthodologies quantitatives comme les scores VaR (Valeur à risque) et CVaR (Valeur à risque conditionnelle).

L'évolution continue du Machine Learning va contribuer à cette transition. Les entreprises bénéficieront ainsi d'évaluations de risques précises et en temps réel facilitant la prise de décision.

04

Actuellement, la cybersécurité est principalement gérée par des spécialistes techniques, qui ont souvent du mal à communiquer efficacement leurs besoins au ComEx. Toutefois, bien que les dirigeants soient parfaitement conscients des enjeux de la cybersécurité et des risques encourus en les ignorant, ils ne disposent pas d'outils leur permettant de combler cet écart de connaissance.

Cette déconnexion explique les difficultés à définir ce qui constitue une stratégie ou un budget de cybersécurité « correct » et « raisonnable ». Par conséquent, les décisions sont rarement prises de façon éclairée mais sont plutôt dictées par des craintes ou par la volonté de suivre les tendances du secteur. Il en résulte un mauvais alignement des priorités, une allocation inefficace des ressources et un manque de responsabilisation. Même si elles pensent prendre les bonnes mesures pour se protéger, les entreprises ont peu de chances d'y parvenir.

Pour relever ces défis, les entreprises doivent adopter une approche stratégique de la cybersécurité intégrant les priorités opérationnelles et les données de performances. Voilà comment :

Des décisions basées sur les données

Collectez et analysez en permanence les données de performances afin de déterminer les activités qui donnent les résultats les plus significatifs et celles pour lesquelles le retour sur investissement est insuffisant.

Supervision complète

Les hauts dirigeants doivent superviser une boucle rétroactive de prise de décision et de retours. Il s'agit de s'assurer que les projets de sécurité s'alignent sur les objectifs généraux, pour in fine ajuster les investissements.

Une culture centrée sur la sécurité

Envisagez la sécurité comme une valeur ajoutée, plutôt que comme un centre de coûts. Cette évolution culturelle permettra des investissements plus judicieux et de meilleurs résultats.

Meilleure communication

Mettez en place des canaux de communication clairs entre les spécialistes en cybersécurité et les hauts dirigeants. Cela peut inclure des réunions d'information régulières, des ateliers et des sessions de formation pour combler l'écart de connaissances.

Métriques de performances

Développez et suivez des KPI (Indicateurs clés de performances) qui mesurent l'efficacité des mesures de cybersécurité. Vous obtiendrez une image plus claire de ce qui constitue un budget de cybersécurité « correct » et « raisonnable ».

En implémentant ces stratégies, les entreprises peuvent prendre des décisions plus pertinentes sur leurs investissements de cybersécurité, pour les aligner sur les objectifs de l'entreprise et obtenir de meilleurs résultats.

05

Les hauts dirigeants vont privilégier une **gestion éclairée de la cybersécurité.**

En l'absence de métriques partagées et interprétables, le risque de cybersécurité ne peut pas être correctement expliqué aux dirigeants décisionnaires. Ces derniers doivent deviner la stratégie de sécurité de l'entreprise, sans pouvoir en mesurer objectivement les résultats.

Il n'existe aujourd'hui aucun processus fiable pour fournir l'objectivité nécessaire et un canal direct vers des décisions basées sur les données. Intégrer la cybersécurité dans la stratégie d'entreprise s'avère donc difficile, voire impossible, ce qui freine ou empêche toute initiative d'évaluation de la posture de risque de l'entreprise.

La gestion de l'exposition va permettre aux hauts dirigeants de développer des compétences essentielles pour prendre des décisions éclairées, cohérentes et explicables de gestion des cyber-risques. Dotés de données robustes et d'outils d'analyse avancée, les dirigeants pourront évaluer les risques en termes business, en améliorant la communication et la collaboration dans toute l'entreprise.

Cela nécessite non seulement de nouvelles capacités de la part des fournisseurs de solutions, mais aussi un changement de culture d'entreprise et une volonté de repenser les processus de prise de décision. Voici des conseils sur la façon d'y parvenir :

Établir un cadre pour évaluer le goût du risque

Définissez la tolérance aux risques de l'entreprise et alignez-la sur les objectifs business. Ce cadre guidera la prise de décision et garantira la cohérence des pratiques.

Implémenter des analyses avancées

Exploitez les informations basées sur les données pour identifier les tendances, prévoir les menaces et mesurer l'efficacité des contrôles de sécurité avec une vision globale du paysage des risques.

Communiquer les risques en termes business

Traduisez les risques techniques en impact business pour impliquer les parties prenantes, et encourager une prise de décision éclairée avec un vocabulaire commun et des métriques interprétables sur les risques.

Renforcer la collaboration entre départements

Éliminez les silos et encouragez la collaboration entre les équipes Sécurité, IT et métiers, en organisant des réunions et des ateliers réguliers pour aligner leurs efforts.

Revoir et ajuster régulièrement

Faites de la prise de décision informée un processus continu. Passez régulièrement en revue les risques, les contrôles et les hypothèses pour les adapter à l'évolution du paysage des menaces.

La gestion de l'exposition évolue et transforme en profondeur le marché de la cybersécurité.

Les dirigeants s'investissent davantage dans la cybersécurité. Fortes de ce soutien stratégique vertical, les équipes de sécurité sont en mesure de répondre rapidement et de manière optimale aux menaces émergentes. Par ailleurs, une répartition plus efficace des ressources et une meilleure visibilité au plus haut niveau des entreprises permettent de placer la gestion des risques au cœur des priorités et d'en tirer tous les bénéfices.

Véritable moteur stratégique, la cybersécurité soutient les objectifs généraux de l'entreprise grâce à un meilleur alignement et à une adhésion renforcée aux enjeux de sécurité. À mesure que cet engagement se diffuse à tous les niveaux de l'entreprise, le changement culturel qui en découle renforce la posture de sécurité globale en influençant le comportement de chaque collaborateur. Grâce aux retours en temps réel d'une base d'utilisateurs informés et sensibilisés aux enjeux de sécurité, l'entreprise est plus réactive face aux menaces.

Enfin, la gestion de l'exposition marque le passage du subjectif à l'objectif, en réduisant la dépendance aux jugements qualitatifs par l'accès à des données quantifiables. Les décisions sont désormais fondées sur des données concrètes et reposent sur des facteurs de risque mesurables. Cette compréhension claire et empirique des risques majeurs permet aux entreprises de réagir plus efficacement, en donnant la priorité au traitement des vulnérabilités les plus critiques.

Il s'agit d'une transformation radicale de la cybersécurité, qui devient un domaine concret et un objectif stratégique pour l'entreprise. La gestion de l'exposition sera le moteur de cette transformation, à court terme et dans les années à venir.

ivanti

Pour en savoir plus ou pour contacter Ivanti, visitez le site www.ivanti.fr