ivanti

Introduction aux métriques de gestion de l’exposition

La gestion de l’exposition transforme en profondeur la façon dont les organisations appréhendent les cyber-risques. La capacité à mesurer le risque se trouve au cœur de cette mutation. Ce guide propose un ensemble de métriques qui aideront les organisations dans leur gestion de l’exposition.

En s’appuyant sur ces métriques, les équipes Sécurité pourront améliorer l’efficacité et l’efficience de leurs opérations grâce à une meilleure priorisation des risques. Elles seront également mieux armées pour quantifier les risques et les communiquer au ComEx, au conseil d’administration et aux autres parties prenantes impliquées dans la gestion de l’exposition.

Métriques opérationnelles

Les équipes Sécurité utilisent ces métriques pour guider les activités quotidiennes de gestion de l'exposition.

Visibilité de la surface d'attaque	
Description	La visibilité des cyberactifs constitue la base de la gestion de l'exposition. Les trois types de cyberactifs suivants sont généralement présents au sein des organisations : ■ Les connus connus : les cyberactifs identifiés comme faisant partie de votre surface d'attaque et qui sont formellement pris en compte, d'une façon ou d'une autre. ■ Les inconnus connus : les cyberactifs identifiés comme faisant partie de votre surface d'attaque, mais sur lesquels vous n'avez aucune visibilité. ■ Les inconnus non connus : les cyberactifs dont vous ne savez pas s'ils font ou non partie de votre surface d'attaque. Une métrique de visibilité de la surface d'attaque mesure la proportion d'exposition effectivement surveillée. En l'analysant, les équipes Sécurité identifient les angles morts à combler pour renforcer la protection contre les cyberattaques exploitant ces lacunes. L'objectif, bien que probablement inatteignable, est une visibilité à 100 %.
Comment calculer cette métrique	Divisez le nombre approximatif de cyberactifs sur lesquels vous avez une bonne visibilité (grâce aux produits ou plateformes d'évaluation de l'exposition que vous utilisez) par le total approximatif d'actifs « connus connus » et « inconnus connus » de votre environnement, puis multipliez par 100 pour obtenir un pourcentage.

Notez que les actifs « inconnus non connus » ne sont pas pris en compte dans le calcul de la visibilité de la surface d'attaque, car ils empêchent de mesurer cette métrique. Toutefois, ils ne doivent pas être ignorés. Traitez les « inconnus non connus » comme des « connus connus » et utilisez la checklist Surface d'attaque d'Ivanti pour vous rapprocher d'une visibilité à 100 % de la surface d'attaque.

Actifs gérés	
Description	Après avoir calculé la visibilité de la surface d'attaque, vous pouvez aller plus loin en calculant les actifs gérés. Cette métrique est utilisée pour déterminer le pourcentage de périphériques activement gérés à l'aide d'un outil UEM (Gestion unifiée des terminaux) qui permet aux administrateurs IT de contrôler les paramètres des périphériques et les stratégies de sécurité. Dans le cadre de la gestion de l'exposition, les « actifs gérés » sont ceux qui génèrent des données d'exposition pour votre équipe Sécurité. Rappelez-vous : la visibilité des actifs n'est que la première étape et on a besoin de données d'exposition pour calculer les risques.
Comment calculer cette métrique	Divisez le nombre d'actifs pour lesquels vous collectez des données d'exposition par le nombre d'actifs visibles (en utilisant la métrique « visibilité de la surface d'attaque » comme vu précédemment), puis multipliez par 100 pour obtenir un pourcentage.

Utilisez la checklist Préparation à la gestion de l'exposition d'Ivanti afin d'identifier les technologies à intégrer à votre pile de cybersécurité pour gérer 100 % de vos actifs.

Score de risque de l'exposition	
Description	Une fois que vous avez une bonne visibilité sur vos cyberactifs et les expositions, vous pouvez commencer à attribuer des scores de risque à ces dernières. Ils permettent à l'équipe Sécurité d'identifier les menaces les plus susceptibles d'affecter l'organisation et de les prioriser pour une remédiation rapide. Cela aide également à déterminer quelles menaces nécessitent l'attention du ComEx, du conseil d'administration et des autres parties prenantes impliquées dans la gestion de l'exposition.
Comment calculer cette métrique	Les produits et plateformes d'évaluation de l'exposition automatisent le processus de calcul du score de risque des vulnérabilités, des erreurs de configuration, des lacunes des contrôles de sécurité et autres expositions. Ils tiennent compte pour cela de divers facteurs : ■ La gravité (ex. : score CVSS et/ou score fournisseur) ■ L'exploitabilité (ex. : intelligence des vulnérabilités et/ou EPSS) ■ L'impact potentiel (ex. : contexte des actifs et/ou impact business) Les scores de risque complets constituent l'une des particularités de la gestion des expositions par rapport à la gestion traditionnelle des vulnérabilités (qui tient uniquement compte de la gravité) ou à la gestion des vulnérabilités basée sur les risques (qui intègre le contexte des menaces, mais pas l'impact business).

Métriques décisionnelles

Ces métriques permettent au ComEx, au conseil d'administration et aux autres parties prenantes de prendre des décisions éclairées en matière de gestion de l'exposition.

Niveau de cyber-risque	
Description	Le niveau de cyber-risque est tout simplement un score numérique qui indique la posture de cybersécurité de l'organisation. Ce score, associé à l'appétence au risque de l'organisation (le niveau de cyber-risque qu'elle est prête à accepter pour atteindre ses objectifs), aide les dirigeants à prendre des décisions éclairées en matière de gestion de l'exposition.
Comment calculer cette métrique	Les produits et plateformes d'évaluation de l'exposition quantifient le niveau de risque de l'organisation en attribuant un score de risque à chaque actif de l'organisation. Ils tiennent compte pour cela de divers facteurs : ▪ Le score de risque des expositions associées à l'actif (voir ci-dessus). ▪ L'accessibilité de l'actif (la facilité avec laquelle on y accède, en externe ou en interne). ▪ La criticité de l'actif (son importance pour l'organisation évaluée en fonction de l'impact d'une perte ou d'une compromission). Les scores de risque des actifs peuvent ensuite être regroupés pour permettre la prise de décision au niveau de l'organisation, d'une unité commerciale ou encore d'une région. Les plages de scores de risque et leur signification varient d'un fournisseur de solution à l'autre, mais la plupart utilisent une échelle de 0 à 100. Les valeurs les plus faibles correspondent à un risque élevé et à une posture de sécurité plus faible, tandis que les valeurs les plus élevées indiquent un risque plus faible et une posture de sécurité renforcée.

Avant de présenter vos résultats aux parties prenantes, utilisez notre diaporama Gestion de l'exposition pour leur expliquer des concepts clés tels que la posture de risque et l'appétence au risque.

Niveau de cyber-risque projeté	
Description	Le niveau de risque actuel de l'organisation n'est qu'un élément du processus décisionnel. Il est tout aussi crucial de projeter les effets d'une décision sur le niveau de risque. ■ Si votre niveau de cyber-risque est inférieur à votre appétence au risque, et que vous envisagez une remédiation pour ramener ce niveau dans les limites de votre appétence au risque (ou vous en rapprocher), cette action pourrait s'avérer particulièrement judicieuse. ■ De la même manière, la remédiation peut être envisagée lorsqu'une exposition non traitée pourrait entraîner un niveau de risque inférieur à l'appétence au risque de l'organisation. ■ Si vous estimez qu'une exposition n'impactera pas les risques, que ce soit en positif ou en négatif, vous pouvez généralement l'accepter et l'évaluer à nouveau ultérieurement. Les métriques de calcul du niveau de cyber-risque aident à analyser la situation d'une organisation et à décider des actions à mener. Pour les décisions importantes, il est toutefois nécessaire de s'appuyer sur des analyses plus poussées comme la perte annuelle estimée (qui sera abordée plus loin).
Comment calculer cette métrique	La projection de l'évolution du niveau de risque en fonction des remédiations recommandées est une fonctionnalité avancée présente dans certains outils et plateformes d'évaluation de l'exposition. Ces projections estiment l'impact des mesures correctives sur les facteurs qui déterminent le niveau actuel de cyber-risque de l'organisation, comme expliqué précédemment.

La perte annuelle estimée (ALE)	
Description	Pour être compris des dirigeants, il est nécessaire de parler leur langage. C'est ce que permet la perte anuelle estimée (ALE) : elle quantifie le risque que représente une exposition en termes financiers.
Comment calculer cette métrique	L'ALE est calculée en multipliant les variables suivantes : ■ La perte simple estimée (SLE, Single loss expectancy). C'est une mesure utilisée pour estimer l'impact d'une cyberattaque sur l'organisation. Elle évalue la valeur monétaire d'un incident en multipliant la valeur de l'actif en danger par le pourcentage de perte qu'une menace pourrait entraîner pour cet actif. ■ Le taux d'occurrence annualisé (ARO). C'est une mesure de probabilité qui estime la fréquence à laquelle la menace risque de se produire sur une période d'un an. En comparant l'ALE actuelle avec l'ALE résiduelle (ALE estimée en cas d'atténuation ou de remédiation d'un risque), les dirigeants peuvent comparer les coûts et les avantages, afin de décider si l'organisation doit traiter le risque ou l'accepter. Bien entendu, comme pour la plupart des décisions en matière de gestion de l'exposition, il faut tenir compte de l'appétence au risque de l'organisation.

Consultez notre eBook Évaluer objectivement le cyber-risque : vers une évaluation des risques axée sur les données dans lequel vous trouverez des instructions pas à pas sur l'utilisation de l'ALE et d'autres métriques pour orienter les décisions de gestion de l'exposition dans votre organisation. Vous pouvez utiliser les diapositives de notre Modèle de rapport d'évaluation des risques pour présenter vos conclusions aux différentes parties prenantes.

Métriques de performances

Ces métriques attestent des résultats des activités de gestion de l'exposition. Face à l'impact positif démontré par ces métriques, l'organisation est plus encline à soutenir vos activités de gestion de l'exposition et à investir dans ce domaine.

Dette de résolution des menaces	
Description	Les équipes Sécurité sont rarement reconnues pour leur travail proactif visant à protéger l'organisation. Elles reçoivent trop souvent des commentaires négatifs, en particulier lorsqu'un incident de sécurité se produit. La gestion de l'exposition peut faire évoluer la situation en impliquant davantage les acteurs business de l'organisation dans les décisions de cybersécurité. Néanmoins, leur participation se limite souvent aux décisions les plus critiques, comme déterminer si une vulnérabilité très médiatisée nécessite une remédiation ou s'il faut investir dans des solutions de sécurité. En réalisant un rapport sur la dette de résolution des menaces, l'équipe Sécurité valorise les efforts engagés dans la gestion de l'exposition. Les métriques de calcul de la dette de résolution des menaces reflètent surtout les actions réalisées. Or, ce qui compte vraiment en matière de gestion de l'exposition, ce sont les résultats concrets. Même si ces métriques montrent l'effort fourni par l'équipe, l'essentiel reste l'impact réel de ce travail.
Comment calculer cette métrique	Les produits et plateformes de gestion de l'exposition fournissent généralement des données que vous pouvez utiliser pour calculer les métriques de dette de résolution des menaces. Il est généralement possible d'appliquer des filtres à ces données pour cibler des informations spécifiques. Par exemple : ■ 9 423 instances de malwares supprimées au 2e trimestre. ■ 399 vulnérabilités liées aux ransomwares éliminées au 1er trimestre. ■ Réduction de 40 % du nombre de vulnérabilités critiques le trimestre dernier.

Évolution du niveau de cyber-risque	
Description	Les niveaux de cyber-risque actuels et projetés permettent de prendre des décisions à court terme pour la remédiation d'une exposition. Toutefois, il est important de suivre l'évolution de ces risques sur le long terme pour évaluer l'impact des décisions prises. Les équipes Sécurité démontrent l'efficacité de leur travail par leur capacité à maintenir le niveau de risque de l'organisation dans les limites de son appétence au risque, voire à l'améliorer si nécessaire. En réexaminant régulièrement les niveaux de cyber-risque actuels et projetés avec les parties prenantes, vous évitez les mauvaises surprises au moment de rendre compte des éventuelles évolutions. Vos rapports sur l'évolution du niveau de cyber-risque deviennent ainsi une occasion de montrer que la gestion de l'exposition fonctionne comme prévu.
Comment calculer cette métrique	L'évolution du niveau de cyber-risque peut être calculée de différentes façons : ■ Changement absolu : différence arithmétique exacte entre les niveaux de cyber-risque à deux dates différentes. Par exemple, si le niveau est de 72 le 1er janvier et de 83 le 31 décembre, le changement est de +11 sur l'année civile. ■ Points de pourcentage : différence en pourcentage entre les niveaux de cyber-risque à deux dates différentes. Dans l'exemple ci-dessus, le changement serait de 15,3 % pour un niveau de risque mesuré sur une échelle de 0 à 100. ■ Courbes : évolution du niveau de cyber-risque entre différentes dates et tendances éventuelles, comme une hausse ou une baisse du risque. Certains produits et plateformes d'évaluation de l'exposition présentent automatiquement ces données sous forme de tableaux de bord.

Retour sur l'investissement de sécurité (ROSI)	
Description	Pour être compris des dirigeants, il est nécessaire de parler leur langage. À ce titre, le retour sur investissement (ROI) est certainement l'un des indicateurs qui intéressent le plus les dirigeants. L'équivalent pour l'équipe Sécurité est le ROSI (Retour sur l'investissement de sécurité). C'est sans doute l'un des outils les plus efficaces pour rendre compte de la gestion de l'exposition. En traduisant en termes financiers les efforts de gestion de l'exposition, l'équipe Sécurité peut démontrer la valeur générée par chaque investissement, ainsi que de la valeur cumulée de tous les efforts de gestion de l'exposition sur une période donnée.
Comment calculer cette métrique	Contrairement au ROI, qui compare les gains financiers d'un investissement à son coût, le ROSI s'intéresse aux pertes financières projetées qui ont été évitées grâce à un investissement en les comparant au coût de ce dernier. Ces pertes projetées peuvent être évaluées assez précisément en combinant les données historiques de l'organisation et une étude du secteur. Pour calculer le ROI, on soustrait le coût d'un investissement de sa valeur actuelle, on divise ensuite par le coût et on multiplie par 100 pour obtenir un pourcentage. En modifiant cette équation (en remplaçant par exemple la valeur actuelle de l'investissement par la valeur des pertes projetées qu'il a permis d'éviter), l'organisation peut calculer le retour sur l'investissement de sécurité (ROSI) et mesurer l'impact financier des investissements en matière de gestion de l'exposition.

À propos d'Ivanti

Ivanti est un éditeur de logiciels d'entreprise qui propose une plateforme IT et Sécurité complète basée dans le Cloud. Ivanti fournit des solutions logicielles qui évoluent avec les besoins de ses clients, afin de permettre aux équipes IT et Sécurité d'améliorer l'efficacité opérationnelle tout en réduisant les coûts et en limitant proactivement les risques de sécurité. La plateforme Ivanti Neurons est native du Cloud. Elle est conçue comme base pour des services et outils unifiés et réutilisables, qui assurent la cohérence en matière de visibilité, d'évolutivité et de distribution sécurisée des solutions. Plus de 34 000 clients, dont 85 des entreprises Fortune 100, ont choisi Ivanti pour relever leurs défis grâce à ses solutions de bout en bout. Chez Ivanti, nous nous efforçons de créer un environnement où tous les points de vue sont écoutés, respectés et valorisés. Nous nous engageons aussi pour un avenir plus durable pour nos clients, nos partenaires, nos collaborateurs et la planète. Pour en savoir plus, visitez le site ivanti.com/fr et suivez-nous sur Twitter (@GoIvanti).

ivanti

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