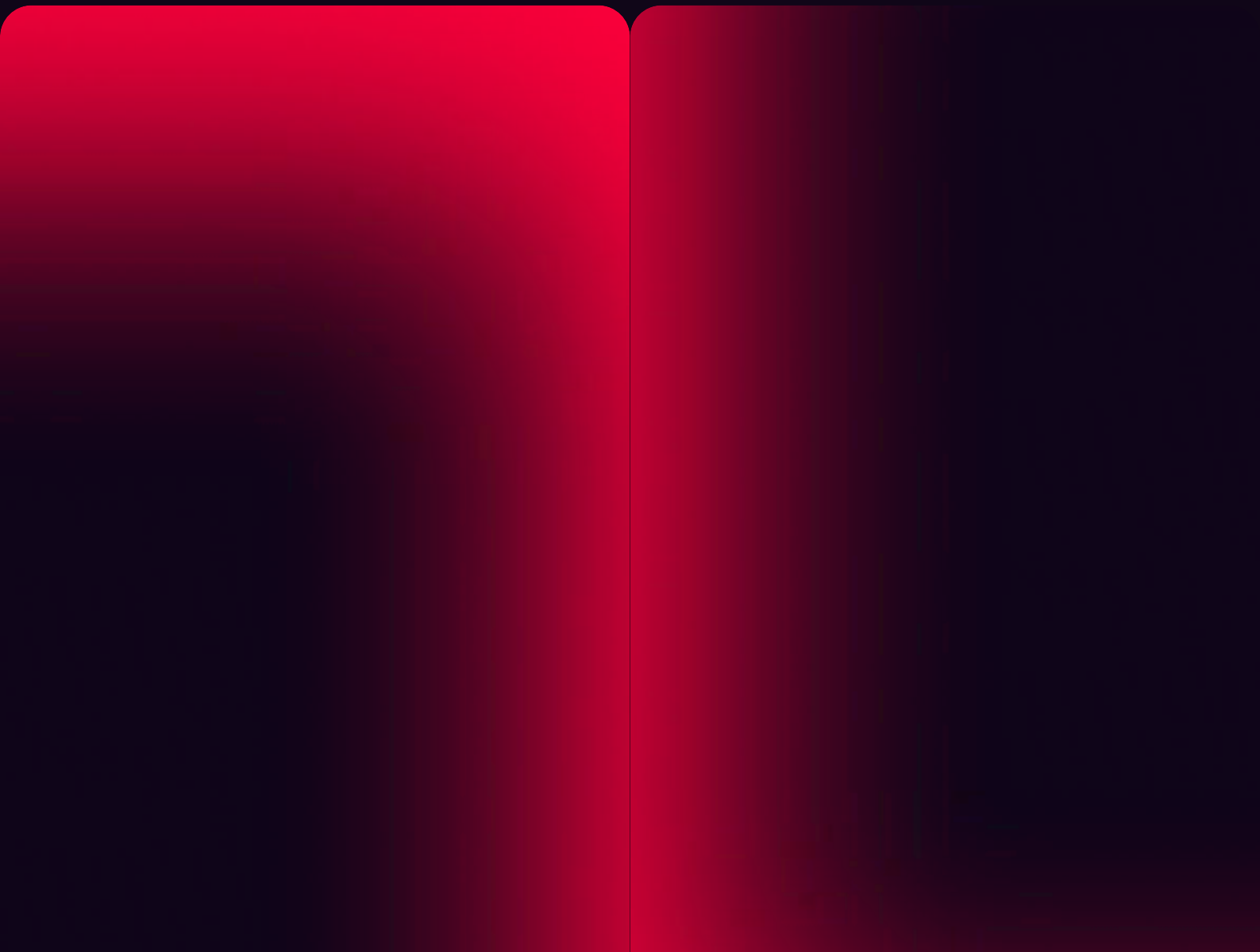
HADRIAN

GUIDE

Au-delà du ROI : Le vrai prix de la prévention des pertes



Un meilleur indicateur pour la cybersécurité offensive

Vous surveillez en permanence le retour sur investissement (ROI) de vos outils. Mais lorsqu'il s'agit de cybersécurité offensive, la meilleure façon de prouver sa valeur est de la comparer au coût d'une violation de données. Le ROI, bien qu'il reste utile dans certains contextes, ne reflète pas toute la réalité. Ce guide vous montrera comment utiliser une nouvelle équation pour déterminer la valeur de vos outils de cybersécurité offensive.

Coût des violations de données

COÛT TOTAL MOYEN D'UNE VIOLATION.

4,88 MILLIONS DE DOLLARS AMÉRICAINS

CROISSANCE MOYENNE ANNUELLE DU COÛT DES VIOLATIONS DE DONNÉES.

10 % ET EN HAUSSE

ÉCONOMIES RÉALISÉES GRÂCE À L'UTILISATION INTENSIVE DE L'IA DANS LA PRÉVENTION.

2,2 MILLIONS DE DOLLARS AMÉRICAINS

Source: IBM Cost of a Data Breach Report, 2024

La valeur de la prévention des pertes

Alors que les coûts substantiels associés à une violation de données sont tangibles, la valeur de la prévention proactive peut sembler abstraite, ce qui complique la présentation d'un argument financier clair en faveur des investissements dans la sécurité. Les mesures traditionnelles du retour sur investissement, bien qu'efficaces dans de nombreux domaines d'activité, ne sont pas adaptées à la cybersécurité, car elles ne permettent pas de quantifier avec précision l'impact des incidents évités. Dans ce cas, **la valeur de la prévention des pertes (Value of Loss Avoidance, VLA)** offre une solution supérieure en quantifiant directement l'investissement dans la réduction des risques par rapport aux pertes financières potentielles liées aux incidents cybernétiques, fournissant ainsi une méthode claire pour démontrer comment les dépenses en matière de sécurité protègent activement les entreprises contre les violations importantes.

La VLA est une simple itération du ROI où vous échangez le bénéfice net contre les pertes évitées.

Simple, n'est-ce pas ? Pas si vite.

Pour obtenir un calcul plus précis basé sur des données et non sur des moyennes ou des spéculations, il existe un tableau pratique qui peut vous aider à déterminer plus précisément l'ampleur des coûts.

Échelle de probabilité d'exploitation

L'échelle de probabilité d'exploitation (Likelihood of Exploitation Scale, LES) permet d'évaluer la probabilité qu'une vulnérabilité donnée soit exploitée avec succès. Cette échelle, qui va de 0 à 10, fournit un cadre clair pour comprendre l'urgence et l'impact potentiel de diverses vulnérabilités.

Probabilité élevée (8 – 3)

Les vulnérabilités de cette catégorie sont très susceptibles d'être exploitées. Les attaquants ciblent généralement les failles accessibles à distance, les faiblesses des technologies largement déployées et les problèmes nécessitant un effort minimal pour être compromis.

Probabilité élevée (8 – 3)

Les vulnérabilités de cette catégorie sont très susceptibles d'être exploitées. Les attaquants ciblent généralement les failles accessibles à distance, les faiblesses des technologies largement déployées et les problèmes nécessitant un effort minimal pour être compromis.

Probabilité modérée (3 – 1)

Les vulnérabilités de cette catégorie ont une chance raisonnable d'être exploitées, mais dépendent généralement de conditions supplémentaires. Les attaquants peuvent exploiter des failles qui nécessitent l'interaction de l'utilisateur, un positionnement réseau spécifique ou des configurations inhabituelles pour réussir.

Probabilité faible (1 – 0,2)

Ces vulnérabilités sont peu susceptibles d'être exploitées sans effort significatif. L'exploitation nécessite généralement des chaînes d'attaques complexes, des connaissances spécialisées ou un accès privilégié, ce qui limite leur attrait pour les attaquants.

Probabilité très faible (0,2 – 0)

Les vulnérabilités de cette catégorie sont rarement exploitées en raison de mesures d'atténuation efficaces, d'une visibilité minimale ou d'exigences d'attaque très spécifiques. Les attaquants ignorent généralement les failles des systèmes isolés, des environnements hérités avec des contrôles d'accès stricts ou ceux qui nécessitent des conditions très spécifiques pour être compromis.

Calculer la perte atténuée en fonction des expositions identifiées

Lorsqu'on estime les pertes atténuées, il est super important de prendre en compte la probabilité d'exploitation pendant la période d'investissement. Pour calculer précisément la perte atténuée pour chaque niveau de gravité d'exposition, on commence par mettre en correspondance le nombre d'expositions identifiées avec une hypothèse d'impact de violation. C'est le coût financier estimé d'une violation à ce niveau de gravité. Ensuite, le LES est utilisé pour quantifier la probabilité d'exploitation réussie pour chaque niveau de gravité de l'exposition. Le LES représente la probabilité qu'une exposition soit exploitée au cours d'une période définie. Ce calcul permet d'obtenir la perte atténuée par exposition. La perte par exposition peut être calculée en fonction du coût moyen des éléments suivants :

- Coûts de récupération des données
- Frais juridiques
- Amendes pour non-conformité et infractions réglementaires
- Coût de l'interruption des activités
- Enquêtes judiciaires
- Augmentation des primes d'assurance

Cela permet de transformer des probabilités abstraites en chiffres financiers quantifiables. Par exemple, en prenant un échantillon d'expositions identifiées, le calcul se présenterait comme suit :

COTE D'EXPOSITION	LES	PERTE PAR EXPOSITION
Critique	3	146 400 $
Élevée	1	34 160 $
Moyenne	0,5	4 880 $
Faible	0,1	195 $

Différences selon les secteurs

Malheureusement, toutes les cyberattaques ne se valent pas et certains secteurs sont davantage ciblés par les cybercriminels que d'autres en raison de leurs marges élevées, de la valeur de leurs données ou de la confidentialité de leur propriété intellectuelle.

Quelles que soient leurs raisons, certains secteurs doivent être prêts à multiplier leur nombre total d'expositions afin de tenir compte des pressions accrues auxquelles ils sont confrontés. Vous pouvez utiliser ce tableau à titre de référence :

SECTEUR	Multiplicateur d'exposition
INDUSTRIE MANUFACTURIÈRE	x7 nombre total d'expositions
FINANCE	x7 nombre total d'expositions
SANTÉ	x5 nombre total d'expositions
GOUVERNEMENT	x4 nombre total d'expositions
ÉNERGIE	x3 nombre total d'expositions
COMMERCE DE DÉTAIL	x2 nombre total d'expositions
AUTRES	Pas de multiplicateur

Calculer la VLA

En gardant à l'esprit que les expositions se produisent rarement de manière isolée et que de nombreuses expositions se produisent souvent en même temps que d'autres, vos coûts peuvent rapidement s'accumuler. Dans un cas prudent, si vous avez 3 expositions critiques, 5 expositions élevées, 8 expositions moyennes et 12 expositions faibles avec les mêmes scores LES indiqués ci-dessus, vous arrivez rapidement à un coût de violation de données de 636 380 $.

Revenons à notre équation de la valeur de la prévention des pertes :
VLA = Perte totale évitée - Coût de l'investissement dans l'outil

Et si nous intégrons également nos hypothèses avec un coût moyen de 70 000 dollars pour un outil de sécurité proactif.

La VLA dans cette estimation s'élève à plus d'un demi-million de dollars. La perte causée par la violation dépasse largement le coût de l'outil qui aurait pu empêcher la violation en premier lieu.

Apportez des économies financières mesurables à votre conseil d'administration

La Valeur de la prévention des pertes (VLA) permet aux équipes de sécurité de justifier efficacement leurs demandes budgétaires en quantifiant l'impact financier potentiel des risques atténués. Cette approche démontre comment les investissements stratégiques dans les outils de sécurité permettent de prévenir de manière proactive les incidents coûteux, en traduisant les risques de sécurité abstraits en indicateurs financiers clairs qui trouvent un écho direct auprès des dirigeants et des membres du conseil d'administration.

Contrairement aux indicateurs traditionnels, tels que le nombre d'incidents évités ou le pourcentage d'expositions atténuées, qui ne parviennent souvent pas à transmettre leur importance financière aux dirigeants d'entreprise, la VLA met l'accent sur des résultats financiers mesurables. Cela illustre précisément comment les investissements dans la cybersécurité améliorent directement les résultats financiers d'une organisation.