



COMMENT METTRE EN PLACE UNE GESTION DES VULNÉRABILITÉS BASÉE SUR LE RISQUE

En 2019, la National Vulnerability Database américaine a enregistré 17 313 nouvelles vulnérabilités, contre 6 447 en 2016.¹

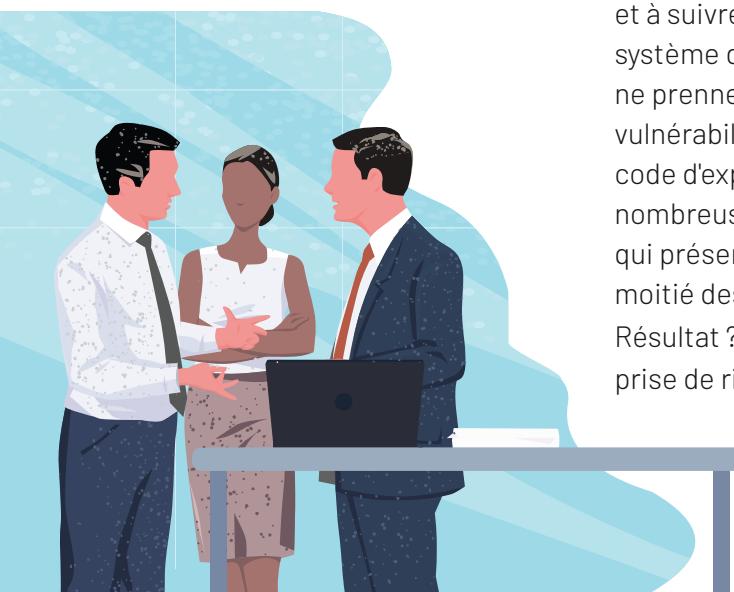


Plus de vulnérabilités = plus de risques

Quelle que soit la taille de votre entreprise, le nombre de vulnérabilités auxquelles elle est exposée quotidiennement augmente de façon exponentielle. En effet, ces trois dernières années, le nombre de vulnérabilités publiées chaque année a presque triplé.

L'explication est simple : avec la transformation digitale qui entraîne une augmentation du nombre et des types d'appareils, de technologies et d'assets tels que le cloud, l'OT et les conteneurs, la surface de cyber-attaque ne cesse de croître. Plus de surface = plus de risques. Dans le même temps, la sévérité des vulnérabilités augmente et les cyber-criminels utilisent des méthodes de plus en plus sophistiquées.

Les équipes de sécurité ont du mal à garder une longueur d'avance et à suivre la cadence. Les approches traditionnelles axées sur le système d'évaluation CVSS (Common Vulnerability Scoring System) ne prennent pas en compte les risques. En fait, pour 76 % des vulnérabilités ayant un score CVSS de 7 ou plus, il n'existe pas de code d'exploit. Parce qu'elles se basent sur l'évaluation CVSS, de nombreuses entreprises perdent du temps à traiter des vulnérabilités qui présentent peu ou pas de risques. Pendant ce temps, près de la moitié des vulnérabilités dangereuses restent dans l'environnement. Résultat ? Une perte de temps, des opportunités manquées et une prise de risque inutile pour l'entreprise.



Pour 76 % des vulnérabilités ayant un score CVSS de 7 ou plus, il n'existe pas de code d'exploit.¹

La puissance du contexte pour mieux évaluer les menaces

Bonne nouvelle : la [gestion des vulnérabilités basée sur le risque](#) offre une meilleure approche pour protéger l'entreprise en s'appuyant sur des modèles de risques générés par l'apprentissage automatique. Les vulnérabilités sont alors évaluées dans le contexte du risque pour l'entreprise. De ce fait, au lieu d'agir en réaction à l'événement, les équipes de sécurité peuvent devenir proactives et se concentrer sur les vulnérabilités qui présentent le plus grand risque dans l'immédiat.

Alors que les méthodes traditionnelles mettent l'accent sur deux étapes uniquement, l'identification et l'évaluation des vulnérabilités, une [approche basée sur le risque](#) va plus loin. Elle vous offre un moyen exhaustif et efficace de réduire le risque pour l'entreprise.

Pour profiter des avantages de la gestion des vulnérabilités basée sur le risque, vous aurez besoin de solutions modernes, capables de fournir une visibilité complète, des évaluations continues et une approche stratégique plus proactive. De plus, les processus traditionnels doivent être étendus pour inclure également trois fonctions supplémentaires : priorisation, remédiation et mesure.



Étape 1 : Tout découvrir Identifiez et cartographiez chaque asset.

La gestion des vulnérabilités commence toujours par un scan de toute votre surface d'attaque pour identifier les points d'exposition.

Vous ne pouvez pas évaluer ce que vous ne pouvez pas voir

Les solutions traditionnelles ne peuvent scanner que l'IT traditionnel, qui se compose d'assets sur site, dont les ordinateurs de bureau, l'infrastructure réseau et les serveurs. Ces solutions n'offrent qu'une visibilité partielle. Le paysage IT actuel est complexe et en constante évolution. Les entreprises utilisent désormais des assets virtuels et cloud, des applications personnalisées, l'IoT et la technologie opérationnelle (OT) connectée. Il est donc essentiel qu'elles aient aussi une visibilité sur ces aspects dynamiques de la surface d'attaque.

La découverte doit également être en continu. De nombreuses entreprises suivent un calendrier de scans périodiques, souvent déterminés par des audits de conformité. Mais des scans cloisonnés et ponctuels offrent une visibilité limitée sur les assets et problèmes potentiels. Le réseau d'entreprise est en constante évolution. Vous ne pouvez donc plus vous contenter de scanner occasionnellement les vulnérabilités. C'est comme si vous aviez une caméra de surveillance qui prendrait une photo une fois par jour au lieu d'une caméra de vidéosurveillance fonctionnant 24 h/24.

En pratique, pour obtenir une visibilité totale, vous devez remplacer votre ancien scanner par un qui soit capable d'identifier et de cartographier tous les assets sur l'ensemble du spectre d'attaque. Vous avez besoin d'une solution dynamique et complète, qui scanne tout, de l'infrastructure réseau aux conteneurs, et qui offre une visibilité continue sur tout l'écosystème. La découverte en temps réel est vitale dans la gestion des vulnérabilités.



Étape 2 : Évaluer en contexte

Soyez informé de l'état de chaque asset.

Pour que votre évaluation ait un impact, vous avez besoin d'une solution capable d'évaluer les vulnérabilités dans le contexte de votre entreprise ainsi que dans un paysage de menaces plus large.

Une évaluation qui va encore plus loin

Bien que le système CVSS soit le principal outil d'évaluation des menaces de vulnérabilité depuis plus d'une décennie, il est loin d'être parfait. Pourquoi ? Parce que les scores CVSS de base sont statiques. Un score de严重性 est attribué une fois à chaque nouvelle vulnérabilité, généralement dans les deux semaines suivant sa découverte. Le plus souvent, ce score n'est jamais mis à jour. Avec l'évolution du paysage des menaces actuel, il devient rapidement obsolète.

En outre, les entreprises qui s'appuient exclusivement sur les scores CVSS pour décider sur quelles vulnérabilités concentrer leurs efforts ne prennent pas du tout en compte le contexte, comme les informations sur les menaces et les exploits, l'activité actuelle des attaquants et l'importance de l'asset concerné pour l'entreprise.

L'une des méthodes les plus couramment utilisées consiste à prioriser toute vulnérabilité dont le score est supérieur ou égal à 7. Mais comme cela concerne 56 % des vulnérabilités, les équipes sont rapidement dépassées par le volume à traiter. Une grande entreprise peut avoir des dizaines de millions de vulnérabilités. C'est donc tout bonnement impossible de suivre le rythme.

De plus, si les menaces ne sont pas mises en contexte, votre équipe peut perdre du temps sur des vulnérabilités qui n'ont pas d'importance et passer à côté de celles qui devraient faire l'objet d'une attention immédiate. Vous avez besoin d'une solution qui évalue constamment tout le contexte de chaque vulnérabilité et actualise son score de risque en conséquence.

Commencez par évaluer le potentiel d'exploitation

Toutes les vulnérabilités ne se valent pas. En fait, la plupart d'entre elles ne sont jamais exploitées et ne présentent donc pas de risque pour votre entreprise. Seules 20 % de toutes les vulnérabilités ont un exploit disponible, ce qui signifie qu'une preuve de concept a été écrite et publiée. Cependant, beaucoup d'entre elles sont écrites par des chercheurs « white hat » à la demande de leurs employeurs, et le pourcentage de vulnérabilités qui sont réellement exploitées dans le cadre d'une cyber-attaque est faible. Seules 24 % des vulnérabilités ayant un score CVSS supérieur ou égal à 7 ont un exploit disponible et peu d'entre elles sont exploitées en environnement réel².

²Source : Tenable Research

Déterminez la probabilité qu'un exploit se produise

L'analyse de l'activité des attaquants dans un paysage de menaces plus large fournit des informations précieuses sur les vulnérabilités susceptibles d'être exploitées dans un avenir proche. Une approche basée sur le risque met les vulnérabilités en contexte en tenant compte de celles qui sont les plus susceptibles d'être exploitées. Si les attaquants ne ciblent pas de vulnérabilités spécifiques à un moment donné, vous pouvez alors concentrer vos ressources sur le risque le plus important.

Considérez ensuite l'impact pour l'entreprise

Chaque asset IT joue un rôle unique dans votre entreprise. Plus l'asset est important pour vos opérations, plus ce sera problématique pour vous si celui-ci présente des vulnérabilités. Plus un asset est vital pour une entreprise, plus le risque est grand s'il est compromis, même si la vulnérabilité elle-même n'a pas un score élevé. Si une attaque cible les services et systèmes essentiels (qui varient selon l'entreprise et le secteur d'activité), l'impact sera plus grand pour l'entreprise.

Même une vulnérabilité avec un score plus faible peut représenter un risque élevé pour l'entreprise si elle est présente sur un asset critique. Par exemple, une vulnérabilité qui obtient un score de 5 et qui figure dans la base de données financière d'une entreprise peut être considérée comme plus critique qu'une vulnérabilité de niveau 10 se trouvant sur un asset moins important, tel qu'un serveur web. Ce n'est que lorsque vous possédez toutes les données contextuelles que vous pouvez prendre une décision éclairée.

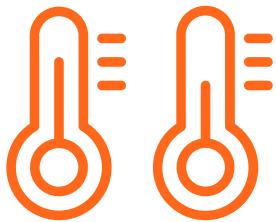
« Les vulnérabilités peuvent être découvertes et évaluées, tandis que leur exploitation peut être anticipée et prédictive grâce à des actions préventives priorisées visant à changer la posture de sécurité et de risque de l'entreprise. »

- Gartner³

³ How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation, Gartner, janvier 2020

« Mettez en œuvre une priorisation des vulnérabilités multidimensionnelle basée sur le risque, en incluant des facteurs tels que la sévérité de la vulnérabilité, l'activité d'exploitation actuelle, la criticité pour l'entreprise et l'exposition du système affecté. »

– Gartner⁴



Étape 3 : Prioriser

Tirez parti de la threat intelligence et du contexte de l'entreprise.

C'est là que toutes les données contextuelles sont rassemblées pour faciliter une prise de décision éclairée. Les équipes de sécurité étant déjà débordées, analyser manuellement les fichiers CSV et les feuilles de calcul est une perte de temps. Elles n'ont tout simplement aucun moyen physique de mener les recherches nécessaires à grande échelle. L'automatisation est nécessaire pour faciliter ce processus.

Pour garder une longueur d'avance sur les attaquants, la gestion des vulnérabilités basée sur le risque utilise des algorithmes d'apprentissage automatique qui identifient et reconnaissent les schémas d'activité pour prédire quelles vulnérabilités sont les plus susceptibles d'être exploitées. Elle combine ensuite ces données avec le score de vulnérabilité et le score de criticité des assets et priorise les vulnérabilités les plus dangereuses, en mettant à jour en permanence les priorités à mesure que le paysage des menaces change. Et elle le fait plus rapidement que n'importe quelle équipe humaine.

L'automatisation permet d'activer une analyse continue et complète des données de vulnérabilité à grande échelle. Elle vous permet de vous concentrer en priorité sur ce qui importe le plus. Vous pouvez ainsi arrêter de gaspiller du temps et des ressources sur des vulnérabilités qui présentent peu ou pas de risque. Une solution adaptée aidera votre équipe à devenir beaucoup plus efficace et à réduire les risques avec des efforts minimes. Vous passerez moins de temps sur des processus manuels, ce qui vous permettra de vous concentrer sur des initiatives de sécurité plus stratégiques.

⁴How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation, Gartner, janvier 2020



Étape 4 : Corriger

Obtenez des résultats quantifiables pour atteindre un objectif commun.

Une fois que votre équipe a déterminé les vulnérabilités à prioriser, il est temps de collaborer avec l'IT pour les corriger. Une collaboration efficace entre les équipes sécurité et IT est primordiale pour la remédiation et peut vous aider à maximiser les bénéfices de vos efforts pour découvrir, évaluer et prioriser les vulnérabilités.

Une liste bien plus courte

Envoyer au service IT une liste contenant des milliers de vulnérabilités à corriger sans instructions claires est une approche inefficace. Grâce à la gestion des vulnérabilités basée sur le risque, vous pouvez fournir à l'IT une petite liste de vulnérabilités à corriger, ce qui peut aider vos équipes à mieux travailler ensemble. Non seulement vous êtes assuré que les vulnérabilités les plus à risque sont corrigées en premier, mais cela aide en plus les équipes de sécurité à montrer pourquoi celles qui figurent en tête de liste sont prioritaires, renforçant ainsi leur crédibilité au sein de l'entreprise.

« Améliorez les fenêtres de remédiation et l'efficacité en utilisant des technologies qui peuvent automatiser l'analyse des vulnérabilités » – Gartner⁵

Intégration aux systèmes IT

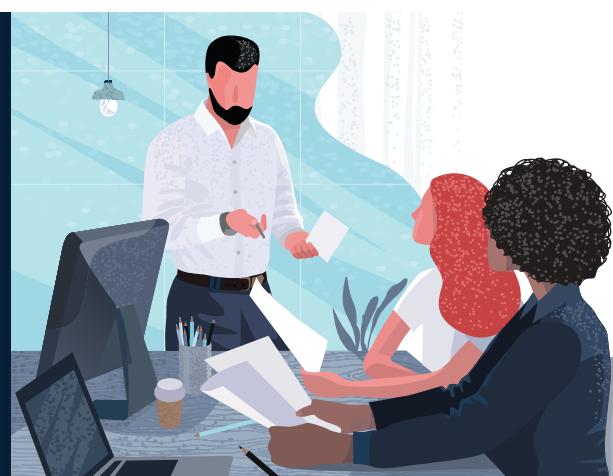
En intégrant la gestion des vulnérabilités à vos systèmes IT, vous pouvez créer une boucle de rétroaction fermée qui garantit que les tâches les plus importantes sont effectuées en premier. Lorsque les équipes de sécurité priorisent la remédiation des vulnérabilités critiques, elles doivent ajouter des informations de remédiation dans les workflows IT. Cela leur permet d'expliquer pourquoi une vulnérabilité est hautement prioritaire et comment la corriger. Une fois la vulnérabilité corrigée, la plateforme IT doit renvoyer ces informations aux équipes de sécurité. Ainsi, la boucle est bouclée et cela garantit que les vulnérabilités critiques sont corrigées. C'est le moyen le plus efficace de s'assurer que les corrections essentielles sont apportées immédiatement et que rien d'important ne passe à travers les mailles du filet.

⁵ How Security and Risk Management Leaders Can Establish Practical Time Frames for Vulnerability Remediation, Gartner, janvier 2020

Facilitez la collaboration entre les équipes sécurité et IT

Tirez parti de l'intégration de Tenable à ServiceNow pour améliorer l'efficacité opérationnelle des équipes sécurité et IT :

- Intervenez rapidement et réduisez les erreurs grâce à l'automatisation et à l'orchestration
- Faites évoluer vos processus à l'aide de workflows parallèles, reproductibles et mesurables
- Suivez un processus de remédiation en circuit fermé à l'aide de scans ciblés répétés





Étape 5 : Mesurer

Identifiez les lacunes et les aspects à améliorer.

Comme pour toute stratégie, le calcul des métriques clés met en lumière ce qui fonctionne bien et peut aider à identifier ce qui peut être amélioré. Ici, vous souhaitez examiner des métriques de sécurité et de maturité telles que le délai d'évaluation, le délai de remédiation et le score de Cyber Exposure au fil du temps pour évaluer les performances de votre entreprise par rapport aux normes du secteur. Si ce que vous faites ne correspond pas aux meilleures pratiques, apportez les rectifications qui s'imposent. Vous ne pouvez pas améliorer ce que vous ne mesurez pas.

Utilisez des métriques pour changer les comportements

Dire aux personnes concernées et aux dirigeants combien de vulnérabilités ont été corrigées par l'équipe ne leur donne pas une image précise de la sécurité. Vous devez leur montrer que vos efforts de remédiation sont efficaces.

En utilisant des métriques qui prouvent que les risques pour l'entreprise ont été réduits, vous pouvez combler cette lacune et démontrer l'efficacité de votre équipe de sécurité. En interne, mesurer le succès est bon pour le moral de vos équipes et vous permet de les garder motivées et actives. Enfin, communiquer les résultats de l'entreprise à l'équipe dirigeante et à d'autres décideurs clés leur prouvera qu'investir dans de nouveaux outils et solutions est bénéfique pour l'entreprise.

« D'ici 2022, les entreprises qui utilisent une méthode de gestion des vulnérabilités basée sur le risque connaîtront 80 % de fuites de données en moins. »

– Gartner⁶

⁶ A Guide to Choosing a Vulnerability Assessment Solution, Gartner, avril 2019

Repensez votre stratégie de sécurité en adoptant une gestion des vulnérabilités basée sur le risque.

Contactez Tenable pour planifier une démo et voir cette approche en action.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046, États-Unis

Amérique du Nord : +1(410) 872 0555

fr.tenable.com

10/05/20 V01

COPYRIGHT 2020 TENABLE, INC. TOUS DROITS RÉSERVÉS. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW ET LOG CORRELATION ENGINE SONT DES MARQUES DÉPOSÉES DE TENABLE, INC. TENABLE.SC, LUMIN, ASSURE ET THE CYBER EXPOSURE COMPANY SONT DES MARQUES DÉPOSÉES DE TENABLE, INC. TOUS LES AUTRES PRODUITS OU SERVICES SONT DES MARQUES DÉPOSÉES DE LEURS PROPRIÉTAIRES RESPECTIFS.