Ivanti Neurons for Risk-Based Vulnerability Management (RBVM)

Faites évoluer votre stratégie de gestion des vulnérabilités pour adopter une approche basée sur les risques, avec Ivanti Neurons for RBVM. Cette offre SaaS vous permet de prioriser efficacement les vulnérabilités et faiblesses à risque élevé afin de mieux vous protéger des fuites de données, des ransomwares et d'autres cybermenaces.

Vers une nouvelle approche de la gestion des vulnérabilités

On décompte plus de 270 000 vulnérabilités connues[1]. Heureusement, les entreprises n'ont pas besoin de corriger absolument toutes les vulnérabilités et les faiblesses présentes dans leur environnement IT. Malheureusement, dans l'approche traditionnelle de la gestion des vulnérabilités, l'identification de la vulnérabilité/faiblesse rare vraiment dangereuse est un processus long et faillible.

Avant même de commencer à prioriser les vulnérabilités/faiblesses afin d'y remédier, les entreprises doivent collecter des données hétérogènes et éparses (résultats des scanners, « threat intelligence », etc.), les normaliser, puis les préparer pour les utiliser. Sans automatisation, ces opérations peuvent s'étaler sur des jours, des semaines, voire des mois, avec toujours le risque d'une erreur humaine.

Et le processus de priorisation n'est pas plus simple ! Prenons le cas des vulnérabilités de ransomware : 74 % ne sont pas classées « Critique » dans la liste CVSS v3, et il en manque 156 dans le catalogue KEV (vulnérabilités exploitées connues) de la CISA. De plus, trois des scanners les plus courants n'ont toujours ni plug-in ni signature de détection pour 20 vulnérabilités de ransomware[2].

De surcroît, les décideurs IT et de sécurité déplorent non seulement le manque de coopération entre leurs équipes mais considèrent que c'est leur principal défi face aux cyberattaques[3]. Ces frictions entre les différentes parties prenantes de la gestion des vulnérabilités peuvent ralentir la remédiation et laisser l'entreprise vulnérable aux attaques.

Principales caractéristiques

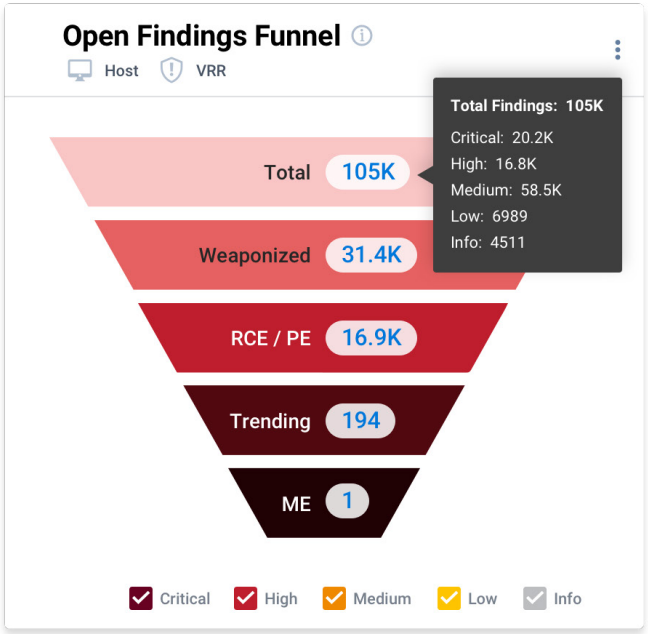
Priorisation des actions immédiates basée sur les risques

En quelques minutes (plutôt que quelques mois), passez de la détection des vulnérabilités et des faiblesses à leur remédiation grâce à une vue contextualisée basée sur les risques qui vous renseignera sur la posture de cybersécurité de votre entreprise. Ivanti Neurons for RBVM mesure les risques et priorise les opérations de remédiation, notamment par la comparaison constante de l'infrastructure de l'entreprise avec :

- les données de vulnérabilité internes et externes ;
- la « threat intelligence » ;
- les résultats des tests d'intrusion manuels et les conclusions d'études ;
- la criticité des actifs.

Mieux encore : vous élaborez un plan d'attaque solidement étayé, sans véritable effort manuel.

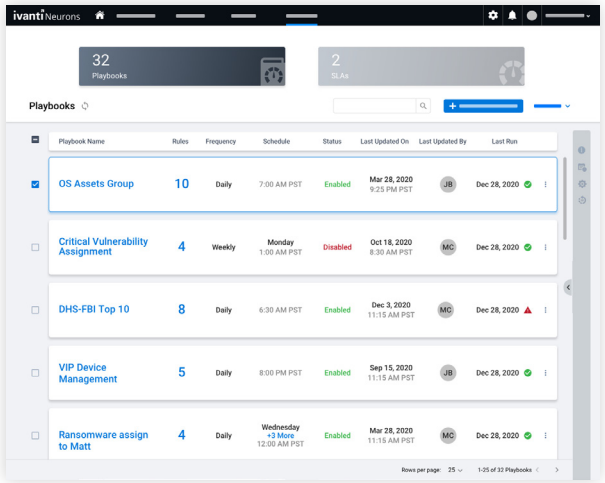
Contrairement au score CVSS, le score VRR propre à Ivanti permet aux entreprises de mesurer précisément l'impact des vulnérabilités et de déterminer les probabilités d'exploitation. Ivanti Neurons for RBVM identifie aussi spécifiquement les vulnérabilités RCE (exécutions de code à distance) et PE (élévation des privilèges), les vulnérabilités liées aux ransomwares, et celles qui sont en vogue et actives. Les entreprises peuvent ainsi se concentrer sur les vulnérabilités les plus dangereuses.



La remédiation avant l'administration

Renforcez votre cybersécurité sans y consacrer tout le temps et les efforts habituels ni commettre les erreurs classiques grâce aux nombreuses options d'automatisation et autres fonctions de performance :

- Création de playbooks pour automatiser les tâches courantes ou répétitives traditionnellement traitées par les analystes de sécurité.
- Définition automatique facultative des dates limites d'élimination des vulnérabilités avec l'automatisation des accords de niveau de service (SLA).
- Alertes en temps quasi réel hors de la plateforme incluant des liens vers la page produit avec les détails de l'événement concerné.
- Filtrage facile des hôtes et de leurs découvertes, en fonction de critères qui révèlent l'exposition réelle aux principales vulnérabilités critiques (ransomwares, CVE en vogue, etc.) à l'aide de vues système distribuées en mode Push par l'équipe de sécurité Ivanti.
- Transmission de listes de vulnérabilités priorisées directement à Ivanti Neurons for Patch Management en vue de leur remédiation : finis les envois de fichiers CSV contenant des ID de CVE par e-mail et par chat.

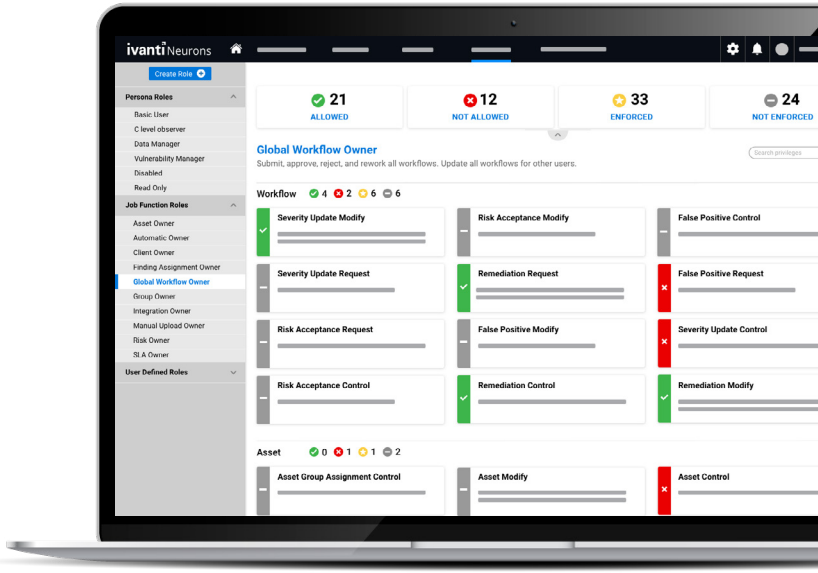


Amélioration de la collaboration entre les acteurs de la sécurité

Favorisez les communications et la coopération entre les parties prenantes à l'échelle de l'entreprise, en leur fournissant des informations pertinentes en rapport avec leur rôle. Ivanti Neurons for RBVM exploite le contrôle d'accès basé sur les rôles pour garantir aux collaborateurs un accès sécurisé à Ivanti Neurons for RBVM.

Depuis le produit, les utilisateurs accèdent à des tableaux de bord selon leur profil, du SOC à la direction. Ils peuvent adapter ces tableaux de bord à des cas d'usage plus spécifiques, voire s'aider de widgets pour en créer d'autres répondant aux besoins précis de certaines équipes et fonctions.

En outre, le produit quantifie le profil de risque de l'entreprise sous forme d'un score Ivanti RS3 qui garantit que toutes les parties prenantes de sécurité s'alignent sur le niveau global de sécurité de l'entreprise. L'intégration bidirectionnelle avec des systèmes de tickets de support comme Ivanti Neurons for ITSM améliore la coordination entre les différents acteurs de la sécurité.



Principales fonctionnalités

Fonctionnalité	Description
Sources de données diverses	Obtenez une vue d'ensemble des cyber-risques grâce à un produit qui absorbe les données provenant des scanners réseau, des postes client, des bases de données et des périphériques IoT, des informations de vulnérabilité de plus de 100 sources indépendantes, des découvertes manuelles des équipes de recherche et de tests d'intrusion, et de sources de données personnalisées.
Moteur de menaces	Bénéficiez d'insights uniques sur les vulnérabilités (notamment, la liste de celles liées aux ransomwares) via des informations de « threat intelligence » provenant d'Ivanti Neurons for Vulnerability Knowledge Base et générées par l'homme et l'IA.
Score VRR (score de risque de la vulnérabilité)	Déterminez rapidement la dangerosité d'une vulnérabilité avec des scores de risque numériques qui tiennent compte de ses attributs intrinsèques, ainsi que du contexte des menaces sur le terrain.
Ivanti RS³	Bénéficiez d'une vue quantifiée du profil de risque de votre entreprise, via une méthode de détermination du score de risque qui tient compte du VRR, de la criticité des actifs, de la « threat intelligence » et de l'accessibilité externe.
Automatisation	Automatisez toute une série de tâches jusqu'alors manuelles pour que les collaborateurs puissent se concentrer sur les actions de remédiation et les initiatives stratégiques plutôt que sur les tâches administratives.
Alertes et notifications	Soyez instantanément averti des événements pertinents grâce à des alertes envoyées presque en temps réel par le moteur de notification. De même, orientez les autres utilisateurs vers des informations importantes en partageant des liens profonds au sein du produit.
COrganisation personnalisable des données	Révélez des insights actionnables grâce aux widgets utilisateur qui permettent de créer des tableaux de bord personnalisés. Vous disposez aussi d'une fonctionnalité de permutation des données sous forme de listes.
Tableaux de bord	Découvrez rapidement comment des vulnérabilités critiques (comme Log4j et celles associées aux correctifs des Patch Tuesday) se manifestent dans votre environnement grâce aux vues basées sur les menaces. Vous pouvez aussi créer et partager vos propres vues personnalisées.
Vues basées sur les menaces	Découvrez rapidement comment des menaces spécifiques (comme BlueKeep, WannaCry ou les 10 principales vulnérabilités exploitées répertoriées par le FBI/la DHS/la CISA) se manifestent dans l'environnement de votre entreprise, à l'aide de filtres basés sur les menaces. Vous pouvez aussi créer et partager vos propres filtres personnalisés.
Intégrations Neurons	Associez Ivanti Neurons for RBVM à Ivanti Neurons for ASPM pour étendre la gestion des vulnérabilités basée sur les risques à une plus grande partie de votre surface d'attaque. Exploitez les intégrations prêtes à l'emploi avec Ivanti Neurons for ITSM et Ivanti Neurons for Patch Management pour donner aux personnes chargées de la gestion des vulnérabilités les moyens de mieux travailler.

À propos d'Ivanti

Ivanti est une entreprise mondiale de logiciels de sécurité et de technologies de l'information dédiée à libérer le potentiel humain en gérant, automatisant et protégeant les données et les systèmes pour favoriser l'innovation continue. Avec des solutions logicielles adaptables aux besoins des clients, Ivanti permet aux équipes informatiques et de sécurité d'améliorer l'efficacité opérationnelle, de réduire les coûts et de réduire de manière proactive les risques de sécurité. Au cœur des offres d'Ivanti se trouve la plateforme Ivanti Neurons, alimentée par l'IA, qui transforme la façon dont les équipes informatiques et de sécurité fonctionnent. En fournissant des services et des outils unifiés et réutilisables, la plateforme aide à garantir une visibilité, une évolutivité et une mise en œuvre sécurisée des solutions, permettant aux équipes de travailler plus intelligemment, pas plus durement. Plus de 34 000 clients, dont 85 des 100 plus grandes entreprises du Fortune 100, ont choisi Ivanti pour relever leurs défis. Ivanti suit les principes de "Secure by Design" pour fournir des solutions logicielles qui évoluent avec les besoins de nos clients afin d'aider les équipes informatiques et de sécurité à améliorer l'efficacité opérationnelle tout en réduisant les coûts et en réduisant de manière proactive les risques. Ivanti favorise un environnement inclusif où les perspectives diverses sont honorées et valorisées, reflétant un engagement envers un avenir durable pour les clients, les partenaires, les employés et la planète. En savoir plus, visitez le site ivanti.fr et suivez-nous sur Twitter (@GoIvanti).réseaux sociaux @GoIvanti.

ivanti neurons

ivanti.fr/neurons
+33 (0)1 76 40 26 20
contact@ivanti.fr

1. Données extraites d'Ivanti Neurons for Vulnerability Knowledge Base le 29 juin 2023
2. Cyber Security Works, Cyware, Ivanti, Securin, « 2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management », 16 février 2023. https://www.securin.io/ransomware/
3. ExtraHop, « Cyber Confidence Index 2022 », 1er mars 2022. https://www.extrahop.com/resources/papers/cyber- confidence-index-2022/