ivanti neurons

Ivanti Neurons for App Security Orchestration & Correlation (ASOC)

Étendez la gestion des vulnérabilités basée sur les risques à la pile d'applications

Avec Ivanti Neurons for ASOC, vous faites évoluer la gestion des vulnérabilités de vos applications vers une approche basée sur les risques. Cette offre SaaS vous permet de prendre rapidement des décisions réfléchies sur les développements à envisager pour renforcer la sécurité des applications internes et front-office.

Une gestion des vulnérabilités basée sur les risques incluant les applis

Le nombre d'applications analysées chaque trimestre a triplé ces 10 dernières années, et la fréquence des analyses a été multipliée par 20 sur cette même période.[1] Sans surprise, les entreprises ayant une approche traditionnelle de la gestion des vulnérabilités ont des difficultés à identifier dans la pile d'applications la vulnérabilité/faiblesse rare qui présente vraiment un danger. En effet, elles sont submergées par les données !

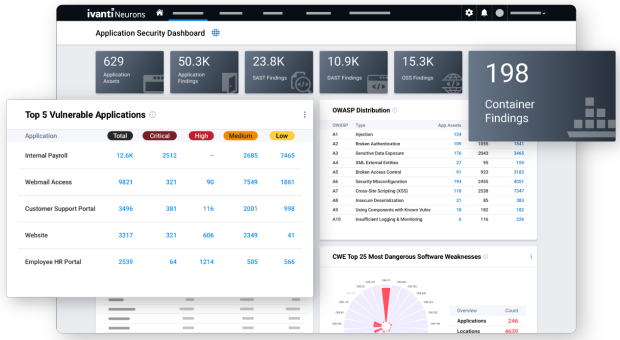
Avant même qu'elles puissent commencer à prioriser les vulnérabilités/faiblesses, ces entreprises doivent collecter tout un éventail de données hétérogènes (SAST, DAST, OSS, résultats des scanners de conteneur, « threat intelligence », etc.), les normaliser, puis les préparer en vue de leur utilisation. Effectués manuellement, ces processus prennent des semaines et sont sujets à l'erreur humaine.

Le processus de priorisation n'est pas meilleur. Prenons les 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 populaires ne proposent toujours pas de plug-in ou de signature de détection pour 20 vulnérabilités de ransomware.[2]

En outre, le manque de coopération entre les différentes équipes impliquées reste la principale difficulté rencontrée lorsqu'il s'agit de se protéger des cyberattaques.[3] Ces frictions entre les parties prenantes de la gestion des vulnérabilités peuvent ralentir la remédiation et laisser l'entreprise vulnérable aux attaques.

Présentation d'Ivanti Neurons for ASOC

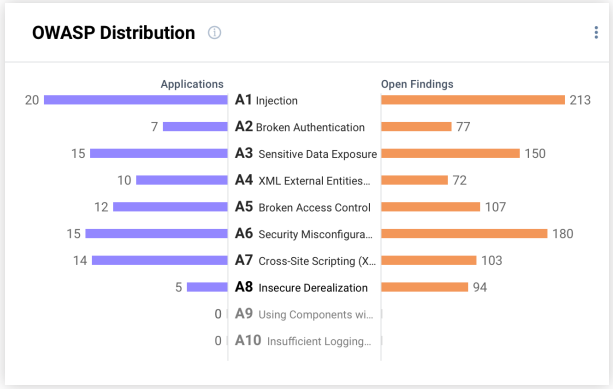
Avec Ivanti Neurons for ASOC, vous adoptez une approche basée sur les risques pour gérer les vulnérabilités de votre pile d'applications. Ses diverses fonctions sont regroupées au sein d'une interface unique, si bien que vous pouvez progressivement sortir de l'approche « gestion en chaise pivotante » caractéristique des pratiques traditionnelles de gestion des vulnérabilités.



Principales fonctionnalités

Visibilité complète sur l'exposition aux risques de votre pile d'applications

Bénéficiez d'une visibilité complète sur l'exposition aux risques de la pile d'applications, du développement à la production. Ivanti Neurons for ASOC unifie toutes les données d'analyse des applications (SAST, DAST, OSS et conteneur) pour repérer les vulnérabilités et les faiblesses, et prioriser leur élimination.



Ivanti Neurons for ASOC étant une solution indépendante du scanner, l'équipe DevOps peut librement choisir les différents outils d'analyse dont elle a besoin pour chaque phase du cycle de vie du développement. La solution normalise les données de vulnérabilité des applications et les résultats d'analyse, puis les compare en continu avec les tendances des menaces actives sur le terrain. Les utilisateurs connaissent ainsi immédiatement les dangers les plus sévères pour leur entreprise. Ils peuvent en outre effectuer un « drill-down» à l'emplacement exact du code dans la pile d'applications.

Depuis le tableau de bord Sécurité des applications, les utilisateurs peuvent s'informer sur la progression des développements applicatifs visant à traiter les failles de sécurité. En plus d'une image complète des vulnérabilités, des CWE et des OWASP qui menacent l'entreprise, il informe sur les derniers résultats d'analyse et leur taux de remédiation.

Priorisation des actions immédiates basée sur le risque

Grâce à une vue contextualisée de la posture de cybersécurité de votre entreprise, quelques minutes suffisent (au lieu de quelques mois) pour détecter les vulnérabilités et les faiblesses et y remédier. Ivanti Neurons for ASOC mesure les risques et priorise les opérations de remédiation via un processus qui implique une comparaison constante des applications de l'entreprise avec :

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

Mieux encore : vous élaborez un plan d'attaque mûrement réfléchi, pratiquement sans aucun effort manuel.

Contrairement au score CVSS, le score VRR (Vulnerability Risk Rating) exclusif d'Ivanti permet aux entreprises de mesurer précisément l'impact d'une vulnérabilité et de déterminer ses probabilités d'exploitation. Ivanti Neurons for ASOC identifie aussi spécifiquement les vulnérabilités RCE (Exécution de code à distance) et PE (Élévation des privilèges), de ransomware, ainsi que celles qui sont en vogue et actives. Les entreprises peuvent ainsi se concentrer sur les vulnérabilités les plus dangereuses.

Focus sur la remédiation plutôt que sur l'administration

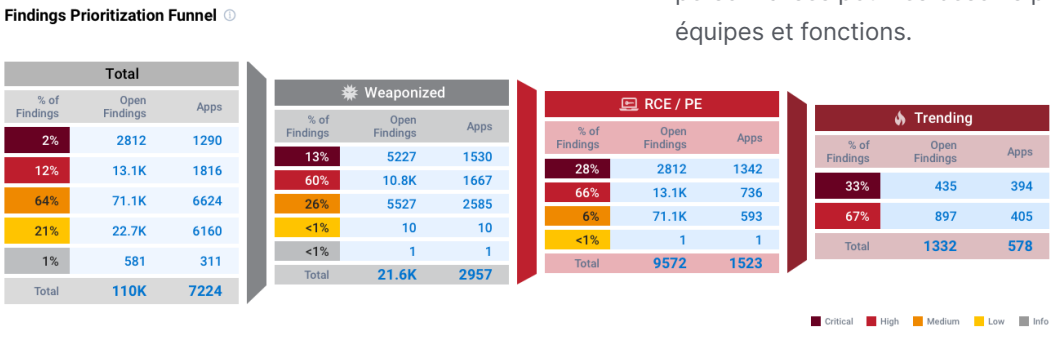
Renforcez votre cybersécurité sans la perte de temps, les efforts, et les erreurs généralement associés à cette démarche, grâce à différentes options d'automatisation et autres fonctions qui améliorent l'efficacité :

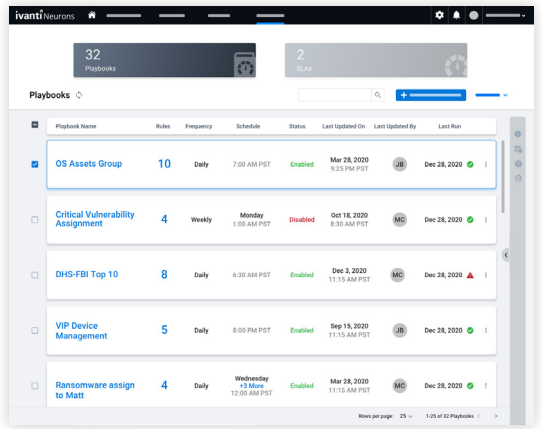
- Création de playbooks pour automatiser les tâches courantes ou répétitives traditionnellement gérées par les analystes de sécurité.
- Définition automatique des dates limites de remédiation des vulnérabilités, avec l'automatisation des accords de niveau de service (SLA).
- Réception d'alertes pratiquement en temps réel, en dehors de la solution, avec des liens vers la page contenant les détails de l'événement auquel vous êtes abonné.
- Filtrage facile des applications et de leurs résultats en fonction de critères de tendance qui révèlent l'exposition 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.

Amélioration de la collaboration entre les acteurs de la sécurité

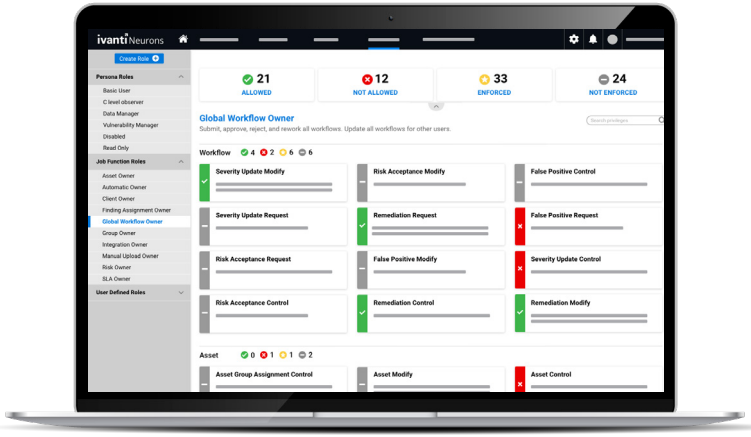
Favorisez les communications et la coopération entre les parties prenantes de la sécurité, en leur fournissant des informations pertinentes en rapport avec leur rôle. Ivanti Neurons for ASOC emploie un mécanisme RBAC (contrôle d'accès basé sur les rôles) qui permet de fournir un accès sécurisé à la solution à tout le personnel éligible.

Depuis la solution, les utilisateurs accèdent à des tableaux de bord prédéfinis conçus pour tout le personnel, des SOC aux dirigeants. Ces tableaux de bord peuvent être adaptés à des cas d'usage plus spécifiques. D'autre part, des widgets utilisateur permettent de créer des tableaux de bord personnalisés pour les besoins précis de certaines équipes et fonctions.





En outre, la solution quantifie le profil de risque de l'entreprise sous forme d'un score Ivanti RS[3]. Ce score garantit que toutes les parties prenantes de la sécurité s'alignent sur le niveau global de sécurité pour l'entreprise. L'intégration bidirectionnelle avec les systèmes de gestion des tickets comme Ivanti Neurons for ITSM améliore la coordination entre les différentes parties prenantes.



Fonctionnalités

Fonctionnalité	Description
Sources de données diverses	Obtenez une vue d'ensemble des cyber-risques grâce à une solution qui collecte les données des scanners d'applications (SAST, DAST, OSS, conteneur), les données de vulnérabilité de plus de 100 sources indépendantes, les découvertes manuelles des équipes de recherche et de tests d'intrusion, et des sources de données personnalisées.
Moteur de menaces	Bénéficiez d'insights uniques sur les vulnérabilités (notamment, la liste de celles qui sont liées aux ransomwares) via des informations de « threat intelligence » générées par l'homme et l'IA à partir d'Ivanti Neurons for Vulnerability Knowledge Base.
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 et 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, des multiples sources de « threat intelligence » et de l'accessibilité externe.
Automatisation	Remplacez toute une série de tâches manuelles par l'automatisation, pour que les collaborateurs puissent se concentrer sur les opérations 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 en partageant des liens profonds au sein de la solution.
Organisation personnalisable des données	Révélez des insights actionnables grâce aux widgets utilisateur qui permettent de créer des tableaux de bord entièrement personnalisés. Vous disposez aussi d'une fonctionnalité de permutation des données sous forme de listes.
Tableaux de bord	Exécutez des requêtes visuelles performantes et découvrez les risques encourus par vos actifs et votre infrastructure via des tableaux de bord prédéfinis et personnalisables dotés de fonctions « drill-down ».
Vues basées sur les menaces	Découvrez rapidement comment des vulnérabilités critiques (comme Log4j et celles associées aux publications Patch Tuesday) se manifestent dans votre environnement, grâce aux vues basées sur les menaces. Vous pouvez aussi créer et partager vos propres vues personnalisées.
Intégrations Neurons	Combinez Ivanti Neurons for ASOC et Ivanti Neurons for RBVM pour élargir la gestion des vulnérabilités basée sur les risques à une plus grande zone de votre surface d'attaque. Exploitez l'intégration prête à l'emploi avec Ivanti Neurons for ITSM pour donner plus de moyens à vos spécialistes en gestion des vulnérabilités et leur permettre d'être plus efficaces.

À propos d'Ivanti

Ivanti améliore et sécurise l'Everywhere Work pour favoriser la réussite des entreprises et l'efficacité des collaborateurs. Nous mettons la technologie au service des gens, et pas l'inverse. Aujourd'hui, les collaborateurs utilisent une multitude de périphériques personnels et professionnels pour accéder aux données et applications IT sur plusieurs réseaux, afin de rester productifs où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Ivanti est l'une des rares entreprises technologiques capable de détecter, de gérer et de protéger tous les actifs IT et postes client d'une entreprise. Plus de 40 000 clients, dont 88 entreprises Fortune 100, ont choisi Ivanti pour fournir une expérience numérique d'excellence aux collaborateurs, et améliorer la productivité et l'efficacité de leurs équipes IT et Sécurité. 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.fr et suivez @GoIvanti.

ivanti

Pour plus d'informations ou pour contacter Ivanti, visitez ivanti.fr

1. Veracode, "State of Software Security v12", 2021. https://info.veracode.com/report-state-of-software-security-volume-12.html
2. Cyber Security Works, Cyware, Ivanti, Securin, "2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management", 16 February 2023. https://www.securin.io/ransomware/
3. ExtraHop, "Cyber Confidence Index 2022", 1 March 2022. https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/