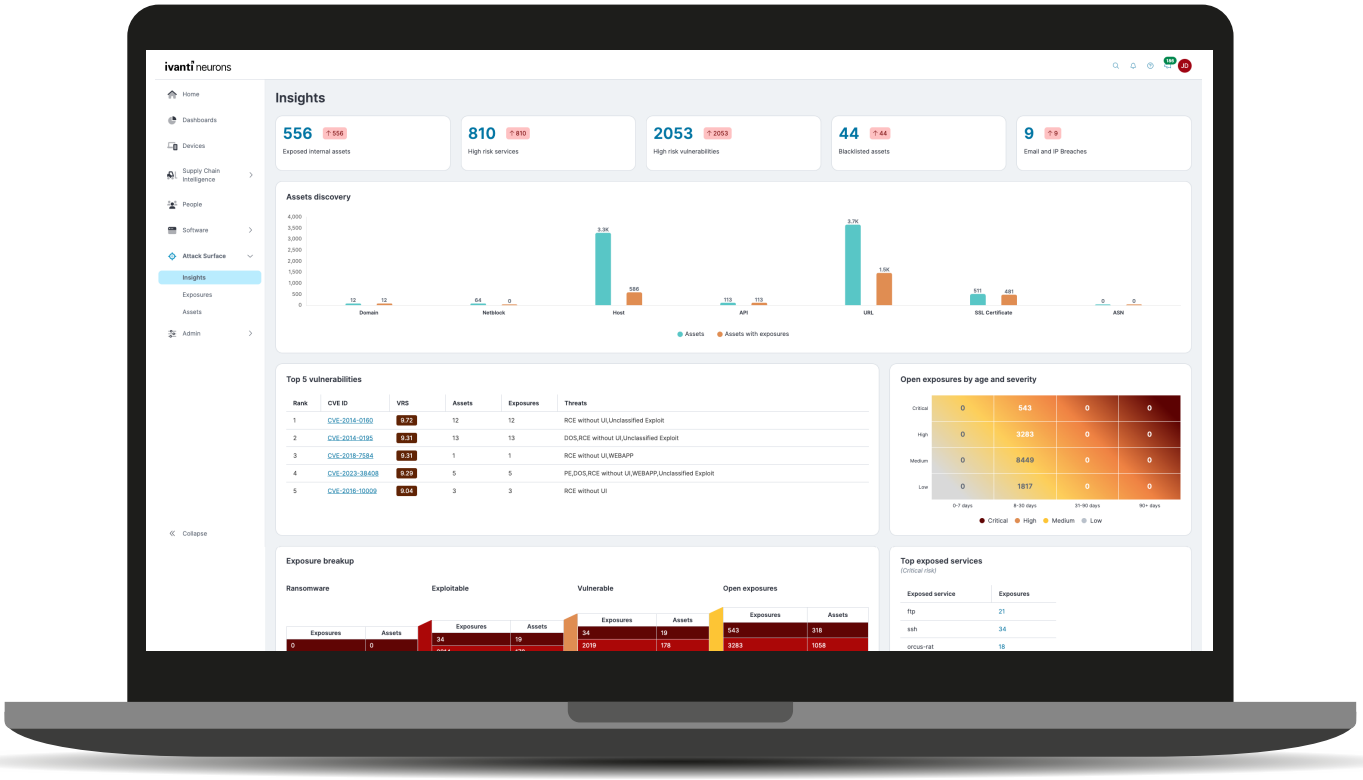
Ivanti Neurons for EASM

Combattez l'expansion de la surface d'attaque grâce à une visibilité complète sur les actifs tournés vers l'extérieur et des informations décisionnelles sur les expositions

L'expansion croissante de l'Everywhere Work et la transformation digitale ont provoqué une augmentation incontrôlée de la surface d'attaque. Ivanti Neurons for External Attack Surface Management (EASM) fournit une vue complète et en temps réel des actifs tournés vers l'extérieur et des expositions associées. Ces informations vous permettent d'éliminer les expositions à haut risque pour vous protéger proactivement des cyberattaques en surveillant votre surface d'attaque.



Expansion incontrôlée de la surface d'attaque

Le passage à l'Everywhere Work et la transformation digitale ont accéléré le recours au Shadow IT et aux outils Cloud. En parallèle, les entreprises constatent une adoption croissante des périphériques IoT et une plus grande interconnexion des supply chains.

Résultat : les équipes Sécurité manquent de visibilité sur leur surface d'attaque totale, et en particulier sur les actifs tournés vers l'extérieur et les expositions qui leur sont associées.

Des actifs inconnus, non vérifiés, non gérés et sans correctifs exposent les entreprises à des risques sévères : fuites de données, sanctions financières et interruptions de service. Pour protéger correctement leur entreprise, les équipes Sécurité ont besoin d'une visibilité permanente sur la totalité de leur surface d'attaque.

C'est là qu'intervient Ivanti Neurons for EASM

Avec Ivanti Neurons for EASM, vous obtenez et maintenez une bonne visibilité de tous les actifs tournés vers l'extérieur, sur toute la surface d'attaque de votre entreprise. Vous bénéficiez d'une intelligence décisionnelle basée sur les risques encourus par ces actifs afin de vous protéger proactivement des fuites de données, sanctions financières et interruptions de service.

Principales fonctions

Obtention d'une visibilité complète

Bénéficiez d'une bonne visibilité sur tous les actifs connectés à Internet et des expositions associées, sur toute la surface d'attaque de votre entreprise. La surveillance sans agent révèle les actifs que les outils de découverte traditionnels sont incapables de détecter, ainsi que ceux qui ne sont généralement pas surveillés par les équipes de sécurité : compartiments Amazon S3 mal configurés, environnements d'assurance qualité et de développement, sites Web et applis Java exécutées sur des serveurs que tout le monde pensait hors service.

La surveillance en continu garantissant une visibilité en temps quasi réel sur ces actifs, vous savez immédiatement s'ils sont exposés. De même, vous pouvez réagir dès que de nouveaux actifs sont déployés.

Types d'actifs découverts par l'EASM	Vecteurs d'exposition découverts par l'EASM
■ API ■ Domaine ■ Hôte ■ Bloc réseau ■ Certificat SSL ■ URL	■ Sécurité des applications ■ Fuites de données ■ État de santé DNS ■ Sécurité des e-mails ■ Sécurité réseau ■ Fréquence d'application des correctifs ■ Ingénierie sociale

Grâce à une fonction de l'espace de travail, les actifs et les expositions peuvent être regroupés par catégorie (par Département et par Filiale, par exemple). Cela s'avère utile lorsque vous utilisez Ivanti Neurons for EASM pour surveiller les surfaces d'attaque externes d'entreprises tierces, comme les partenaires de la supply chain.

Priorisation des expositions les plus dangereuses

Bénéficiez d'informations décisionnelles sur les vulnérabilités de votre surface d'attaque externe afin de concentrer vos efforts de remédiation au bon endroit. Vous obtenez notamment un score VRS (Vulnerability Risk Score) pour chaque CVE détectée par Ivanti Neurons for EASM.

VRS facilite la prise de décision, car il permet aux équipes de sécurité de quantifier les risques que représente une vulnérabilité et de comprendre son contexte de menace. Il tient compte des scores CVSS indiqués dans la base NVD (Base nationale des vulnérabilités américaine), ainsi que de divers autres attributs reflétant l'impact d'une vulnérabilité dans un environnement donné.

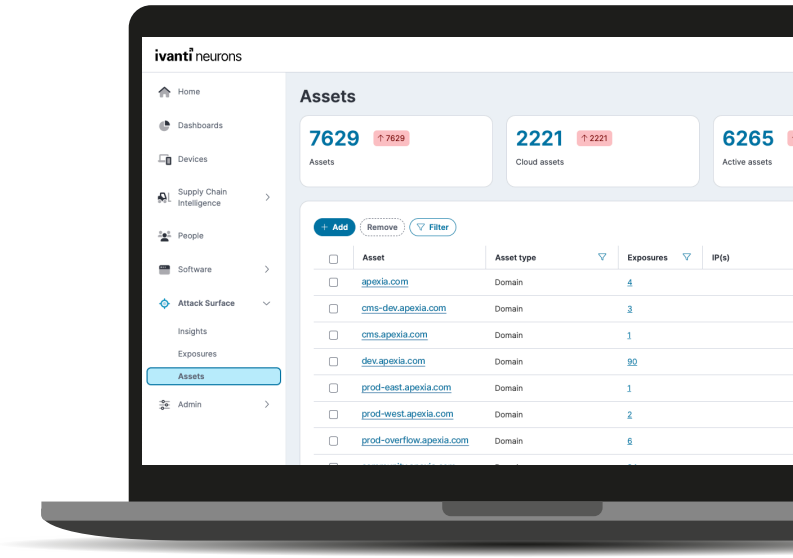
Signalisation des risques

Les rapports de sécurité au format PDF vous permettent de satisfaire aux exigences de reporting des parties prenantes. Ils peuvent aussi être utiles lors de l'évaluation des risques associés aux partenaires, aux fournisseurs et aux acquisitions d'entreprise. Ces rapports exportables fournissent des informations détaillées sur les expositions associées à la surface d'attaque externe de votre entreprise.

Gestion des failles dans la surface d'attaque

Exploitez la puissance d'Ivanti Neurons pour combler les failles critiques révélées par Ivanti Neurons for EASM dans votre surface d'attaque. L'utilisation conjointe d'Ivanti Neurons for EASM et des produits suivants, vous permettra de répondre le plus rapidement possible aux problèmes qui impactent les actifs tournés vers l'extérieur :

- Ivanti Neurons for ITSM : orchestrez la réponse aux incidents entre toutes les équipes.
- Ivanti Neurons for UEM : gérez et sécurisez les postes client.
- Ivanti Neurons for Patch Management : corrigez les vulnérabilités.



Cas d'usage EASM étendus

L'EASM permet de résoudre de nombreuses difficultés rencontrées par les entreprises modernes.

- **Découverte et inventaire des actifs numériques**
  Découvrez et inventoriez les actifs tournés vers l'extérieur à partir des sites Web, adresses IP, noms de domaine, certificats SSL et services Cloud dans les environnements Cloud, IT, IoT et OT.
- **Analyse et priorisation des expositions**
  Priorisez la remédiation des expositions qui impactent les actifs tournés vers l'extérieur (vulnérabilités sans correctif, erreurs de configuration, ports ouverts, etc.).
- **Limitation de la prolifération du Cloud et du Shadow IT**
  Identifiez les actifs publics de tous les fournisseurs Cloud, y compris les instances Cloud créées par des collaborateurs en dehors du canal approprié.
- **Détection des fuites de données**
  Surveillez les fuites de données ou l'exposition de données sensibles dues aux outils de collaboration et aux applications Cloud utilisés en interne et par des tiers.
- **Évaluation des risques liés aux filiales, tierces parties et cibles d'acquisition**
  Exécutez des contrôles de sécurité complets avant d'intégrer de nouvelles entités dans vos systèmes informatiques.
- **Réduction des attaques par hameçonnage et ingénierie sociale**
  Surveillez les domaines d'hameçonnage, identifiez les sites Web usurpés, et détectez les attaques par ingénierie sociale potentielles visant vos collaborateurs et vos clients.
- **Respect des exigences de conformité réglementaire**
  Mettez-vous en conformité avec les réglementations, notamment le RGPD, les normes HIPAA et PCI DSS qui nécessitent la découverte et l'inventaire des actifs.

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 ivanti.com.

ivanti

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

1. Forrester, « The External Attack Surface Management Landscape, Q1 2023 », 9 janvier 2023