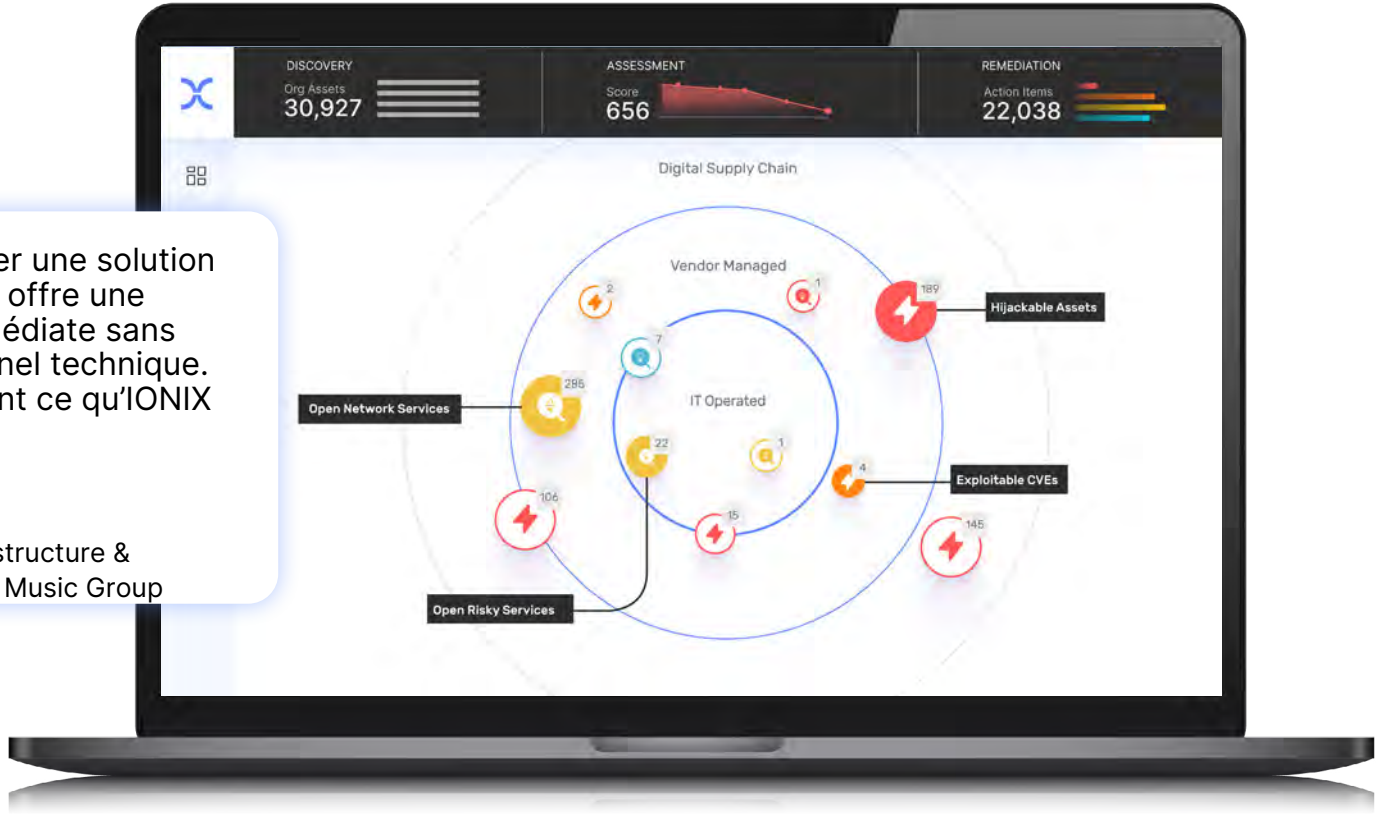
IONIX

BROCHURE

IONIX ATTACK SURFACE MANAGEMENT

EXPOSEZ LES MENACES SUR VOTRE VRAIE SURFACE D'ATTAQUE



« Il est rare de trouver une solution de cybersécurité qui offre une rentabilité quasi immédiate sans impact sur le personnel technique. Mais c'est exactement ce qu'IONIX a proposé. »

John Remo
SVP Global Cloud / Infrastructure & Cybersecurity at Warner Music Group

PLUS DE 20 % DE VOTRE RISQUE D'ATTAQUE réside dans la chaîne d'approvisionnement numérique

IONIX Attack Surface Management offre une concentration maximale sur vos risques de surface d'attaque exploitables les plus importants, y compris au plus profond de la chaîne d'approvisionnement numérique.

VOYEZ VOTRE SURFACE D'ATTAQUE COMME UN ATTAQUANT LE FERAIT, DE L'EXTÉRIEUR VERS L'INTÉRIEUR

L'exposition au risque d'attaque de votre organisation va au-delà des actifs que vous possédez. En effet, un acteur malveillant déterminé à pénétrer votre organisation ne se soucie pas de savoir s'il attaque directement votre actif connecté à Internet ou s'il exploite une vulnérabilité d'un service numérique tiers qui lui donne un accès à votre environnement. Seul IONIX surveille chaque actif et connexion connecté à Internet, se concentre sur les risques les plus critiques pour votre entreprise et fournit des recommandations pour remédier rapidement aux menaces exploitables et réduire le risque d'attaque.

AVANTAGES D'IONIX

- Découvrez-en plus – obtenez une couverture complète de la surface d'attaque
- Évaluez plus en détail – comprenez ce qui est important à corriger et évitez les alertes bruyantes
- Validez automatiquement – tests non intrusifs pour les expositions critiques
- Priorisez plus intelligemment – pas un inventaire des actifs, une carte connectée de l'exploitabilité
- Corrigez plus rapidement – MTTR de jours, pas de mois

« Après avoir travaillé avec IONIX pendant plus d'un an, nous sommes convaincus que sa plateforme ASM nous offre la visibilité essentielle dont nous avons besoin pour résoudre le défi difficile de la gestion des risques et des vulnérabilités de l'ensemble de notre chaîne d'approvisionnement numérique. »

René Rindermann
CISO, E.ON

CAS D'USAGES

Gestion continue de la surface d'attaque
Adaptez automatiquement la couverture aux changements et surveillez les risques.

Sécurité de la chaîne d'approvisionnement numérique
Protégez votre organisation contre les menaces pesant sur la chaîne d'approvisionnement numérique.

Réduction de la surface d'attaque
Réduisez systématiquement les risques critiques et mettez hors service les actifs inutilisés et négligés.

Gestion des risques de fusions et acquisitions
Gérer le cyber-risque tout au long du processus d'acquisition, de l'évaluation à l'intégration.

Contrôle des risques des filiales
Centralisez la supervision et localisez la gestion de la surface d'attaque avec une attribution automatisée.

Sécurité des opérations dans le cloud
Gagnez en visibilité et gérez l'exposition aux risques sur les plateformes de cloud public.

Gestion des vulnérabilités
Augmentez votre programme existant avec la découverte, l'évaluation et la priorisation automatisées des surfaces d'attaque.

Validation de la surface d'attaque
Tests automatisés pour valider les expositions et déterminer l'exploitabilité des menaces zero-day

COMMENT IONIX FONCTIONNE

DÉCOUVERTE DE LA SURFACE D'ATTAQUE | ÉVALUATION DES RISQUES | VALIDATION DE L'EXPOSITION | PRIORISATION DES RISQUES | REMÉDIATION ACCÉLÉRÉE

DÉCOUVERTE DE SURFACE D'ATTAQUE

Découvre votre véritable surface d'attaque et sa chaîne d'approvisionnement numérique

Le moteur de découverte multicouche d'IONIX crée un inventaire complet de votre organisation du point de vue de l'attaquant, y compris les 20 % de votre surface d'attaque exploitable de votre chaîne d'approvisionnement numérique :

- Suivi des événements mondiaux - surveillance de l'enregistrement global de PKI et de domaine
- Découverte de FQDN et d'IP - Découverte basée sur l'apprentissage automatique de tous les domaines, sous-domaines et IP
- Indexation inversée - domaines, blocs IP et plateformes cloud
- Réduction des faux positifs - Les résultats des « preuves de découverte » utilisent le ML pour attribuer avec précision chaque actif

IONIX représente votre surface d'attaque à l'aide d'un modèle ML dynamique basé sur des graphiques, avec des nœuds et des dépendances continuellement mis à jour et un ensemble en constante évolution de chaînes de destruction potentielles évaluées.

ÉVALUATION DES RISQUES

Identifie les risques dans leur contexte, à grande échelle

IONIX effectue une évaluation approfondie de chaque actif selon 13 catégories d'actifs, notamment Cloud, PKI, Web, DNS, automatisée à grande échelle dans l'ensemble de votre environnement. Grâce à Connective Intelligence brevetée, l'évaluation des risques d'IONIX s'étend de manière récursive de vos propres actifs à votre chaîne d'approvisionnement numérique. En évaluant les actifs et les connexions, IONIX identifie les vulnérabilités de connexion à risque (risques externes dus aux chaînes DNS connectées, aux services Web tiers et aux dépendances externes) qui ont un impact sur votre posture de sécurité. De plus, les scores de risque IONIX regroupent les problèmes et les risques de sécurité dans des repères de surface d'attaque de haut niveau dans plusieurs catégories, offrant des moyens pratiques d'améliorer votre programme de sécurité.

VALIDATION DE L'EXPOSITION

Automatise la simulation d'exploitation

IONIX effectue des tests de sécurité actifs et non intrusifs qui simulent des attaques externes sur l'ensemble de votre surface d'attaque. Sans perturber les opérations, IONIX Exposure Validation teste des milliers de risques et étend continuellement sa couverture en réponse aux menaces émergentes, notamment les vulnérabilités exploitables, les erreurs de configuration critiques, les expositions de données, etc. L'approche IONIX identifie les expositions critiques, garantissant ainsi que les équipes de sécurité à court de ressources peuvent se concentrer sur les risques les plus importants pour leur entreprise et obtenir l'adhésion des parties prenantes informatiques pour accélérer la correction.

COMMENT IONIX FONCTIONNE

DECOUVERTE DE LA SURFACE D'ATTAQUE

EVALUATION DES RISQUES

VALIDATION DE L'EXPOSITION

PRIORISATION DES RISQUES

REMÉDIATION ACCÉLÉRÉE

PRIORISATION DES RISQUES

Se concentre sur les risques les plus importants

Les équipes de sécurité doivent tenir compte du contexte commercial unique d'un actif à risque. Le cadre de priorisation d'IONIX combine la gravité des risques, l'exploitabilité, le rayon d'explosion et les renseignements sur les menaces pour aider l'équipe de sécurité à rester concentrée sur les risques les plus importants pour leur organisation. IONIX hiérarchise dynamiquement les menaces en fonction de l'importance des actifs sur quatre dimensions : l'accès aux données sensibles, le contexte commercial, la réputation de la marque et l'impact opérationnel des dépendances. La priorisation basée sur les risques d'IONIX s'appuie sur la gravité (CVSS et EPSS) ainsi que sur les vecteurs d'attaque tels que les erreurs de configuration et d'autres problèmes de sécurité critiques tels que les enregistrements DNS suspendus, le stockage exposé, les risques de script intersite, les mots de passe faibles/ inexistants.

REMÉDIATION ACCÉLÉRÉE

Prévient les attaques avant qu'elles ne se produisent

Les flux de travail intelligents d'IONIX alignent les tâches de correction sur le fonctionnement des opérations de sécurité. Vous passez ainsi moins de temps à acheminer les tickets et plus de temps à résoudre les risques critiques. Les problèmes de sécurité sont regroupés en éléments d'action concis, ce qui réduit le bruit et fournit une clarté immédiate sur ce qui doit être fait. Les éléments d'action sont automatiquement attribués à la bonne entité commerciale ou filiale, et assignés au personnel concerné, pour un délai de résolution plus rapide.
IONIX s'intègre aux systèmes de gestion des informations et des événements de sécurité (SIEM), au SOAR, aux logiciels du centre d'opérations de sécurité (SOC) et aux systèmes de ticketing, accélérant ainsi la correction grâce à des flux de travail rationalisés entre les équipes.

DEMANDEZ UN SCAN GRATUIT ICI

Ionix est représenté en France par AMC SOFT
https://amcsoft.fr - contact@amcsoft.fr
Plus d'information sur ionix.io

BROCHURE IONIX