IONIX

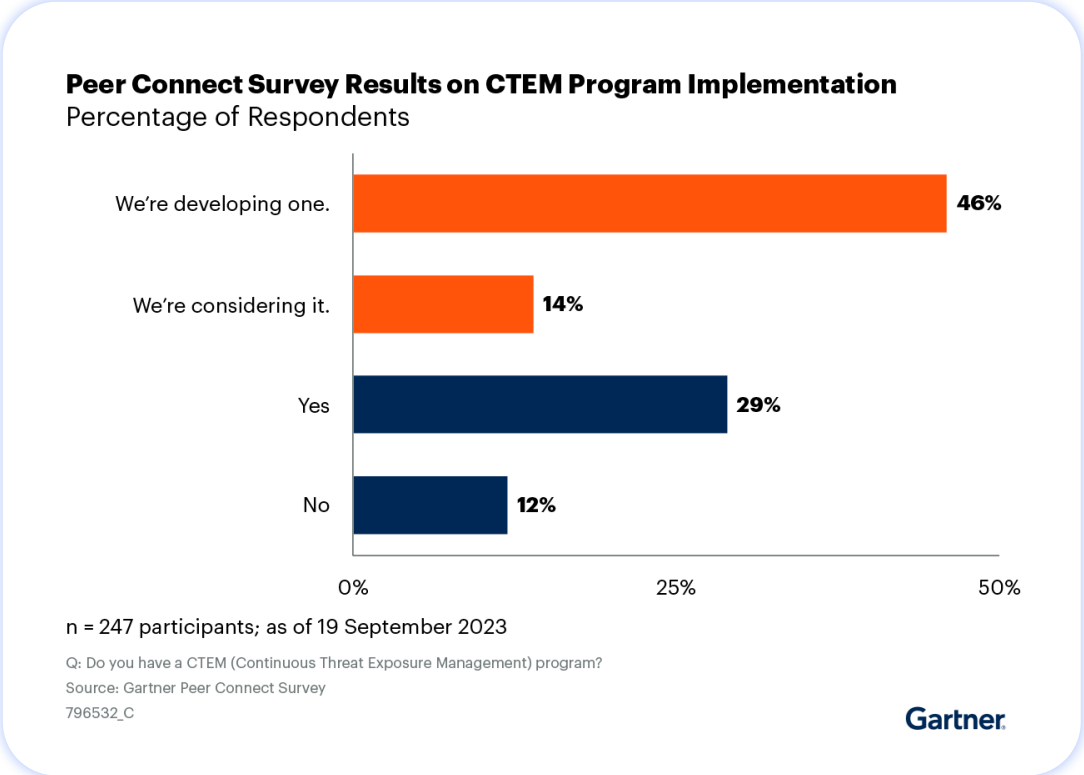
LIVRE BLANC

GESTION CONTINUE DE L'EXPOSITION AUX MENACES (CTEM) AVEC IONIX

Une approche proactive de la gestion de l'exposition utilisant la priorisation basée sur le contexte et la validation des exploits pour atténuer les risques

Ce livre blanc fournit des informations sur la manière dont les experts et les analystes du secteur envisagent d'adopter une approche plus globale et proactive pour gérer les expositions à la cybersécurité. Nous expliquons comment un nouveau cadre connu sous l'appellation CTEM – Continuous Threat Exposure Management – peut répondre au besoin d'une meilleure sécurité. Nous abordons également la manière dont les clients d'IONIX passent d'une approche réactive à une approche proactive en identifiant, évaluant et atténuant en permanence les menaces potentielles.

Votre entreprise envisage-t-elle une approche CTEM ? D'après les données de l'enquête Gartner ci-dessous, il semble que beaucoup envisagent de passer à une gestion proactive de l'exposition. Ce livre blanc vous aidera à comprendre comment aborder la CTEM de manière que votre équipe puisse la mettre en œuvre efficacement.



LA LACUNE DE LA SURFACE D'ATTAQUE

Dans le paysage numérique actuel, les entreprises sont confrontées à un nombre croissant de cybermenaces sophistiquées. La surface d'attaque s'étend et devient plus difficile à gérer, les recherches d'ESG indiquant une fluctuation mensuelle de 5,5 %. Les équipes, les outils et les processus de sécurité deviennent également de plus en plus complexes, créant des lacunes en matière de couverture. Comment les entreprises performantes gèrent-elles leur exposition à la surface d'attaque et prennent-elles le contrôle des outils et des processus ? Plusieurs raisons principales expliquent cet lacune :

1

SURFACE D'ATTAQUE ÉLARGIE

Les nouvelles technologies comme le cloud computing et l'IoT, ainsi que les tendances comme la transformation numérique, ont considérablement augmenté les surfaces d'attaque des organisations.

2

DES MENACES QUI CHANGENT RAPIDEMENT

De nouvelles vulnérabilités, méthodes d'attaque et exploits zero-day apparaissent fréquemment, introduisant de nouveaux types de risques, rendant de plus en plus difficile la défense contre les cybermenaces.

3

MANQUE DE CONSCIENCE CONTEXTUELLE

Les outils traditionnels se concentrent sur la découverte des vulnérabilités, mais manquent de contexte global de risque et d'impact sur l'entreprise, ce qui empêche les équipes de sécurité de hiérarchiser les activités en fonction des risques réels.

4

DES ATTAQUES PLUS SOPHISTIQUÉES

Les cyberattaquants adoptent de nouveaux outils et technologies, leur permettant de mener des attaques sophistiquées qui exploitent les angles morts des organisations, causant des dommages importants.

5

VUE DE L'INTÉRIEUR VERS L'EXTÉRIEUR

Les outils de cybersécurité visent à protéger les actifs détenus et gérés par l'organisation. Avec la prolifération des applications cloud et gérées par des fournisseurs, les entreprises constatent qu'en fait, un pourcentage important de leur surface d'attaque est constitué d'actifs connectés à Internet qu'elles ne possèdent pas ou ne gèrent pas elles-mêmes.

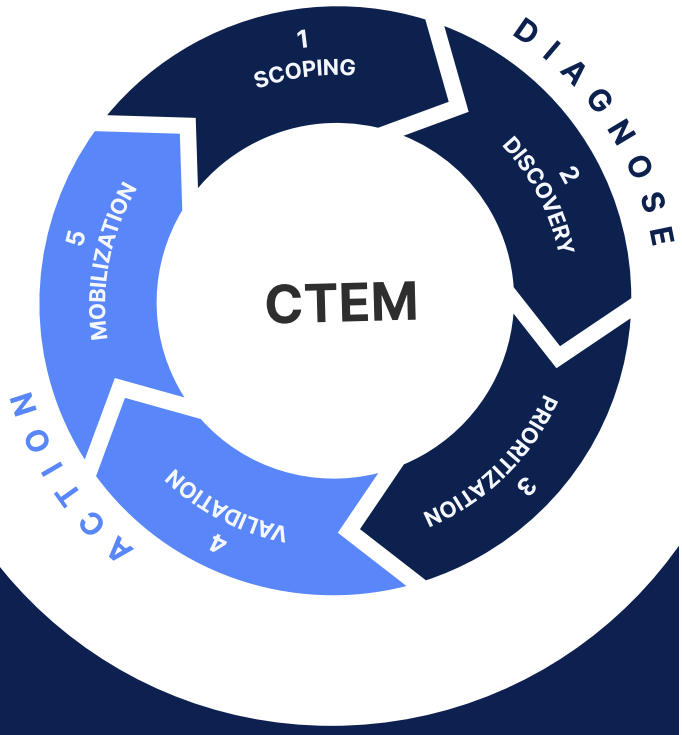
Les outils traditionnels se concentrent sur la découverte des vulnérabilités, mais manquent de contexte global de risque et d'impact pour l'entreprise, empêchant les équipes de sécurité de hiérarchiser les activités en fonction des risques réels.

Une nouvelle approche est nécessaire.

À mesure que les défis mentionnés ci-dessus s'intensifient, les organisations se rendent compte qu'elles adoptent une approche tactique réactive pour gérer leur exposition aux risques. Elles doivent plutôt aligner leurs équipes, leurs outils et leurs processus sur un cadre qui permette de hiérarchiser et d'atténuer les risques de manière beaucoup plus globale.

QU'EST-CE QUE LA CTEM?

Pour aider les entreprises à identifier, hiérarchiser et traiter systématiquement les risques de sécurité, améliorant ainsi leur posture globale de sécurité, Gartner a introduit le cadre de gestion continue de l'exposition aux menaces (CTEM). Contrairement aux catégories Gartner classiques définies par des outils logiciels dans un domaine de pratique donné, le CTEM est un cadre qui englobe de nombreux outils et processus cybernétiques disparates. Idéalement, un programme CTEM permet de passer de mesures réactives à un processus proactif et continu d'identification et d'atténuation des risques de sécurité potentiels. Ce cadre complet comprend cinq étapes clés : la définition de la portée, la découverte, la priorisation, la validation et la mobilisation.



1. PORTEE

Définit les limites de la surface d'attaque d'une organisation. Elle représente une vue complète des actifs numériques, y compris l'infrastructure traditionnelle et les ressources cloud. Elle reflète les opérations commerciales critiques et le paysage des risques de l'organisation, fournissant le contexte de la gestion continue de l'exposition aux menaces.

2. DECOUVERTE

Identifie et répertorie les actifs dans le périmètre défini, en créant des profils de risque complets qui intègrent vulnérabilités potentielles, expositions et posture de sécurité. Cela permet la prise de décision basée sur les risques dans les étapes ultérieures.

3. PRIORISATION

Prioriser les expositions en fonction de l'urgence, de la gravité, des contrôles existants et du risque global pour l'organisation, cette approche se concentre sur les actifs de grande valeur et les systèmes commerciaux critiques, fournissant une justification claire des décisions de priorisation.

4. VALIDATION

Confirme que les attaquants peuvent exploiter les vulnérabilités et évalue la réponse du système à de telles attaques. Cette validation implique des simulations automatisées ainsi que des évaluations manuelles. Elle permet de comprendre le risque réel et de vérifier l'efficacité et la faisabilité des mesures correctives suggérées.

5. MOBILISATION

Veille à ce que les équipes de sécurité mettent en œuvre efficacement les résultats des étapes précédentes en définissant des normes de communication et en établissant des flux de travail d'approbation inter-équipes documentés, qui incluent l'approbation, les processus de mise en œuvre et les déploiements d'atténuation.

L'ASM est un bon point de départ pour le CTEM

Alors, si nous voulons lancer un programme CTEM, par où commencer ? Les outils de gestion de la surface d'attaque ont explosé en termes d'utilisation et de popularité au cours des cinq dernières années. La plupart des entreprises qui ont mis en œuvre ASM, ou souvent EASM (outils axés sur les actifs externes) dans le cadre de leurs outils cybernétiques, l'utilisent pour s'assurer que leurs actifs connectés à Internet ont été scannés et inventoriés. Cependant, ces dernières années, ASM a considérablement évolué et représente désormais un endroit idéal pour démarrer un programme CTEM. Voici les caractéristiques des programmes ASM matures :

UNE PORTÉE PLUS ÉTROITE AVEC UN IMPACT SIGNIFICATIF

L'EASM se concentre sur les actifs externes d'une organisation. Cela offre une portée relativement étroite, ce qui permet aux organisations de démarrer plus facilement leur parcours CTEM. Malgré son objectif plus restreint, la gestion de la surface d'attaque externe est cruciale car elle constitue le principal point d'entrée de nombreuses cybermenaces.

VISIBILITÉ DU POINT DE VUE DE L'ATTAQUANT

L'EASM permet de comprendre comment un attaquant perçoit l'organisation de l'extérieur. En comprenant et en gérant la surface d'attaque externe, les organisations peuvent traiter de manière proactive les vulnérabilités et les erreurs de configuration avant qu'elles ne soient exploitées par les acteurs malveillants.

TEMPS DE VALORISATION RAPIDE

Les outils EASM fonctionnent de l'extérieur, de manière non intrusive. Ils détectent et exposent en permanence les risques sur les actifs connectés à Internet des organisations et sur leurs chaînes d'approvisionnement numériques. En réduisant de manière proactive leur surface d'attaque externe, les équipes de sécurité peuvent rapidement démontrer la valeur du programme CTEM aux parties prenantes. Cela peut aider à obtenir l'adhésion à une expansion et à des investissements supplémentaires dans le programme.

FONDAMENTALE POUR UNE EXPANSION ULTÉRIEURE

EASM aide les organisations à briser les silos de sécurité en fournissant une vue holistique de leurs environnements informatiques hybrides sur site et cross-cloud. En commençant par EASM, les organisations peuvent établir des processus, des flux de travail et des mécanismes de collaboration fondamentaux. Une fois ceux-ci en place, il devient plus facile d'étendre le programme CTEM pour inclure d'autres domaines.

S'ALIGNE AVEC LA TRANSFORMATION NUMÉRIQUE

À mesure que les entreprises adoptent de plus en plus de services cloud, de plateformes en ligne et d'interfaces numériques pour leurs opérations, la surface d'attaque externe devient encore plus critique. EASM s'aligne sur les tendances de la transformation numérique, garantissant qu'à mesure que les entreprises évoluent, elles disposent des contrôles de sécurité nécessaires pour faire évoluer en permanence leur posture de sécurité.

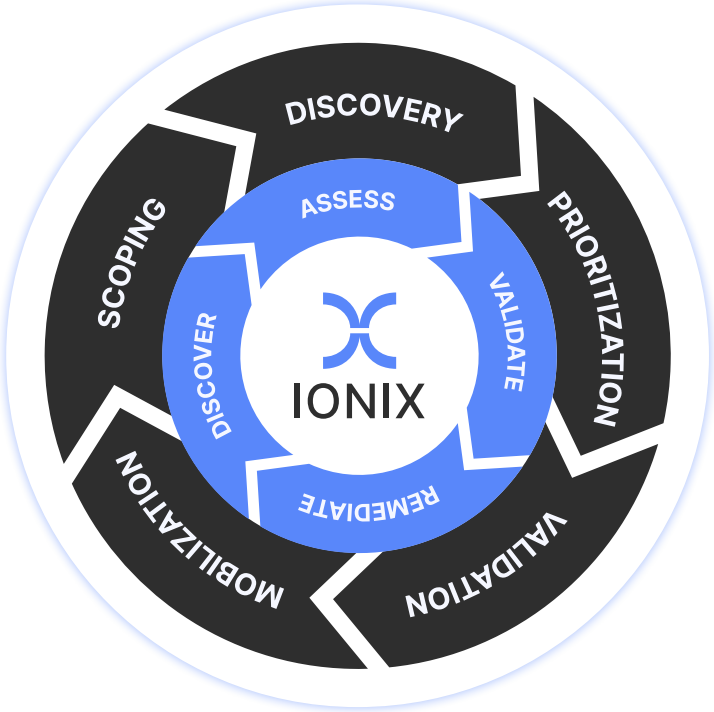
En adoptant l'EASM comme premier cas d'utilisation pour la CTEM, les entreprises peuvent briser les silos de sécurité et obtenir une vue globale de leur surface d'attaque du point de vue des attaquants. Il s'agit d'un point de départ pratique qui offre une valeur immédiate tout en ouvrant la voie à une stratégie CTEM plus complète.

ADRESSAGE DU CTEM AVEC IONIX

IONIX ASM aide les entreprises à comprendre le contexte commercial des expositions, garantissant une stratégie de défense plus complète et proactive, améliorant ainsi la posture globale de cybersécurité et protégeant les actifs critiques.

Considérez l'illustration ci-dessous pour comprendre comment IONIX considère à la fois ASM et CTEM comme un « continuum de sécurité proactive ». Il y a cinq ans, ASM était utilisé uniquement pour la visibilité des actifs, la création d'inventaires d'actifs et l'évaluation des risques potentiels. À mesure que le marché s'est consolidé, certains ont conservé leur vision désuète de l'ASM. Aujourd'hui, nous constatons que la découverte et l'évaluation des actifs ne sont que la première étape d'un programme de sécurité proactif qui comprend la priorisation des résultats, la validation des exploits et bien sûr la correction.

« Si l'on prend conscience que le nombre d'actifs et de vulnérabilités découverts n'est pas une réussite en soi, une évaluation précise basée sur le risque commercial et l'impact potentiel est bien plus précieuse. »
(Gartner)



1 PORTÉE

Pour identifier efficacement l'impact sur l'entreprise lors de la phase de définition de la portée, il est essentiel de se concentrer sur la couverture la plus large possible. IONIX crée une portée plus large que d'autres approches en incluant les actifs organisationnels (à la fois dans le cloud et sur site), les actifs gérés par les fournisseurs, les actifs tiers comme les services SaaS et même les actifs connectés à ces tiers que nous appelons la « chaîne d'approvisionnement numérique ». En se concentrant sur une portée beaucoup plus large, IONIX garantit une compréhension complète et adaptée à l'entreprise de la surface d'attaque.

2 DECOUVERTE

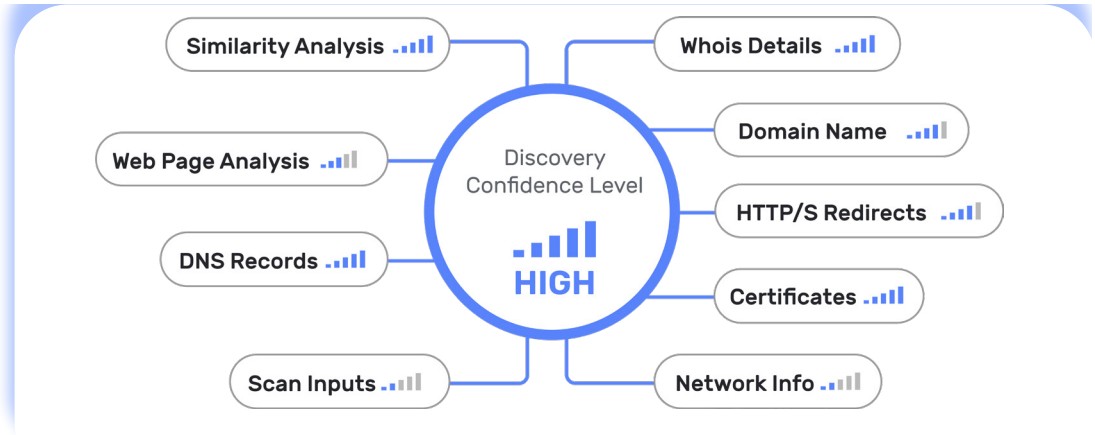
Le moteur de découverte multicouche d'IONIX utilise des algorithmes d'intelligence connective et d'apprentissage automatique dans neuf méthodes de découverte distinctes, ce qui lui permet de découvrir jusqu'à 50 % d'actifs organisationnels en plus par rapport aux approches traditionnelles.
Il implique l'identification et le catalogage de tous les actifs, y compris les actifs numériques, les ressources cloud, l'infrastructure sur site, les appareils IoT, les connexions tierces et bien plus encore.

Les techniques d'attribution avancées de la plateforme minimisent les faux positifs, garantissant ainsi une identification précise des actifs. Ce processus continu et adaptatif s'adapte à l'évolution de l'empreinte numérique d'une organisation, améliorant constamment les capacités de découverte en s'appuyant sur les résultats antérieurs et en intégrant de nouvelles données.

L'une des fonctionnalités clés d'IONIX Discovery est sa fonction Discovery Evidence, qui offre une visibilité claire et compréhensible sur le processus complexe de collecte et d'attribution des preuves. Discovery Evidence détaille les informations spécifiques collectées pour chaque actif et leur contribution à la détermination de l'appartenance de l'actif à l'organisation. Les preuves sont présentées en relation avec les mots-clés utilisés lors de la phase de définition de la portée (tels que les noms d'entreprise, les marques ou les entités juridiques) et sont comparées entre les différentes méthodes de découverte employées par la plateforme.

IONIX comble également les failles de sécurité, en offrant une visibilité et des informations complètes sur les environnements AWS, Azure et GCP, en identifiant non seulement les actifs mais aussi le réseau complexe d'interconnexions qui pourraient potentiellement être exploitées. Cette approche transcende les limites des outils de gestion de posture comme CSPM en intégrant une vue plus large qui inclut les expositions involontaires à Internet et les vulnérabilités de la chaîne d'approvisionnement numérique.

En adoptant EASM comme premier cas d'utilisation pour CTEM, les entreprises peuvent briser les silos de sécurité et obtenir une vue holistique de leur surface d'attaque du point de vue des attaquants.

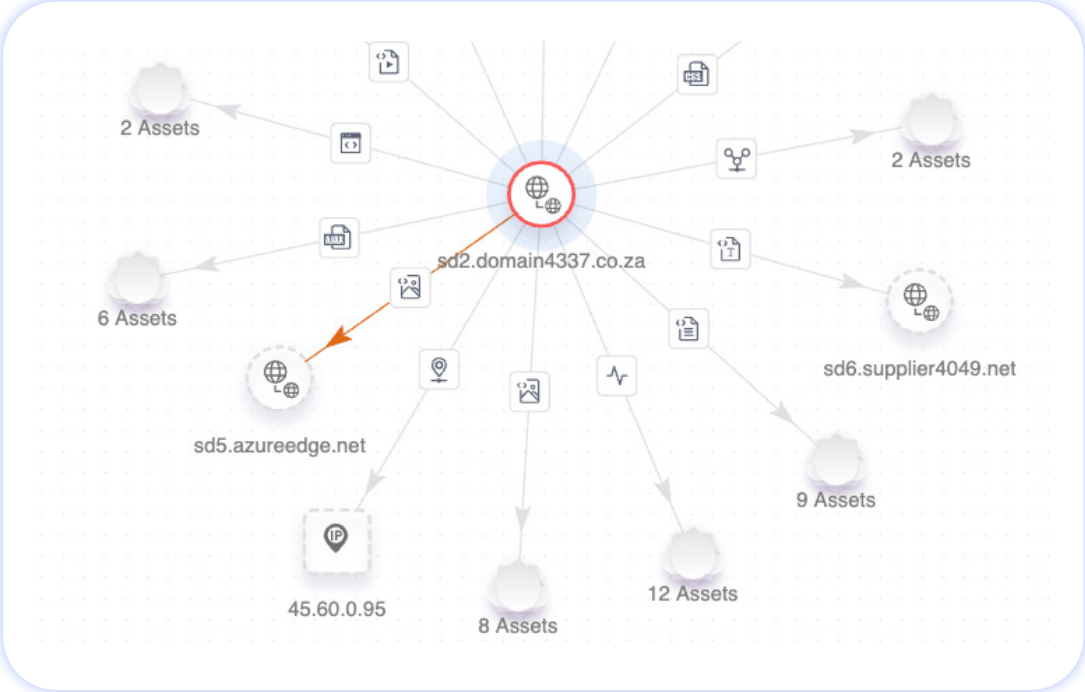


L'approche globale d'IONIX permet aux organisations de maintenir un inventaire précis et à jour de leur surface d'attaque, de comprendre le raisonnement derrière les attributions d'actifs et de prendre des décisions éclairées sur leur posture de cybersécurité. En fournissant ce niveau de détail et de transparence, IONIX offre une précision avec un taux extrêmement faible de faux positifs.

3 PRIORISATION

La nouvelle approche d'IONIX en matière de cartographie des chemins d'attaque repose sur une compréhension des interdépendances entre les actifs organisationnels et de l'impact de chaque actif sur les autres actifs. Nous appelons cela « Connective Intelligence ».
Connective Intelligence suggère que la posture de sécurité et le risque d'un actif donné ne dépendent pas seulement de l'hygiène et de la posture de sécurité de l'actif lui-même, mais également de la posture de sécurité des actifs dont il dépend, directement et indirectement (2e, 3e à Ne degré).

Contrairement à d'autres approches de cartographie des chemins d'attaque, l'approche d'IONIX cartographie les dépendances réelles, plutôt que théoriques, dont l'exploitabilité a été validée. La connectivité et les dépendances sont vérifiées et validées pour aider les clients à comprendre les risques qu'elles entraînent.



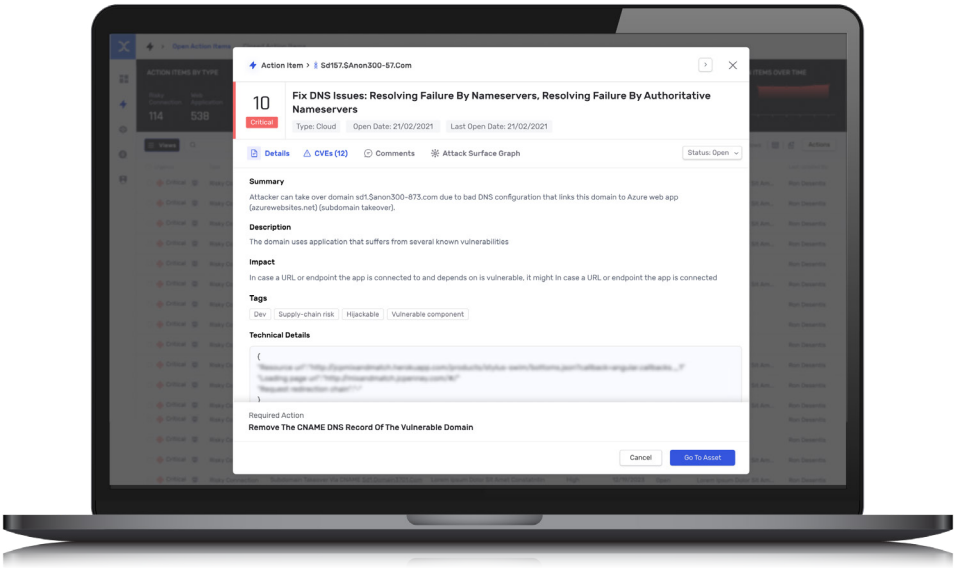
Connective Intelligence de IONIX amène la gestion de la surface d'attaque à un niveau supérieur en prenant en compte non seulement les actifs discrets sur la surface d'attaque, mais également en mettant en évidence les risques introduits par les actifs connectés. De plus, Connective Intelligence permet de prendre en compte non seulement les actifs externes détenus ou contrôlés par l'organisation, mais également tous les actifs tiers qui constituent la chaîne d'approvisionnement numérique.

4 VALIDATION

IONIX Exposure Validation exploite une boîte à outils de techniques de simulation d'attaques pour effectuer des tests non intrusifs de vos systèmes, en identifiant les expositions sans risque de perturbation. Notre approche valide l'exploitabilité dans le monde réel, garantissant que les équipes de sécurité peuvent se concentrer sur les menaces les plus importantes pour votre entreprise. Les principales caractéristiques d'IONIX Exposure Validation incluent :

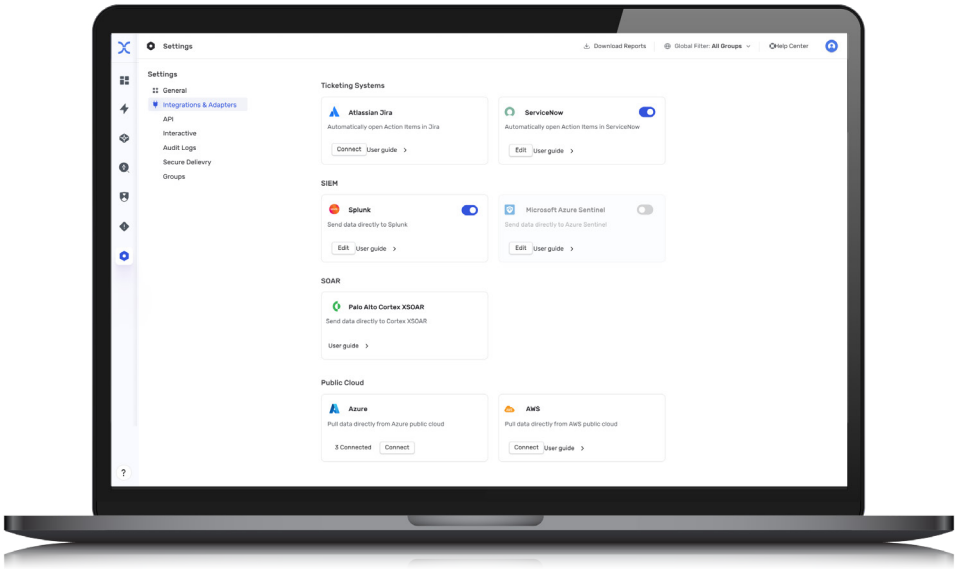
• des techniques de test non intrusives : conçues pour valider en toute sécurité les contrôles de sécurité dans les systèmes opérationnels sans affecter leur fonctionnalité ou leurs performances.
• l' identification des risques exploitables : identification des vulnérabilités qui représentent une menace réelle pour votre organisation, afin que vos équipes de sécurité puissent accélérer la correction et réduire efficacement les risques.
• le validation automatisée : tests de sécurité continus qui s'adaptent à l'évolution du paysage des menaces et aux changements organisationnels, garantissant que vos défenses restent robustes au fil du temps.
• l'automatisation et l'efficacité : réduction du besoin de tests manuels approfondis, gain de temps et de ressources tout en améliorant votre posture de sécurité.

Les capacités de gestion continue et adaptative des menaces d'IONIX aident les organisations à garder une longueur d'avance sur les menaces émergentes, réduisant ainsi l'exposition et les dommages potentiels.



5 MOBILISATION

L'essentiel de cette étape est de s'assurer que les risques sont traités et acheminés vers les équipes compétentes pour gérer et appliquer les mesures correctives nécessaires. 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 pour faciliter la résolution rapide des problèmes critiques.
Ces intégrations permettent aux organisations d'optimiser leurs activités concernant les risques associés en facilitant une communication et une harmonisation efficaces entre les équipes de sécurité et les autres parties prenantes de l'organisation.



IONIX a également développé deux fonctionnalités essentielles qui permettent aux clients de remédier rapidement aux problèmes : les éléments d'action et la protection active. Un aspect clé d'une correction efficace consiste à créer des éléments d'action robustes qui peuvent regrouper et résoudre plusieurs problèmes à la fois. Grâce à Connective Intelligence, IONIX peut détecter qu'une vulnérabilité détectée sur plusieurs actifs (applications, sites Web, services) provient d'un seul actif, créant ainsi un seul élément d'action, plutôt que plusieurs éléments d'action, un pour chaque actif vulnérable.

IONIX est le seul fournisseur de solutions EM à proposer une fonctionnalité appelée « Protection active » qui prévient immédiatement les menaces à haut risque auxquelles les entreprises ne peuvent pas faire face autrement, sans intervention humaine. La protection active peut identifier les erreurs de configuration liées à la chaîne d'approvisionnement numérique et neutraliser automatiquement ces menaces en prenant essentiellement le contrôle de l'actif jusqu'à ce qu'une organisation puisse mettre en œuvre une correction sur l'actif.

Avec IONIX, les entreprises peuvent gérer efficacement leurs filiales et autres structures organisationnelles complexes à l'aide d'une plateforme centralisée unique. Notre solution permet une attribution automatisée des entités commerciales combinée à un partitionnement des accès. Elle permet aux équipes locales de gérer efficacement leur surface d'attaque tout en permettant aux SOC centralisés de mettre en œuvre des normes de sécurité à l'échelle de l'organisation. Chaque filiale peut avoir sa propre équipe de sécurité avec un RBAC dédié, tandis que les services de sécurité de l'organisation mondiale peuvent suivre l'exposition aux risques et les mesures à prendre dans toutes les filiales.

« La gestion des expositions (EM) est une plateforme qui consolide les vulnérabilités et les expositions dans une perspective organisationnelle, les cartographie sur un chemin d'attaque et identifie les points d'étranglement que les équipes de correction doivent prioriser. » Eric Nost, Forrester

PAS SEULEMENT GARTNER

Les analystes définissent la gestion des expositions (EM) de différentes manières. Eric Nost, analyste chez Forrester, la décrit comme une plateforme qui consolide les vulnérabilités et les expositions d'un point de vue organisationnel, les cartographie sur un chemin d'attaque et identifie les priorités de correction. Comme Gartner, Nost considère la gestion des expositions comme une approche holistique de découverte, de hiérarchisation, de cartographie et de correction des expositions. Cependant, il souligne l'importance de rendre opérationnelle la correction pour simplifier les flux de travail des analystes de sécurité.

La mise en œuvre de CTEM ou EM permet aux entreprises d'évaluer en permanence leur surface d'attaque, d'identifier les vulnérabilités et de traiter les expositions critiques en temps réel. Cette approche aide les organisations à garder une longueur d'avance sur les menaces émergentes, à réduire le risque global et à maintenir une sécurité robuste.

RESUMÉ

IIONIX aide à la mise en œuvre du CTEM en proposant des solutions adaptées à chaque étape d'un programme CTEM, y compris la définition de la portée, la découverte, la priorisation, la validation.
et la mobilisation.

1. Visibilité complète des actifs : IONIX garantit qu'aucun actif critique ne soit négligé, offrant une vue complète de la surface d'attaque de l'organisation, essentielle pour une gestion efficace de l'exposition.

2. Priorisation précise des risques : en minimisant les faux positifs et en validant les expositions suspectes, IONIX aide les organisations à se concentrer sur les véritables menaces, en dirigeant les ressources de sécurité vers les risques les plus importants.

3. Approche orientée entreprise : en intégrant le contexte de l'entreprise dans la définition de la portée et les évaluations des risques, IONIX garantit que les mesures de sécurité s'alignent sur les priorités de l'entreprise protégeant ainsi les fonctions critiques.

4. Gestion proactive des menaces : les capacités de gestion continue et adaptative des menaces d'IONIX permettent aux organisations de garder une longueur d'avance sur les menaces émergentes, réduisant ainsi l'exposition et les dommages potentiels.

5. Tâches opérationnelles simplifiées : en aidant les équipes de sécurité à gérer les risques par filiale, en regroupant les recommandations de correction en éléments d'action et en intégrant les outils de gestion SOC les plus populaires, IONIX fournit un support opérationnel supérieur.

IONIX garantit que les organisations peuvent mettre en œuvre CTEM de manière efficace, en obtenant des défenses de cybersécurité robustes et adaptées à l'entreprise qui protègent les actifs critiques et maintiennent l'intégrité opérationnelle. Contactez-nous pour une démonstration dès aujourd'hui !

Demandez un scan ICI

Ionix est représenté en France par AMC SOFT
https://amcsoft.fr - contact@amcsoft.fr
Learn more at ionix.io