Ambionics Uncovery

Cartographiez en continu votre surface d'attaque et éliminez vos angles morts

OBJECTIF

Identifiez les actifs exposés, l'informatique non référencé et les dérives de configuration avant qu'ils ne deviennent des points d'entrées pour un attaquant.

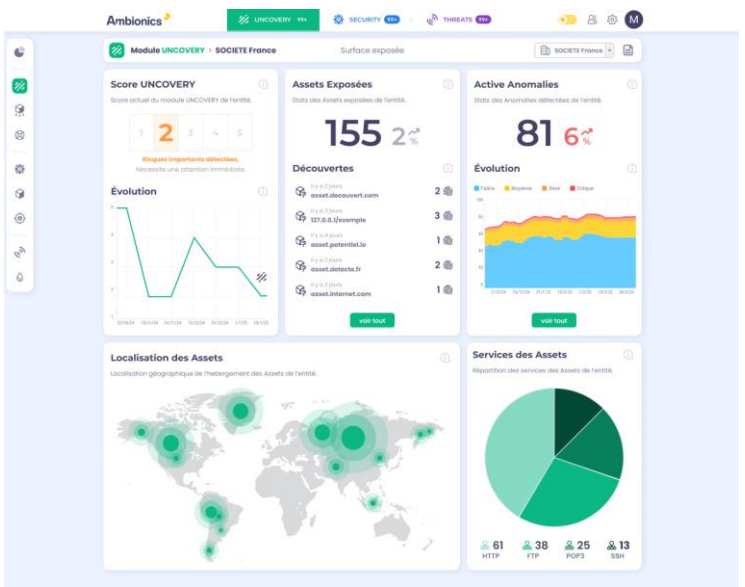
Un module de cartographie de la surface externe pour identifier et surveiller vos actifs sur Internet

→ **Cartographier votre surface d'exposition :** Identifier l'ensemble de votre surface d'exposition externe grâce à un inventaire précis, à jour et sans faux positifs

→ **Consolider les actifs légitimes et illégitimes :** sites web non déclarés, interfaces d'administration, équipements connectés, etc...

→ **Détecter vos actifs non référencés**

→ **Révéler des anomalies :** Analyse de l'exposition via des modules spécialisés & **Suivre un plan de remédiation** pour des actions correctives rapides



CAS CONCRET

Maitrise de l'informatique non référencé

CONTEXTE

Un groupe multisite découvre que plusieurs actifs exposés sur Internet ne figurent dans aucun inventaire centralisé. Entre filiales, prestataires et projets métiers, des sous-domaines, interfaces d'administration et services web restent visibles sans pilotage clair.

MISSION

Le module Uncovery cartographie en continu l'ensemble de la surface exposée du groupe, identifie les actifs inconnus, détecte les anomalies d'exposition et suit les évolutions techniques dans le temps depuis un portail centralisé.

VALEUR

En quelques semaines, l'organisation récupère une vision consolidée de ses actifs exposés, réduit significativement son informatique non référencée et priorise rapidement les actions de remédiation sur les actifs les plus critiques.

Pourquoi choisir notre solution Ambionics Uncovery ?

→ Une solution unique intégrant cartographie de la surface externe, tests d'intrusion en continu et renseignement sur les menaces cyber

→ L' expertise de LEXFO est française et reconnue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au travers de plusieurs qualifications.

→ Une équipe dédiée de +50 pentesters pour vous accompagner

Ambionics Security

Validez la sécurité réelle de vos applications avec des tests d’intrusion continus orientés exploitation

OBJECTIF

Identifier, qualifier et rejouer les vulnérabilités exploitables pour piloter une réduction durable de votre exposition cyber.

Capacités clés

→ **Scans qualifiés & zéro faux positif :** Validation humaine systématique des vulnérabilités découvertes par nos propres scanners

→ **Pentests continus & ciblés :** Audits manuels réguliers combinés à une recherche continue des failles applicatives

→ **Anticipation des vulnérabilités inconnues :** Surveillance active et vérification prioritaires des menaces émergentes critiques sur vos actifs

→ **Contre-audit hebdomadaire :** Les vulnérabilités sont rejouées chaque semaine pour garantir la correction et l’absence de régression

CAS CONCRET

Sécurisation continue des applications web

CONTEXTE

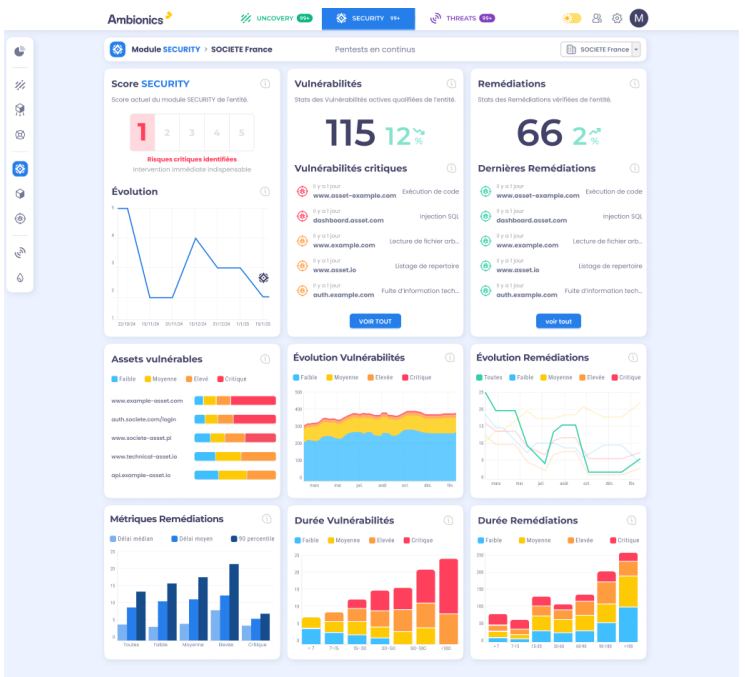
Les mises à jour applicatives fréquentes rendent les audits annuels insuffisants, laissant l'organisation aveugle face aux vulnérabilités nouvellement introduites ou émergentes.

MISSION

Déploiement d'une démarche de tests d’intrusion en continu : scans automatisés réguliers qualifiés (zéro faux positif), tests d’intrusion boîte grise en continu et détection proactive des menaces critiques.

VALEUR

Les équipes obtiennent des alertes fiables et immédiatement actionnables. Chaque vulnérabilité est rejouée chaque semaine afin de valider la correction et de prévenir la régression, assurant une réduction durable du risque.



Pourquoi choisir notre solution Ambionics Security ?

→ Une solution unique intégrant cartographie, tests d’intrusion en continu et cartographie de la menace

→ L’ expertise de LEXFO est française et reconnue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au travers de plusieurs qualifications.

→ Une équipe dédiée de +50 auditeurs pour vous accompagner

Ambionics Threats

Détectez vos fuites de données sensibles

OBJECTIF

Détectez vos fuites de données sensibles et surveillez les menaces qui ciblent votre entité.

Capacités clés

→ **Surveillez 24h/24, 7j/7** l'ensemble des sources internet pour détecter les menaces émergentes contre votre entreprise : Internet clandestin, forums spécialisés, plateformes d'achat

→ Bénéficiez **d'une combinaison d'outils automatisés et d'experts** pour valider et analyser tout signal faible et élément suspect

→ **Intégrez cette veille a vos processus internes pour renforcer la détection de fuites** et accélérer la prise de décision dans la lutte contre les cybermenaces et la fraude

→ **Personnalisez la recherche par mots-clés** pour cibler précisément les données sensibles liées à votre secteur ou à vos technologies

CAS CONCRET

Veille continue sur les fuites de données

CONTEXTE

Face à l'explosion des fuites de données et des cybermenaces, la surveillance proactive de l'image numérique est devenue un enjeu de résilience critique pour les organisations.

MISSION

Mise en place d'une veille sur toutes les couches d'Internet sur 150 mots-clés et d'une protection anti-défiguration pour 40 sites Internet avec alertes en temps réel.

VALEUR

Fiabilisation des alertes par analyse humaine (zéro faux positif) et capacité d'investigation directe auprès des acteurs malveillants pour qualifier précisément les risques