DOSSIER DE PRESSE

Patrowl

FASTER THAN ATTACKERS

Identifier et renforcer la posture de sécurité externe

Se concentrer sur la remédiation

Éliminer les tâches chronophages et source d'erreurs

QUI EST PATROWL ?

Fondée en 2020, la société Patrowl est un éditeur français leader de la sécurité offensive, du test d'intrusion automatisé et de la gestion continue de l'exposition aux menaces.

identifie les vulnérabilités (connues, référencées et inconnues) type OWASP (PTaaS et CART)

Patrowl cartographie (EASM) **les actifs exposés sur internet** (applications, site web, accès distants, Cloud, etc.)

propose un plan de remédiation et les moyens de contrôler l'exécution des corrections

Développée par 3 spécialistes de la cybersécurité, Patrowl est accessible à des utilisateurs non experts et leur permet d'élever rapidement le niveau de sécurité de leur système d'information. Patrowl s'adresse en priorité aux ETI et aux grands comptes, tous secteurs confondus.

SON HISTOIRE

Le concept Patrowl voit le jour à l'occasion de l'audit d'un site e-commerce. Alors qu'aucune vulnérabilité n'est détectée, le site fait l'objet d'une attaque quelques semaines plus tard. L'analyse révèle qu'une nouvelle fonctionnalité de commentaires ajoutée après l'audit est en cause.

La démonstration était faite : les processus sécurité traditionnels ne sont plus adaptés au rythme élevé d'évolution des produits numériques. Trop rares, limités à une cartographie circonscrite à un instant T, les tests d'intrusion sont inefficaces dans le temps. Quelques mois après, l'association d'une surveillance en continu à un système d'automatisation à grande échelle donnait naissance à la solution de sécurité offensive Patrowl.

SES FONDATEURS

Nicolas MATTIOCCO - Président, Security Expert
Vladimir KOLLA - Directeur général, Security Expert
Florent MONTEL - Directeur général, Security Expert

PRIX, RECONNAISSANCE ET RÉFÉRENCEMENTS

En 2022 : Patrowl est lauréat du Prix du Public à l'occasion des Assises de la Cybersécurité.

Patrowl entre dans le radar des startups prometteuses de Wavestone et au catalogue GouvTech.

En 2023 : Patrowl remporte les Prix de l'Innovation des Assises de la Cybersécurité du jury et du public.

En 2024 : Patrowl dépasse les 700 000 actifs surveillés et participe à la rédaction du Livre Blanc 2024 sur la gestion des vulnérabilités dans le cadre du Campus Cyber.

Patrowl est référencé aux catalogues CAIH et RESAH à destination des établissements de santé.

Patrowl remporte le trophée FinTech de l'innovation de la Banque Postale Asset Management.

Patrowl est lauréat France 2030 du concours d'innovation i-Nov "Automatisation des tests d'intrusion".

En 2025 : Patrowl est lauréat du grand prix de la startup du Forum InCyber (FIC).

Le radar Wavestone ajoute Patrowl au classement des scale-ups.

FINANCEMENTS

Patrowl boucle sa première levée de fonds de 2 millions € en 2022, et réalise en 2024 une levée de fonds série A de 11 millions € menée par Crédit Mutuel Innovation, Swen Capital Partners, Bpifrance et Auriga Cyber Ventures.

PERSPECTIVES

En recrutement continu (47 collaborateurs à ce jour), Patrowl déploie une roadmap 2025-2026 riche de nouvelles fonctionnalités, en réponse aux retours d'expérience et suggestions de ses clients avec lesquels l'éditeur coopère régulièrement.

LA SOLUTION

Patrowl est une solution de sécurité offensive qui opère des tests d'intrusion automatisés et la gestion continue de l'exposition aux menaces.

UNIQUE SUR LE MARCHÉ EUROPÉEN, PATROWL SE DÉCLINE SELON 3 NIVEAUX DE MATURITÉ CYBER :

NIVEAU 1

La (re)decouverte en continu de tous les actifs exposés sur Internet constitue le socle fondamental du pilotage et de la gestion des risques.

NIVEAU 2

L'advanced EASM qualifie et organise les risques liés au contexte et aux technologies en place, en référence à la PSSI élaborée dans l'organisation.

NIVEAU 3

La technologie de pentests automatisés et en continu recherche les vulnérabilités susceptibles de compromettre les SI, les données et la réputation.

« Nous avons été rapidement convaincus de la pertinence de la solution Patrowl. Elle répond très précisément à deux vraies problématiques d'entreprise : elle nous assure de l'absence de toute erreur humaine, de configuration notamment, et veille à ce que nous n'exposions que le strict nécessaire, sans inonder les services IT d'un flot de données difficiles à exploiter. » **MGEN**

« Grâce à Patrowl, nous sommes passés de tests d'intrusion qui nous prenaient énormément de temps à des rapports clairs et vérifiés que nos ingénieurs peuvent corriger immédiatement. Cela nous fait gagner du temps, de l'argent et nous évite des maux de tête. » **Xplor**

Patrowl ne nécessite pas de temps de configuration ni de compétences spécifiques en interne. D'un usage très accessible, Patrowl permet d'élever rapidement le niveau de cybersécurité et de réduire les risques.

« L'implémentation du test relatif à la vulnérabilité SharePoint (CVE 2025 53770) s'est avérée pleinement opérationnelle : notre Blue Team a été immédiatement alertée. Nous avons reçu la notification préventive concernant le nouveau test Patrowl à 15h57 et, dès 16h36, une alerte était déclenchée. » **Brest Métropole**

Les changements constants (SCRUM, Agile, DevOps,etc.) et la mutation des systèmes d'information (5G, travail à distance, Cloud, SaaS, Shadow IT notamment) entrainent une perte de visibilité et de contrôle. **Patrowl alerte les équipes en temps réel sur les vulnérabilités et les menaces** connues et détectées et décèle le Shadow IT et les sites web de phishing utilisant la marque de l'entreprise.

LA SOLUTION

« Nous faisions traditionnellement des tests d'intrusion, mais leur principal inconvénient est d'être obsolètes dès le lendemain de la remise du rapport. Le Pentest en continu est une solution innovante parfaitement en adéquation avec l'extrême évolutivité de l'informatique d'entreprise d'aujourd'hui. » **MGEN**

Patrowl exécute des tests d'intrusion de qualité manuelle mais étendus **sur un périmètre infini et en continu**.

« L'utilisation de la plateforme Patrowl a grandement contribué à l'amélioration de la surveillance de nos actifs exposés sur internet. Avant de l'intégrer à nos opérations, nous faisions face à des défis constants pour identifier et prioriser les failles dans notre infrastructure. Grâce à la solution Patrowl, nous avons non seulement pu automatiser cette tâche, mais également obtenir une visibilité claire et détaillée sur notre posture de sécurité. » **Arkhineo**

Patrowl propose l'hyper-automatisation des tâches de surveillance, toujours très chronophages. Les équipes peuvent enfin se concentrer sur la remédiation et les actions à forte valeur ajoutée.

« Nous sommes guidés pas à pas sur la manière de faire, avec une explication précise de l'alerte qui a été levée, de sorte que l'on peut comprendre ce qui se passe, savoir quelle application n'a pas respecté toutes les bonnes pratiques pour un service ouvert sur Internet. »

CH Avignon Technologies et Innovations hospitalières - octobre 2024

Patrowl collationne l'ensemble des vulnérabilités ayant un impact réel sur l'entreprise, qualifiées, priorisées et contextualisées puis fournit des recommandations à la remédiation pragmatiques et actionnables.

« Patrowl est d'ores et déjà aussi efficace que simple à exploiter. Depuis que nous l'utilisons, la solution donne des résultats très pertinents. » **Heetch**

Rapports exhaustifs des contrôles réalisés en 1 click, portail consolidé d'accès à l'exposition externe, au plan d'action priorisé et à l'ensemble des vulnérabilité, Patrowl supporte les organisations multi-tenant.

NETWORK AND INFORMATION SECURITY 2 (NIS2)

Patrowl est entièrement conforme aux exigences de NIS 2 en matière de tests d'intrusion en continu des actifs grâce à la Cybersécurité Offensive as-a-Service.

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Patrowl est entièrement conforme aux exigences de DORA en matière de surveillance continue des actifs grâce à la Cybersécurité Offensive as-a-Service.

RISK INSIGHT

La fonctionnalité Risk Insight présente une vue simplifiée, focalisée sur les cas d'usage métiers ou techniques les plus pertinents (certificats, applications web, mails, services non recommandés exposés, etc.), et permet de traiter les risques.

TRENDING ATTACKS

Radar continu, la fonctionnalité Trending Attacks agrège toutes les vulnérabilités, exploits publics, bulletins CERT et le catalogue CISA KEV. Chaque menace est analysée par algorithmes puis validée par des experts qui la qualifient et jugent de son exploitabilité.

CONTACTS

CONTACT PRESSE

AGENCE PORTISED – YUCATAN
Rémy Roche
Tél : +33 1 53 63 27 20
Mobile : +33 6 74 83 51 57
rroche@yucatan.fr

CONTACT PATROWL

Mobile : +33 7 68 78 46 34
press@patrowl.io

Patrowl

www.patrowl.io