RAPPORTS AUTOMATISÉS

Une nouvelle fonctionnalité qui consolide la conformité cyber des entreprises.

Patrowl

Nouvelle fonctionnalité : Patrowl consolide les preuves de conformité cyber des entreprises

Avec la livraison de rapports de surveillance externe exhaustifs, Patrowl aide les entreprises à justifier du respect des mesures de cybersécurité et à démontrer leur approche responsable à l'occasion d'audits, de contrôles ou lors de la souscription d'une police de cyberassurance.

Paris, le 15 juin 2023 — Patrowl, leader français de l'Offensive Security as-a-Service et du Pentest as-a-Service, permet désormais la livraison de rapports à la demande, portant sur la totalité des contrôles effectués sur l'ensemble des actifs exposés, et leurs résultats. Ces rapports s'inscrivent dans l'éventail de preuves exigées pour démontrer la mise en place des mesures adéquates de cybersécurité.

Patrowl : les rapports à la demande désormais disponibles

Parmi les nouvelles fonctionnalités attendues en 2023, la possibilité d'exports automatisés des rapports Patrowl est la plus plébiscitée. Dans l'objectif de fournir, notamment aux tiers, la preuve de leur couverture cybersécurité, les entreprises disposent dorénavant des rapports complets des tests d'intrusion réalisés en continu, de l'ensemble des contrôles effectués, des résultats obtenus.

Au quotidien, Patrowl effectue une analyse approfondie des failles détectées, alerte sur les plus critiques et livre ses recommandations priorisées et contextualisées. C'est pourquoi Patrowl est accessible à toutes les entreprises, quel que soit le niveau d'expertise interne.

Les rapports à la demande, quant à eux, délivrent la totalité de l'information collectée, renseignent sur le niveau d'exposition sur Internet, la solidité des actifs concernés et le rythme des contrôles opérés.

« Cette information entière et détaillée devient de plus en plus nécessaire, à de multiples occasions. Audits, polices d'assurance, respect des textes réglementaires, les rapports automatisés Patrowl apportent la preuve de l'étendue de la couverture sécurité sur Internet, mais également du degré de résilience des entreprises » explique Vladimir Kolla, co-fondateur et co-directeur général de Patrowl.

Patrowl, en phase avec DORA, NIS 2, Cyberscore et CRA

Entre 2023 et 2025, de nombreux textes européens viennent et viendront renforcer les obligations cybersécurité d'un nombre grandissant d'organisations.

Ainsi, le règlement DORA (Digital Operational Resilience Act), destiné au secteur financier, requiert notamment des contrôles permanents sur la base de Pentests et la détection continue des vulnérabilités.

La directive NIS 2, qui élargit considérablement le périmètre des entreprises concernées, impose le déploiement de tests d'intrusion et l'identification des risques et des vulnérabilités.

Enfin, la certification de cybersécurité des plateformes numériques, destinée au grand public et dénommée Cyberscore, exige l'évaluation du niveau d'exposition sur Internet, la connaissance, la maîtrise et l'audit des actifs exposés.
Points communs de ces réglementations nouvelles, la cartographie et la parfaite connaissance de la surface d'attaque externe des entreprises, tout comme la détection des vulnérabilités des actifs exposés ressortent du domaine d'action de Patrowl. Ainsi, la détection des failles éventuelles contenues dans les logiciels IoT adresse également le Cyber Resilience Act.

Plus de 30 familles de contrôles réalisés

Bases de données, gestion des authentifications, injections (Command, XSS, SQLi, XXE, etc.), fichiers critiques, réputation (blacklisting), etc., Patrowl opère au total plus d'une trentaine de familles de contrôles et fournit leurs heures d'exécution, les résultats obtenus et les vues par actif concerné et par contrôle de sécurité.
À venir au 3e trimestre 2023 : sur la base de ces Security Checks, les organisations publiques et privées pourront explorer plusieurs cas d'usage proposés par Patrowl, tels que la sécurité du mail ou des applications, ou encore la gestion des certificats. Usecases orientés métier, ces pages dédiées disponibles sur l'interface facilitent la sélection des sujets cyber à travailler.

À propos de Patrowl

Fondée en 2020, la société française Patrowl est éditrice de la solution d'Offensive Security as-a-Service éponyme qui :
– cartographie (EASM) et teste en continu (PTaaS/CART) les actifs exposés sur internet (applications, site web, accès distants, Cloud, etc.),
– identifie les faiblesses (vulnérabilités et défauts de configuration),
– propose un plan de remédiation et les moyens de contrôler l'exécution des corrections.

Patrowl est à ce jour la seule société de droit européen capable d'offrir aux entreprises, aux collectivités territoriales, aux établissements et services publics, une plateforme complète de surveillance externalisée, l'accompagnement des équipes cybersécurité à l'interprétation de la cartographie et le conseil à la remédiation de toutes les failles critiques avérées.

Développée par 3 spécialistes de la cybersécurité, la solution 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 grands comptes, tous secteurs confondus.