Patrowl veille sur l'exposition en ligne de MGEN

Début 2023, le Security Operation Center de MGEN s'est doté de la solution Patrowl afin de renforcer encore sa sécurité, de consolider la connaissance de ses actifs exposés sur Internet et de disposer d'une solution en continu de test d'intrusion. Au quotidien, la solution Patrowl est une alliée précieuse pour MGEN, très exigeante sur la protection de son système d'information.

MGEN, la solidarité à la pointe de la cyberprotection

Membre fondateur du Groupe VYV, premier acteur mutualiste de santé et de protection sociale, MGEN est un acteur majeur de la protection sociale en France. MGEN gère le régime obligatoire d'assurance maladie et la complémentaire santé et prévoyance de plus de 4,2 millions de bénéficiaires, ainsi que des établissements sanitaires et médico-sociaux, et des centres médicaux-dentaires.

Parce qu'elle assure la prise en charge des dépenses de santé et participe ainsi à l'accès aux soins, MGEN poursuit une mission d'intérêt général dont la continuité de service doit être garantie. Le programme cybersécurité de MGEN a mis en place en 2021 un Security Operation Center (SOC) à la Direction Sécurité des Systèmes d'Information, afin de renforcer sa stratégie de défense cyber.

En 2022, une équipe est créée pour gérer le SOC, sous la responsabilité de Maxime Granatini.

« *Nous étions opérationnels pour effectuer une surveillance en 24/7 de l'ensemble du SI de MGEN. Mais l'activité de la mutuelle est extrêmement dynamique. Entre les évolutions de la réglementation entraînant des modifications parfois profondes des systèmes, les innovations, les partenariats, nous avions également besoin d'une vue complète, exhaustive, aussi précise que possible de notre exposition sur Internet. Ou, dit autrement, de notre surface d'attaque externe* » explique Maxime Granatini, Responsable SOC, DSSI MGEN.

Le SOC MGEN fait le choix de Patrowl pour tous ses actifs en ligne

Tous les sujets sécurité doivent être traités. Si le phishing est un puissant vecteur d'attaque dont il faut savoir se prémunir, « *les failles dans les infrastructures externes exposées sur Internet sont exploitables à une telle vitesse que le risque est aussi grand que les tentatives d'hameçonnage. Internet est scanné tous les jours* » rappelle Maxime Granatini.

Son équipe et lui avaient donc besoin d'une solution dynamique face au risque encouru, capable d'identifier en continu l'ensemble du périmètre d'exposition, et de repérer les failles

et les vulnérabilités urgentes à corriger. « *Pour bien se protéger, il faut bien connaître sa surface d'attaque* ».

Fin 2022, la société Patrowl propose à l'équipe SOC MGEN de réaliser un POC de leur solution d'EASM et de Pentest en continu. « *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* ».

L'équipe SOC MGEN opte alors pour la solution d'EASM et de Pentest en continu de Patrowl dès janvier 2023. « *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* ».

Une surface d'attaque bien maîtrisée

Opérationnelle immédiatement, puisque sans installation prérequise, la solution Patrowl permet alors à l'équipe SOC MGEN de lister les adresses IP et domaines critiques, sur lesquels opérer du Pentest en continu (ou Pentest as a Service).

Face à un scanner de vulnérabilité traditionnel, Patrowl fait toute la différence en analysant les rapports de Pentest pour ne faire remonter au SOC que l'information utile et les recommandations de correction associées. « *Patrowl va beaucoup plus loin dans les tests d'intrusion et les analyses de ses experts nous sont très utiles* », note le responsable du Security Operation Center de MGEN.

En parallèle, les membres du SOC ont pu rapidement détecter la part de shadow IT soupçonnée. « *Il s'agit généralement de sites partenaires, sur lesquels nous n'exerçons pas de responsabilités particulières, mais que nous devons connaître pour pouvoir alerter* », précise Maxime Granatini. L'EASM permet à l'équipe SOC d'organiser et de maîtriser la surface exposée, d'en connaître tous les aspects et les localisations. « *Patrowl permet de tout mettre à plat et de nous assurer de la solidité de l'ensemble ».*

Pour l'heure, le SOC MGEN dispose au quotidien du plus crucial : la découverte de l'exposition et des failles critiques. Maxime Granatini entend néanmoins aller plus loin dans l'exploitation de la richesse de données issues de Patrowl. « *Patrowl est une solution conçue pour ne pas inonder les services IT d'un flot de données difficiles à exploiter. Mais nous sommes curieux d'en savoir plus, c'est pourquoi nous avançons pas à pas, en collaboration avec les équipes de Patrowl, dans l'utilisation de ces ressources complémentaires* ».

Une collaboration qui tient ses promesses

MGEN est toujours à la recherche de solutions innovantes, dans ce secteur foisonnant de la cybersécurité. « *Il y a beaucoup de choses à faire, beaucoup de challenges, pour lesquels nous avons besoin de solutions pragmatiques. Patrowl nous permet d'adresser l'enjeu d'identification de la surface d'attaque et le problème de l'obsolescence des Pentests*

traditionnels. L'équipe connaît parfaitement son métier et la société Patrowl a bien compris le besoin cyber des organisations » observe Maxime Granatini, qui a particulièrement apprécié de voir l'excellence de la relation se poursuivre dans le temps avec l'expert du « Pentest as a Service ».

« *Nous avons avec eux des échanges fluides, très clairs. Les interactions sont permanentes et nous gagnons en maturité sur l'utilisation avancée de Patrowl. Nous savons que l'outil peut offrir encore plus. Nous sommes heureux de contribuer, à notre échelle, à son évolution* ». De fait, la roadmap 2023 de Patrowl est étoffée et propre à répondre aux nouvelles attentes de ses utilisateurs.

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.

Contact Presse : Sophie Terrien — agence Portised — sophie.terrien@portis-ed.fr — 06 09 17 24 79