HADRIAN

AROMA360

ÉTUDE DE CAS

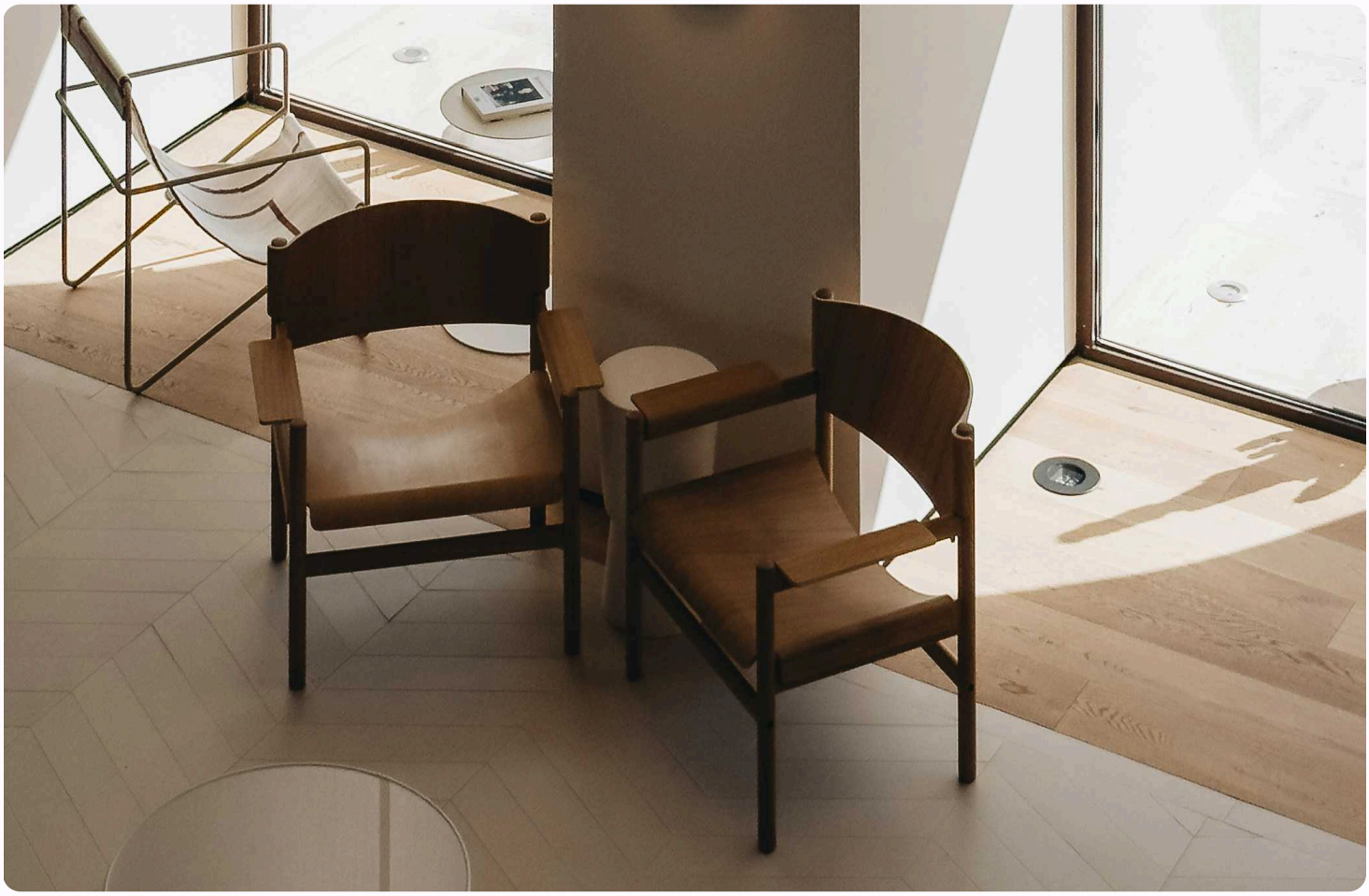
Comment Aroma360 a appliqué une visibilité de l'extérieur pour prendre le contrôle de sa surface d'attaque

RETAIL, ÉTATS-UNIS

À propos de Aroma360

Aroma360 est une marque de parfumerie de luxe basée à Miami, spécialisée dans le marketing olfactif et le branding pour les environnements hospitality et retail. Fondée en 2013, l'entreprise conçoit, fabrique et entretient des systèmes de diffusion de fragrances et des parfums signatures pour certains des groupes hôteliers et marques retail les plus reconnus au monde, notamment le Ritz-Carlton, Marriott, Four Seasons, Ferrari et W Hotels. Avec plus de 300 employés, des clients dans 22 pays et une opération moderne d'e-commerce, de gestion client et d'abonnement soutenant ses partenariats dans l'hospitality, Aroma360 détient un volume significatif de données personnelles clients (PII) liées aux commandes, comptes et livraisons récurrentes.

FONDÉE	EMPLOYÉS	PAYS DESSERVIS
2013	2.000+	22+



Défis

01 Garder une longueur d'avance sur les menaces ciblant la marque

En tant que marque reconnue, le profil public et la réputation d'Aroma360 attirent une attention constante d'acteurs malveillants. Les playbooks standard de réponse aux incidents sont conçus pour le confinement après coup, tandis que la priorité de l'équipe de sécurité était la disruption précoce en minimisant la fenêtre d'exposition.

02 Aucune vue de l'extérieur sur la surface d'attaque

Sans une vue continue et de l'extérieur de leur environnement, l'équipe n'avait aucun moyen fiable de déterminer quels actifs exposés sur internet pourraient être compromis par un attaquant. Leurs outils étaient conçus pour surveiller l'environnement de l'intérieur, ce qui signifiait qu'ils ne pouvaient signaler que ce qui était déjà connu. Sans cette perspective externe, identifier quels actifs étaient vulnérables à une compromission représentait un véritable défi.

03 Des partenaires exigeant plus qu'une évaluation périodique

En tant que marque au service de grands partenaires dans l'hospitality et le retail, Aroma360 fixait un niveau d'exigence élevé pour démontrer la sécurité de son environnement externe. Un rapport de test de pénétration annuel n'était plus une réponse suffisante au niveau d'assurance attendu par leurs partenaires.

Solution

Identifier l'exposition utilisée comme vecteur d'attaque

Hadrian a identifié les expositions spécifiques sur internet avec des exploits connus que les acteurs de la menace pouvaient utiliser comme vecteurs d'attaque, accompagnées d'un guide de remédiation étape par étape directement lié à cet actif.

Fournir une vue de l'extérieur

Hadrian a fourni à Aroma360 une vue continue et de l'extérieur de l'ensemble de leur infrastructure exposée sur internet. Étant agentless, Hadrian ne nécessitait aucun déploiement à l'intérieur du réseau et a commencé à produire des résultats en quelques minutes après l'onboarding.

Vérification continue après remédiation

Suite à la remédiation, Hadrian a automatiquement retesté l'actif corrigé pour confirmer que l'exposition était entièrement fermée, bouclant la boucle de la découverte jusqu'à la résolution vérifiée.

Résultats

Fiducia su una superficie di attacco ampia e attiva

La présence de la marque Aroma360 signifie que sa surface d'attaque est constamment testée par un large éventail d'acteurs malveillants. Des scripts opportunistes visant à défigurer des pages web aux campagnes sophistiquées utilisant de nouvelles techniques zero-day pour cibler les données de paiement des clients et les programmes de fidélité, la variété des vecteurs d'attaque en jeu exige une couverture allant bien au-delà d'une checklist standard. Hadrian teste l'intégralité de l'OWASP Top 10 avec un large éventail de techniques d'attaque, offrant à l'équipe une visibilité confirmée sur les expositions exploitables quelle que soit la façon dont la menace se manifeste.

Lorsqu'une exposition est identifiée, elle remonte avec des étapes de reproduction propres à cet actif spécifique, permettant à l'équipe d'agir avec conviction plutôt que de perdre du temps à investiguer. Hadrian reteste automatiquement l'actif après remédiation pour confirmer que l'exposition est entièrement fermée, bouclant la boucle de la découverte jusqu'à la résolution vérifiée. Pour une marque où la confiance des clients et l'intégrité des données sont non négociables, cette validation de bout en bout transforme la fonction de sécurité : d'une fonction qui répond aux incidents, elle devient une fonction qui ferme les expositions avant qu'elles ne le deviennent.

Trouver la cause profonde, pas le symptôme

Chaque mesure défensive déployée par l'équipe d'Aroma360 avant Hadrian reposait sur la même hypothèse : que le point d'entrée de l'attaquant se trouvait quelque part à l'intérieur du périmètre connu de l'environnement. Des honeypots, la rotation des identifiants et des contrôles d'accès renforcés furent mis en place pour tenter de contrer les attaques. Cependant, ils n'arrêtaient pas la violation car chaque contre-mesure était orientée de l'intérieur vers l'extérieur, défendant l'environnement tel qu'on le croyait être plutôt que tel qu'un attaquant pouvait le voir de l'extérieur. L'attaquant opérait dans les lacunes entre ce que l'équipe pouvait voir et ce qui était réellement exposé, et rien dans la pile existante n'était conçu pour combler cette distance.

> **« Nous avions essayé des honeypots, la rotation des accès et tous les contrôles internes possibles, mais les données continuaient de fuir. Hadrian nous a montré l'actif unique qui exposait les PII de l'extérieur. Nous l'avons corrigé directement et l'exfiltration s'est arrêtée. C'était la première fois dans cet incident que nous avions le sentiment d'être en avance sur l'attaquant. »**
>
> Responsable Sécurité, Aroma360

Résultats

Hadrian a abordé le problème différemment. En cartographiant l'environnement d'Aroma360 de l'extérieur vers l'intérieur, comme le ferait un attaquant, il a mis en évidence l'exposition spécifique que l'attaquant avait exploitée à plusieurs reprises. Ce qui était resté invisible à tous les outils défensifs internes était, vu de l'extérieur, un point d'entrée unique et identifiable. La cause profonde désormais visible, l'équipe pouvait agir directement sur le problème plutôt que sur ses symptômes.

Une réponse crédible et continue pour les partenaires

Pour une marque dont les partenariats dans l'hospitality et le retail dépendent de la confiance des clients finaux, la capacité à parler avec confiance de l'exposition externe n'est pas une case de conformité à cocher, mais une exigence commerciale. Avant Hadrian, le mieux qu'Aroma360 pouvait offrir à ses partenaires était une évaluation ponctuelle qui devenait obsolète dès sa production. Hadrian a changé cela. Avec une analyse continue et des résultats validés mis à jour en temps réel, Aroma360 peut désormais démontrer à tout moment que sa surface d'attaque externe a été testée, que les expositions sont identifiées dès leur apparition et que rien n'est laissé non validé. Ce passage, de l'assurance périodique à la preuve continue, est ce qu'exigent les partenaires dans le luxe hospitality et retail.

La sécurité offensive d'Hadrian révèle comment des attaques réelles pourraient compromettre les applications et les infrastructures. Notre plateforme autonome effectue des tests en continu afin d'évaluer de manière exhaustive les actifs exposés à Internet. La technologie cloud sans agent est constamment mise à jour et améliorée par l'équipe de hackers éthiques d'Hadrian.

Réserver une démonstration