HADRIAN

AROMA360

FALLSTUDIE

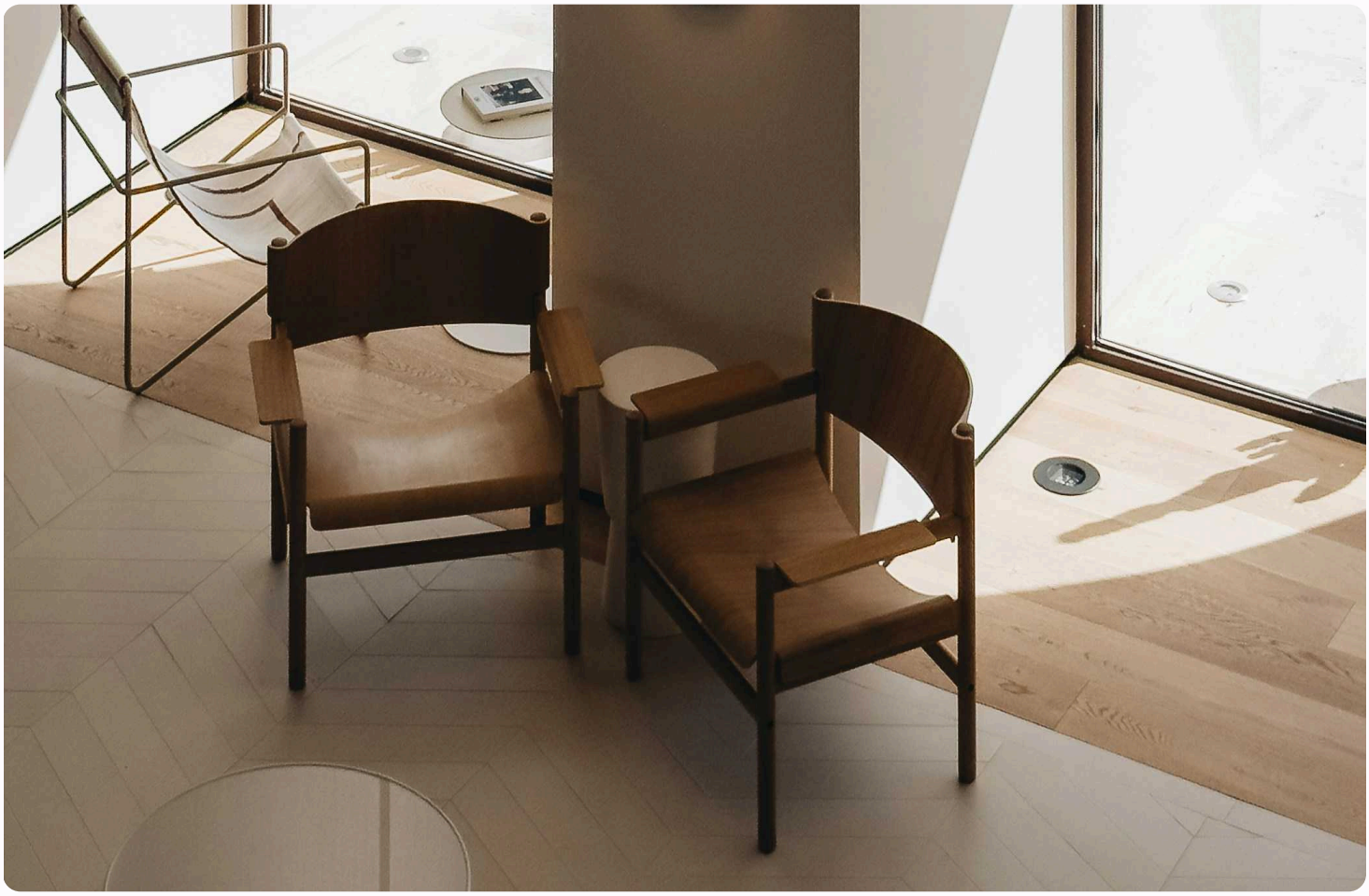
Wie Aroma360 eine Outside-in-Transparenz nutzte, um die Kontrolle über seine Angriffsfläche zu übernehmen

RETAIL, VEREINIGTE STAATEN

Über Aroma360

roma360 ist eine in Miami ansässige Luxus-Duftmarke, spezialisiert auf Scent Marketing und Branding für Hospitality- und Retail-Umgebungen. Gegründet 2013, entwirft, produziert und wartet das Unternehmen Duftdiffusionssysteme und Signature-Fragrances für einige der weltweit bekanntesten Hotelgruppen und Retail-Marken, darunter Ritz-Carlton, Marriott, Four Seasons, Ferrari und W Hotels. Mit über 300 Mitarbeitern, Kunden in 22 Ländern und einem modernen E-Commerce-, Kunden- und Abonnementbetrieb hinter seinen Hospitality-Partnerschaften hält Aroma360 ein bedeutendes Volumen an persönlichen Kundendaten (PII), die mit Bestellungen, Konten und wiederkehrenden Lieferungen verbunden sind.

GEGRÜNDET	MITARBEITER	BEDIENTE LÄNDER
2013	300+	22+



Herausforderungen

01 **Bedrohungen, die auf die Marke abzielen, einen Schritt voraus sein**

Als bekannte Marke zieht das öffentliche Profil und der Ruf von Aroma360 kontinuierlich Aufmerksamkeit von böswilligen Akteuren auf sich. Standard-Incident-Response-Playbooks sind für die nachträgliche Eindämmung konzipiert, während die Priorität des Sicherheitsteams die frühzeitige Unterbrechung war, indem das Expositionsfenster minimiert wurde.

02 **Keine Außenperspektive auf die Angriffsfläche**

Ohne eine kontinuierliche Außenperspektive auf ihre Umgebung hatte das Team keine zuverlässige Möglichkeit festzustellen, welche internetexponierten Assets von einem Angreifer kompromittiert werden könnten. Ihre Tools waren darauf ausgelegt, die Umgebung von innen zu überwachen, was bedeutete, dass sie nur über bereits Bekanntes berichten konnten. Ohne diese externe Perspektive war die Identifizierung anfälliger Assets eine echte Herausforderung.

03 **Partner, die mehr als eine periodische Bewertung verlangen**

Als Marke, die große Hospitality- und Retail-Partner bedient, setzte Aroma360 hohe Maßstäbe beim Nachweis der Sicherheit seiner externen Umgebung. Ein jährlicher Penetrationstest-Bericht war keine ausreichende Antwort mehr auf das Sicherheitsniveau, das ihre Partner erwarteten.

Lösung

✓ **Identifizierung der als Angriffsweg genutzten Exposition**

Hadrian identifizierte die spezifischen internetexponierten Schwachstellen mit bekannten Exploits, die Bedrohungsakteure als Angriffsvektoren nutzen konnten, zusammen mit einer schrittweisen Remediation-Anleitung, die direkt mit dem betroffenen Asset verknüpft war.

✓ **Bereitstellung einer Außenperspektive**

Hadrian verschaffte Aroma360 eine kontinuierliche Außenperspektive auf ihre gesamte internetexponierte Infrastruktur. Als agentlose Lösung erforderte Hadrian keine Bereitstellung im Netzwerk und begann innerhalb von Minuten nach dem Onboarding, Ergebnisse zu liefern.

✓ **Kontinuierliche Überprüfung nach der Remediation**

Nach der Remediation testete Hadrian das gepatchte Asset automatisch erneut, um zu bestätigen, dass die Exposition vollständig geschlossen war, und schloss damit den Kreislauf von der Entdeckung bis zur verifizierten Lösung.

Ergebnis

Vertrauen über eine breite und aktive Angriffsfläche

Die Markenpräsenz von Aroma360 bedeutet, dass ihre Angriffsfläche ständig von einer Vielzahl von Bedrohungsakteuren getestet wird. Von opportunistischen Skripten zur Verunstaltung von Webseiten bis hin zu ausgefeilten Kampagnen, die neuartige Zero-Day-Techniken einsetzen, um Kundenzahlungsdaten und Treueprogramme anzugreifen – die Vielfalt der eingesetzten Angriffsvektoren erfordert eine Abdeckung, die weit über eine Standard-Checkliste hinausgeht. Hadrian testet die gesamte OWASP Top 10 mit einem breiten Spektrum an Angriffstechniken und verschafft dem Team eine bestätigte Sichtbarkeit auf ausnutzbare Expositionen, unabhängig davon, wie die Bedrohung auftritt.

Wenn eine Exposition identifiziert wird, erscheint sie mit Reproduktionsschritten, die für dieses spezifische Asset einzigartig sind, sodass das Team mit Überzeugung handeln kann, anstatt Zeit mit Ermittlungen zu verbringen. Hadrian testet das Asset nach der Remediation automatisch erneut, um zu bestätigen, dass die Exposition vollständig geschlossen ist, und schließt den Kreislauf von der Entdeckung bis zur verifizierten Lösung. Für eine Marke, bei der Kundenvertrauen und Datenintegrität nicht verhandelbar sind, verwandelt diese End-to-End-Validierung die Sicherheitsfunktion von einer reaktiven Incident-Response in eine, die Expositionen schließt, bevor sie zu Vorfällen werden.

Die Grundursache finden, nicht das Symptom

Jede defensive Maßnahme, die das Team von Aroma360 vor Hadrian einsetzte, basierte auf derselben Annahme: dass der Einstiegspunkt des Angreifers irgendwo innerhalb des bekannten Perimeters der Umgebung lag. Honeypots, Credential-Rotation und verschärfte Zugriffskontrollen wurden implementiert, um Angriffe abzuwehren. Sie stoppten den Angriff jedoch nicht, weil jede Gegenmaßnahme von innen nach außen ausgerichtet war – die Umgebung so verteidigend, wie man glaubte, dass sie existiert, anstatt so, wie ein Angreifer sie von außen sehen konnte. Der Angreifer operierte in den Lücken zwischen dem, was das Team sehen konnte, und dem, was tatsächlich exponiert war, und nichts im bestehenden Stack war darauf ausgelegt, diese Distanz zu schließen.

> **„ Wir hatten Honeypots, Access-Rotation und alle internen Kontrollen ausprobiert, die wir aufbieten konnten, und die Daten flossen weiter ab. Hadrian zeigte uns das einzelne Asset, das PII von außen exponierte. Wir haben es direkt gepatcht, und die Exfiltration hörte auf. Es war das erste Mal in diesem Vorfall, dass wir das Gefühl hatten, dem Angreifer voraus zu sein.**
>
> Security Lead, Aroma360

Ergebnis

Hadrian ging das Problem anders an. Indem es die Umgebung von Aroma360 von außen nach innen kartierte – so wie ein Angreifer es tun würde –, legte es die spezifische Exposition frei, die der Angreifer wiederholt ausgenutzt hatte. Was für jedes interne Abwehr-Tool unsichtbar geblieben war, war von außen ein einziger identifizierbarer Einstiegspunkt. Mit der nun sichtbaren Grundursache konnte das Team direkt auf das Problem reagieren statt auf seine Symptome.

Eine glaubwürdige, kontinuierliche Antwort für Partner

Für eine Marke, deren Hospitality- und Retail-Partnerschaften vom Vertrauen der Endkunden abhängen, ist die Fähigkeit, mit Zuversicht über externe Expositionen zu sprechen, kein Compliance-Kontrollkästchen, sondern eine geschäftliche Anforderung. Vor Hadrian konnte Aroma360 seinen Partnern bestenfalls eine punktuelle Bewertung anbieten, die im Moment ihrer Erstellung bereits veraltete. Hadrian änderte das. Mit kontinuierlichem Scanning und in Echtzeit aktualisierten validierten Ergebnissen kann Aroma360 nun jederzeit nachweisen, dass ihre externe Angriffsfläche getestet wurde, dass Expositionen beim Auftreten identifiziert werden und dass nichts unvalidiert bleibt. Dieser Wandel – von periodischer Versicherung zu kontinuierlichen Belegen – ist das, was Partner im Luxus-Hospitality- und Retail-Bereich fordern.

Die offensive Sicherheit von Hadrian zeigt, wie reale Angriffe Anwendungen und Infrastruktur gefährden können. Unsere autonome Plattform führt kontinuierlich Tests durch, um alle mit dem Internet verbundenen Ressourcen umfassend zu bewerten. Die cloudbasierte, agentenlose Technologie wird vom Ethical-Hacker-Team von Hadrian ständig aktualisiert und verbessert.

Demo buchen