HADRIAN

AROMA360

CASO DI STUDIO

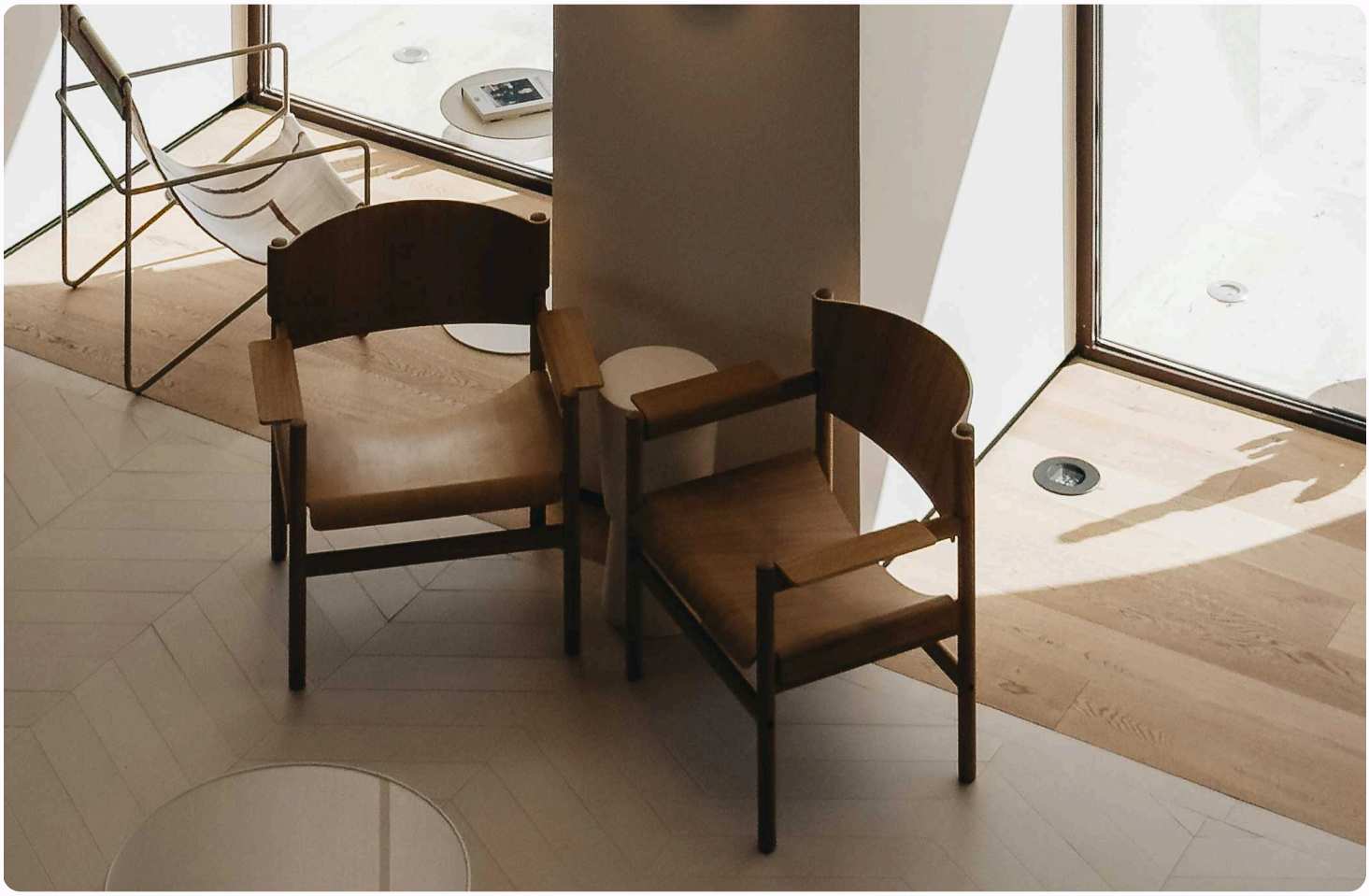
Aroma360 blocca una violazione attiva correggendo l'asset esposto individuato da Hadrian

RETAIL, STATI UNITI

Informazioni su Aroma360

Aroma360 è un brand di profumazione di lusso con sede a Miami, specializzato nel scent marketing e branding per ambienti hospitality e retail. Fondata nel 2013, l'azienda progetta, produce e gestisce sistemi di diffusione di fragranze e profumi esclusivi per alcuni dei gruppi alberghieri e brand retail più rinomati al mondo, tra cui Ritz-Carlton, Marriott, Four Seasons, Ferrari e W Hotels. Con oltre 300 dipendenti, clienti in 22 paesi e un'operazione moderna di e-commerce, gestione clienti e abbonamenti a supporto delle partnership nel settore hospitality, Aroma360 detiene un volume significativo di dati personali dei clienti (PII) legati a ordini, account e consegne ricorrenti

FONDATA	DIPENDENTI	PAESI SERVITI:
2013	300+	22+



La sfida

01 **Anticipare le minacce che prendono di mira il brand**

In quanto brand affermato, il profilo pubblico e la reputazione di Aroma360 attirano costantemente l'attenzione di attori malintenzionati. I playbook standard di incident response sono progettati per il contenimento a posteriori, mentre la priorità del team di sicurezza era l'interruzione precoce, riducendo al minimo la finestra di esposizione.

02 **Nessuna visione dall'esterno della superficie di attacco**

Senza una visione continua e dall'esterno del proprio ambiente, il team non aveva modo affidabile per determinare quali asset esposti su internet potessero essere compromessi da un attaccante. Gli strumenti erano progettati per monitorare l'ambiente dall'interno, il che significava che potevano segnalare solo ciò che era già noto. Senza quella prospettiva esterna, identificare quali asset fossero vulnerabili alla compromissione rappresentava una sfida concreta.

03 **Partner che richiedono più di una valutazione periodica**

Servendo importanti partner nel settore hospitality e retail, Aroma360 poneva un alto standard nel dimostrare la sicurezza del proprio ambiente esterno. Un report di penetration test annuale non era più una risposta sufficiente al livello di garanzia che i loro partner si aspettavano.

Soluzione

✓ **Identificare l'esposizione utilizzata come vettore di attacco**

Hadrian ha identificato le specifiche esposizioni su internet con exploit noti che gli attori delle minacce potevano utilizzare come vettori di attacco, insieme a una guida alla remediation passo dopo passo collegata direttamente a quell'asset.

✓ **Fornire una visione dall'esterno**

Hadrian ha fornito ad Aroma360 una visione continua e dall'esterno dell'intera infrastruttura esposta su internet. Essendo agentless, Hadrian non richiedeva alcuna distribuzione all'interno della rete e ha iniziato a produrre risultati entro pochi minuti dall'onboarding.

✓ **Verifica continua dopo la remediation**

A seguito della remediation, Hadrian ha automaticamente ritestato l'asset corretto per confermare che l'esposizione fosse completamente chiusa, completando il ciclo dalla scoperta alla risoluzione verificata.

Il risultato

Fiducia su una superficie di attacco ampia e attiva

La presenza del brand di Aroma360 significa che la sua superficie di attacco viene costantemente testata da un'ampia gamma di attori minacciosi. Dagli script opportunistici per deturpare le pagine web alle campagne sofisticate che utilizzano nuove tecniche zero-day per colpire i dati di pagamento dei clienti e i programmi fedeltà, la varietà dei vettori di attacco in gioco richiede una copertura che va ben oltre una checklist standard. Hadrian testa l'intera OWASP Top 10 con un'ampia gamma di tecniche di attacco, fornendo al team una visibilità confermata sulle esposizioni sfruttabili indipendentemente da come arriva la minaccia.

Quando viene identificata un'esposizione, emerge con passaggi di riproduzione unici per quell'asset specifico, così il team può agire con convinzione anziché perdere tempo a investigare. Hadrian ritesta automaticamente l'asset dopo la remediation per confermare che l'esposizione sia completamente chiusa, completando il ciclo dalla scoperta alla risoluzione verificata. Per un brand in cui la fiducia dei clienti e l'integrità dei dati sono non negoziabili, questa validazione end-to-end trasforma la funzione di sicurezza da una che risponde agli incidenti a una che chiude le esposizioni prima che possano diventarlo.

Trovare la causa principale, non il sintomo

Ogni misura difensiva dispiegata dal team di Aroma360 prima di Hadrian operava sulla stessa ipotesi: che il punto di ingresso dell'attaccante si trovasse da qualche parte all'interno del perimetro noto dell'ambiente. Honeypot, rotazione delle credenziali e controlli degli accessi più rigidi furono implementati per tentare di contrastare gli attacchi. Tuttavia, non riuscivano a bloccare la violazione perché ogni contromisura era orientata dall'interno verso l'esterno, difendendo l'ambiente così come si credeva esistesse, piuttosto che come un attaccante poteva vederlo dall'esterno. L'attaccante operava nei gap tra ciò che il team poteva vedere e ciò che era effettivamente esposto, e nulla nello stack esistente era progettato per colmare quella distanza.

> **"Avevamo provato honeypot, rotazione degli accessi e ogni controllo interno possibile, ma i dati continuavano a fuoriuscire. Hadrian ci ha mostrato il singolo asset che esponeva i PII dall'esterno. Lo abbiamo corretto direttamente e l'esfiltrazione si è fermata. È stata la prima volta in quell'incidente in cui ci siamo sentiti un passo avanti all'attaccante."**
>
> Security Lead, Aroma360

Il risultato

Hadrian ha affrontato il problema diversamente. Mappando l'ambiente di Aroma360 dall'esterno verso l'interno, come farebbe un attaccante, ha individuato l'esposizione specifica che l'attaccante aveva sfruttato ripetutamente. Ciò che era rimasto invisibile a ogni strumento difensivo interno era, dall'esterno, un singolo punto di ingresso identificabile. Con la causa principale ora visibile, il team poteva agire direttamente sul problema anziché sui suoi sintomi.

Una risposta credibile e continua per i partner

Per un brand le cui partnership nel settore hospitality e retail dipendono dalla fiducia dei clienti finali, la capacità di parlare con sicurezza dell'esposizione esterna non è una casella di conformità da spuntare, ma un requisito commerciale. Prima di Hadrian, il massimo che Aroma360 poteva offrire ai partner era una valutazione puntuale che diventava obsoleta nel momento stesso in cui veniva prodotta. Hadrian ha cambiato tutto ciò. Con scansione continua e risultati validati aggiornati in tempo reale, Aroma360 può ora dimostrare in qualsiasi momento che la propria superficie di attacco esterna è stata testata, che le esposizioni vengono identificate non appena emergono e che nulla viene lasciato non validato. Questo passaggio, dalla garanzia periodica all'evidenza continua, è ciò che i partner nel lusso hospitality e retail richiedono.

La sicurezza offensiva di Hadrian rivela come gli attacchi reali potrebbero compromettere le applicazioni e l'infrastruttura. La nostra piattaforma autonoma esegue test continui per valutare in modo completo le risorse esposte a Internet. La tecnologia basata su cloud e senza agenti viene costantemente aggiornata e migliorata dal team di hacker etici di Hadrian.

Prenota una demo