breachday

EXERCISE PLATFORM

WHITE-LABEL PARTNER PROGRAM

Breachday for MSPs & Advisory Firms

Deliver live, audit-ready tabletop exercises under your own brand, without building or maintaining the software yourself.

SOC 2 · PCI DSS 4.0 · SEC 1.05 · ISO 22301 · CMMC · CISA CTEP

PREPARED FOR

Advisory, MSSP & Distribution Partners

breachday.io · Partner Program · 2026

01 · INTRODUCTION

Executive Summary

A Recurring Delivery Line You Don't Have to Build

Every client you advise on incident response, business continuity, or technology risk eventually hits the same wall. The plan is documented, but nobody has tested it under real conditions. Breachday closes that gap, and the partner program lets you sell it as a branded, recurring line inside your own practice.

The program is built for firms that already hold a compliance or advisory relationship with their clients: MSSPs and vCISO providers, technology consultancies, and multi-service professional services firms, including accounting and audit firms with a cybersecurity or technology consulting practice. If you want to grow advisory revenue without growing headcount at the same rate, this is the model.

You already know which frameworks each client answers to, and your clients already trust you to tell them what a tested plan looks like. What most firms lack is a delivery mechanism that scales past PowerPoint decks and a single facilitator's calendar.

Breachday's MSP Partner Program gives you a fully isolated, white-labeled instance of the platform for every client. Live facilitation, real-time participant response capture, and branded audit-ready reporting, all running under your firm's name and priced per client slot on one annual agreement.

02 · THE PROBLEM

Compliance Is Forcing the Issue

Five regulatory and audit forces are independently pushing organizations toward incident response and continuity plans that have been tested, not only written:

- ✓ PCI DSS 4.0 Requirement 12.10 requires annual incident response plan testing with documented results.
- ✓ SOC 2 auditors increasingly expect tabletop evidence rather than a policy binder alone when assessing the Security and Availability Trust Services Criteria.
- ✓ SEC Item 1.05 and Regulation S-K Item 106 require public registrants to assess and disclose material incidents within four business days, which no team can do cold.
- ✓ ISO 22301 requires a documented Business Impact Analysis and an active exercise program that validates the continuity management system on an ongoing basis.
- ✓ CMMC requires Department of Defense contractors handling Controlled Unclassified Information to demonstrate a mature, tested security program as part of certification. A written plan alone will not satisfy an assessor.

THE GAP ADVISORS KEEP HITTING

Clients need to show a tested plan on a recurring cadence. Running that test manually (building a deck, wrangling a room, writing up the after-action notes) consumes senior consultant hours that don't scale across a client book, and it ties the quality of every engagement to whichever consultant knows that client's environment best.

03 · SALES ENABLEMENT

Recognizing the Buying Signal

When Tabletop Testing Becomes a Live Conversation

Tabletop testing rarely gets bought on its own. It surfaces inside a broader risk, compliance, or technology conversation your team is already having. These signals reliably indicate a client is ready to hear about it:

- ✓ A cyber insurance renewal or new policy application that raises incident-response testing requirements.
- ✓ A near-miss, or a peer organization in the client's industry or region experiencing a real incident.
- ✓ Clients fielding their own due-diligence requests, such as vendor security questionnaires, SOC 2 letters, or customer audits, and needing to show their own house is in order.
- ✓ A new technology deployment or significant infrastructure change that reopens the incident response plan.
- ✓ Executive or board-level attention on cybersecurity, often following a budget cycle or a board presentation.
- ✓ Organizational scale. Orgs above roughly $20M in annual revenue typically carry a dedicated security budget rather than treating security as overhead.

These signals rarely arrive through a dedicated security or compliance team alone. Account managers, auditors, and relationship leads across a firm are often the first to hear them, which makes tabletop testing a natural addition to whatever technology or risk conversation those teams already have with clients.

04 · PLATFORM

Platform Overview

What Breachday Does

Breachday is a facilitator-led, real-time tabletop exercise platform. A facilitator runs the room from a live console. Participants join from their own device using a short room code and respond to scenario injects as they're released, with every action, vote, and observation captured automatically against a per-inject record.

Core Differentiators

- ✓ No participant accounts or installs. Join from a phone, tablet, or laptop with a room code.
- ✓ Custom role seats per client: Incident Commander, Legal, Comms, IT, executive, or any role the client's org chart requires.
- ✓ Live inject delivery on a phase-based timeline, with freeform, vote, and confidence-slider response types.
- ✓ A scenario library built on real-world public breaches plus CISA CTEP-aligned sector templates.
- ✓ Automatic after-action reporting covering timeline, attributed responses, vote tallies, observations, and linked BC assets, exported as a branded PDF.
- ✓ A lessons-learned tracker so clients close the loop on what the exercise surfaced.

05 · WORKFLOW

How It Works

From Scenario to Signed-Off Report

The same five-step flow runs identically inside every client org. Only the branding changes.

01 · Design the scenario

Choose a default or CTEP-based template, or clone and customize one for the client's environment. Tag the client's IT assets and BIA processes the exercise will touch.

02 · Launch the exercise

Open the room with one click and share the room code. No client-side installs or accounts to provision.

03 · Join the room

Stakeholders join from any device, pick a display name, and claim a role seat.

04 · Run the tabletop

Release injects on the timeline and capture votes, freeform responses, and live facilitator observations as the room works the incident.

05 · Review the report

Generate the after-action report covering timeline, decisions, vote tallies, and lessons learned, branded with the client's logo or your firm's.

06 · COMPLIANCE

Compliance Mapping

One Exercise, Multiple Audit Trails

Every exercise run inside a client's Breachday org produces a report that maps to the controls their auditor or assessor is already asking about, giving you one deliverable that supports several client engagements at once.

MOST COMMON

SOC 2

- → CC7.3: Evaluating security events
- → CC7.4: Responding to security incidents
- → CC7.5: Recovery from identified events
- → A1.2 / A1.3: Availability & environmental BCM

ANNUAL REQUIREMENT

PCI DSS 4.0

- → Req 12.10.1: IR plan exists, reviewed, tested
- → Req 12.10.2: Annual testing & documented results
- → Req 12.10.4: Personnel trained on IR duties
- → Req 12.10.5: IR plan covers all required elements

PUBLIC COMPANIES

SEC Cyber Disclosure

- → Item 1.05: 4-day material incident readiness
- → Item 106(b): Cyber risk management disclosure
- → Item 106(c): Board oversight & management role
- → Materiality drills: legal / finance / comms rehearsal

BCM STANDARD

ISO 22301

- → Clause 8.2: BIA & risk assessment
- → Clause 8.5: Exercise program & testing
- → Clause 9.1: Performance evaluation
- → Clause 10: Continual improvement & lessons learned

Breachday is not a substitute for legal or audit advice. Control mappings are guidance for compliance and assessment teams, and the client's auditor or assessor has the final say.

07 · DELIVERY MODEL

Scaling Delivery Without Scaling Headcount

Associate-Ready Facilitation

In a manually run tabletop, most of the client's institutional knowledge (org structure, who owns what, how departments interact during an incident) has to live in the facilitator's head and gets rebuilt fresh for every client. That's why manual delivery tends to require a senior, client-familiar consultant, and why it's hard to scale a tabletop practice past the calendar of your most experienced people.

Breachday gets that knowledge from the format itself rather than from pre-loading a client's environment. Because every participant responds directly, in their own role, in real time, the room does the correlation work a facilitator would otherwise do by hand. Legal assumes IT already looped in the regulator. IT assumed Comms had a holding statement ready. That gap surfaces in the moment, through participants working the incident against each other, instead of through a facilitator who isn't in their environment day to day.

The result is that a less senior team member can facilitate a strong exercise, because they're orchestrating the room and capturing what happens rather than carrying the client's entire business in their head. Your most experienced consultants can then run more engagements across your client base each quarter, and exercise quality stops depending on which specific person happens to be free that week.

08 · PARTNER PROGRAM

White-Labeled Delivery, Fully Isolated Clients

Each client slot is a complete, isolated Breachday organization with its own users, data, scenarios, and reports, running the full Pro-tier feature set under your firm's brand. You set what you charge your clients. Breachday powers the platform behind it.

- ✓ White-labeled PDF reports carrying your firm's branding rather than Breachday's.
- ✓ Fully isolated client orgs with complete data and user separation between clients.
- ✓ Pro-tier features in every client org: CISA CTEP templates, IT asset register, BIA, unlimited crisis communication plans.
- ✓ A partner portal for cross-client member and organization management.
- ✓ Seed scenarios pre-installed in every client org from day one.
- ✓ Priority support and consultant-style scenario and template cloning across your client base.
- ✓ A dedicated customer success manager at 50+ client slots.

Slots	Billing	Reference Pricing
10 (minimum)	Annual only	**$2,500 / client / yr ($25,000 / yr total)**
11–100	Annual only	**Per-slot rate steps down as slot count increases**

All partner tiers include a 14-day onboarding period and seed scenarios in every client org. Contact us for a volume quote above 10 slots.

09 · WHY BREACHDAY

Built by a Practitioner

Breachday was founded and is actively operated by a working GRC security analyst who sits in the same audits your clients do. The product reflects that: scenario content that reads like a real incident, reports built to satisfy an auditor, and a roadmap driven by what compliance teams get asked for rather than by feature parity with legacy GRC suites.

Proof of Impact

For recurring advisory relationships such as vCISO retainers, managed security services, and ongoing risk advisory, clients increasingly expect more than reassurance that the engagement is going well. They want a number, a visual trend, or a concrete artifact showing the money they spend produced a real improvement. A Breachday report gives partners that: a comparable, trackable record of response times, decision gaps, and closed lessons-learned items that makes an ongoing security relationship demonstrable at renewal.

Trust & Security Posture

- ✓ Data encrypted at rest and in transit across every plan tier.
- ✓ Optional data protection mode on Plus and Pro, with ephemeral, auto-purged session data for sensitive scenarios.
- ✓ Row-level tenancy, so client organizations never see one another's data. This is a structural requirement for any multi-client deployment.
- ✓ Infrastructure built on SOC 2 Type II certified providers (Supabase, Vercel, Neon) as an evidentiary bridge while Breachday's own SOC 2 attestation is pursued on a deliberate, buyer-driven timeline.
- ✓ Continuous automated security scanning (SAST/DAST) on every code change.

10 · NEXT STEPS

Bringing Tested Readiness to Your Client Base

The fastest way to evaluate the partner program is to see it running. Pick one client relationship, run a live 30-minute scenario together, and look at the after-action report it produces.

→ Book a partner walkthrough: a live demo of the facilitator console, participant join flow, and a sample audit-ready report.
→ Choose a starting slot count based on your current client roster (10-slot minimum).
→ Onboard over 14 days with seed scenarios already installed in every client org.
→ Roll out white-labeled tabletop exercises as a standing line item across your engagements.

breachday.io/contact · Book a compliance / partner demo