



No Cloud Required

Building tabletop scenarios from data you can't upload

Richard Suls /||/ US Lead, Security Advisory

REVERSESEC

The exercise everyone passes



INJECT 03

A ransomware group has encrypted several servers. A note demands payment within 72 hours. A journalist has emailed asking for comment.

Whose company is this?

Nobody's.

A scenario written for everyone tests no one.

The inputs that would fix it are the ones that can't leave the building.



Incident reviews



Architecture docs



Runbooks



Vendor inventories

REVERSE

So we bring the model to the data

THE ENGAGEMENT BOUNDARY



Client documents



Model on dedicated hardware



Facilitator who reads everything

Intake logged. Access logged. Destruction certified.



Nothing leaves.

No vendor, no cloud, no terms of service to interpret.



Regulators now expect exercised response. Technical tabletops drill your responders. Crisis management exercises drill leadership decisions. DORA, NIS2, NYDFS 500 and their peers treat both as table stakes.

Their documents already know the scenario



The failure point mentioned once

A dependency named in passing in an architecture document nobody had reread



The system in three runbooks

Assumed available by all of them, owned by none of them



The promise nobody kept

An incident review action item, closed on paper, open in reality



And after the exercise, the rhyme

This year's stall matched to a finding flagged two years ago, before anyone in the room held their job

Findings from real engagements. Details reconstructed, not redacted.

Even paying for every token, the math works



Cheaper

Design hours drop. Compute is a rounding error against consulting time. Clients have paid less per exercise.



Sharper

Injects built from their reality, not a template. The room recognizes its own organization and stops role-playing.



Deeper

Findings tied to the client's own history, so the debrief lands as evidence, not opinion.

The pairing does this. The model alone does not.

It confabulates, it cannot see what was never written down, and a tool that helps you think is not a tool you defend under oath.



You don't need permission.

The hardware is a few thousand dollars. The models are open. The corpus is already yours, sitting in a document system, waiting to tell you which scenario to run.

Richard Suls · Reversesec, Security Advisory · Reversesec.com

REVERSESEC