

SHADOW BREACH™

ONE ENGINE FOR RED TEAM OPS, EXERCISE RED CELL, & REPEATABLE TESTING

Your hardware. Your rules. The report is already written.

ShadowBreach™ attacks and documents in the same motion. A local model plans, executes, and records why it did what it did, all inside your enclave. Run an assessment, throw a red cell at a training audience, or re-run the identical test on the next build. The report is done when the engagement is.

That reasoning trail is the product. Pull a finished, framework-mapped report at any point in the operation and read the decision behind every action in it. Tools and TTPs carry safety levels, so you set where the model stops and a human takes over. Junior and senior operators run the same tradecraft, and the write-up stops costing days.

01 Red Team Ops

REPLACES LEGACY C2 TOOLING

Access, execution, and post-exploitation under one operator console.

The model pursues the objective; the operator holds authority over every escalation.

Findings land mapped to MITRE ATT&CK and OWASP before the debrief.

02 Workforce Development

EXERCISE & SCENARIO RED CELL

One red cell applies pressure across several training audiences at once.

Difficulty scales to the audience and rises as the defenders improve.

Rationale logs double as the after-action product and the teaching material.

03 Repeatable Testing

T&E WITH EXPEDITED REPORTING

Save an engagement as a test pack and re-run it against every build.

Fixed parameters keep runs comparable, so a delta means a real change.

Reports generate per run, cutting the T&E write-up from weeks to minutes.

Learn more & request a demo:

AUTONOMY YOU CAN HAND TO AN OPERATOR & DEFEND IN A DEBRIEF

ShadowBreach runs at three levels of autonomy, so a team can dial how much the model decides on its own. Every tool and TTP carries a safety level, and the human-in-the-loop threshold can be set in any mode. Nothing above the line executes without an operator, and every action is recorded with the reasoning that produced it.

AI Modes of Operations

MODE 01

Playbook

DETERMINISTIC SIMULATION

A fixed sequence runs the same way every time. The basis for repeatable test packs and scripted exercise injects.

MODE 02

Hybrid

OBJECTIVE-DRIVEN

You set the objective. The model determines the steps to reach it and reports the path it chose.

MODE 03

Autonomous

UNSCOPED

No objective given. ShadowBreach attacks what is in front of it and documents everything it finds.

Governance State

Every tool & TTP has a safety level.

Risk is assigned to the technique itself, not determined during execution.

You set the intervention threshold.

Anything at or above that threshold pauses for operator approval, in any mode.

Held actions are fully recorded.

What was proposed, why, and who approved it lands in the engagement report.

ShadowBreach vs. Legacy C2

CAPABILITY	SHADOWBREACH	LEGACY C2
Engagement Reporting	Generated on demand, mid-operation	Manual, days to weeks after
Decision Transparency	Reasoning recorded per action	Command log only
Inference & Data Handling	Local model, air-gap capable	Not applicable
Tradecraft Consistency	Senior-level tradecraft on every engagement	Varies with the operator on console
Repeatable Test Packs	Saved, versioned, re-runnable	Custom scripting
Exercise & Red-cell Mode	Multi-audience scenarios, scaling difficulty	One operator, one target set
Framework Alignment	MITRE ATT&CK and OWASP mapped	Left to the operator



Learn more & request a demo: