Continuous Detection Validation

Use Anvilogic Blueprints to turn every SafeBreach simulation into validated, deployed detection coverage, automatically, with a board-ready evidence trail - no new headcount needed.

THE PROBLEM

Coverage gaps grow faster than your team can close them

Gaps in security coverage surfaced by solutions like SafeBreach - along with MITRE ATT&CK reviews, hunts, audits, red teams, and new CVEs - are overpowering detection engineers across the security industry. Most teams now realize that automation is the only way to ensure threats don't outpace MTTD.

80 FOUND / SPRINT → **20** ACTUALLY FIXED

Manual detection design and tuning can no longer keep up with findings, with detection engineers only closing about 20 gaps a sprint

Simulation findings must become coverage

Every simulation report that turns into a Jira ticket for manual review runs the risk of the validation work never reaching production.

THE SOLUTION

SafeBreach

The SafeBreach CTEM Platform is the first enterprise-grade, closed-loop solution designed to shift siloed security activities toward an intel-driven exposure management program.

ANVILOGIC

Anvilogic Blueprints are reusable, multi-step AI workspaces that use analyst expertise to automate tasks across the entire SOC - with human approval gates where it matters most.

How to build a continuous detection validation workflow

STEP 1

Simulation Result Intake & Triage

Blueprint pulls SafeBreach's completed test's results via their Read API and normalizes them to a structured triage set.

STEP 2A

Detection Design

For each priority candidate, Anvilogic's Blueprint produces atomic detection plans scoped to the technique tested.

STEP 2B

Data Source Binding & Query Authoring

Blueprints then hands each plan to the search layer, binds it to the right data source, and authors the query.

STEP 3

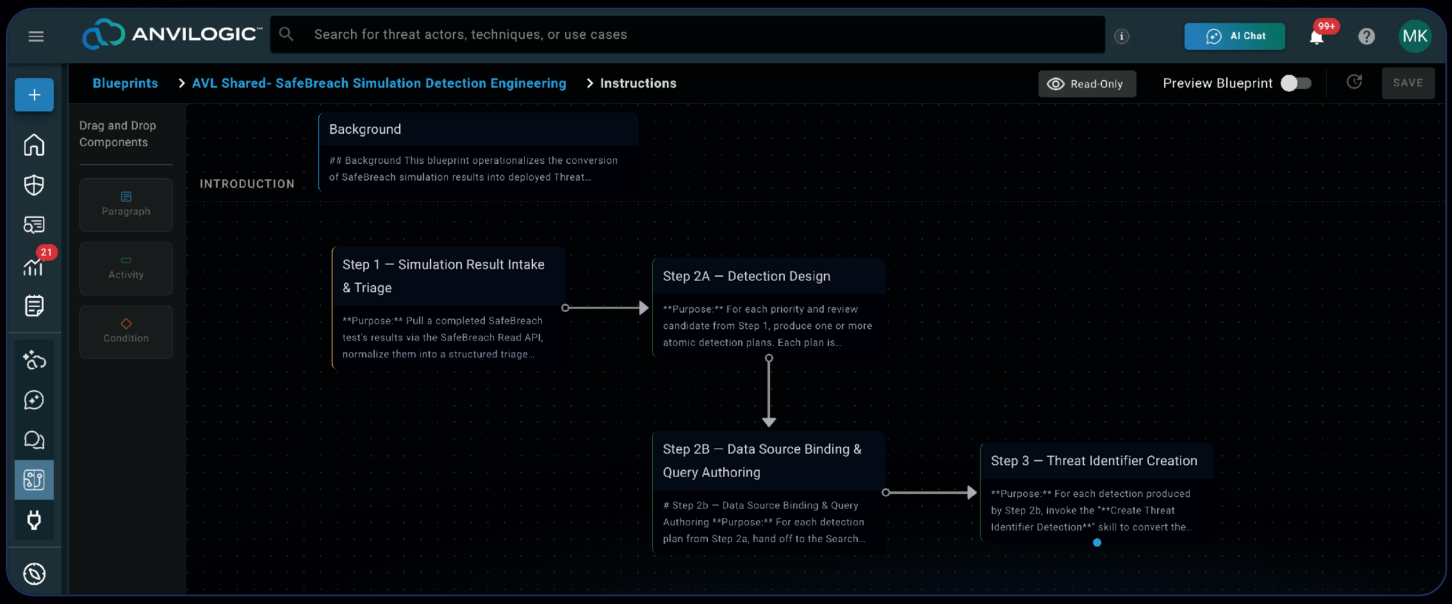
Threat Identifier Creation

Blueprints invokes the CreateThreat Identifier Detection skill to convert each detection into deployable coverage.

ANVILOGIC™ | SafeBreach

From validated security gap to deployed detection - automatically

Every step, prompt, and data-source binding is visible and editable. Detection engineers can inspect the logic, adjust a step, and re-run against the next SafeBreach campaign.



Gaps are closed, not queued, and coverage is scaled, not staffed

Runs on every campaign, minimal analyst lift

Converts each simulation result into deployed, tuned detections automatically. Your team focuses on the work only humans can do.

Continuous, board-ready proof of coverage

Every simulation cycle becomes validated coverage with a full audit trail. Show measurable risk reduction, every quarter.

Explore Blueprints use cases across the SOC

Data Lake Feed Onboarding

Onboards raw bronze/silver feeds into production-ready ETL SQL pipelines mapped to Anvilogic's gold schema, with human approval gates.

Automating L1 Investigations

Automates the L1 triage runbook end-to-end across SIEMs and data lakes, standardizing investigations and exposing the analytic method as it runs.

Ready to kill the backlog and close every coverage gap?

Learn more about how SafeBreach and Anvilogic Blueprints turn every simulation result into deployed coverage - no added adding headcount.