SafeBreach

SafeBreach for Detection Engineering

Prove detection coverage. Strengthen resilience. Reduce risk.

For modern enterprises—especially financial institutions, critical infrastructure providers, and other mature security organizations—the challenge with their detection engineering program isn't about having detection rules; it's about proving they work.

Security teams today often:

Customize Rules Without Validation: Detections are tailored across SIEMs, EDRs, and firewalls. But without simulation and verification, it's unclear whether they ever fire.

Struggle with Log Complexity: Logs arrive in inconsistent formats from dozens of integrations. Without normalization and parsing, critical details are lost or misrepresented, obscuring true risk.

Bear Heavy Operational Overhead: Legacy parsers required custom scripting, which increased dependency on support teams and slowed time-to-value for customers.

Face Pipeline Risk: Even when detections work, SIEM ingestion delays, broken integrations, or corrupted forwarding can prevent alerts from reaching analysts.

The result is blind spots in resilience reporting. CISOs cannot show boards or regulators whether controls actually work, while detection engineers lack the bandwidth, capacity, and resources to validate and tune detections at scale.

Detection Engineering with SafeBreach

SafeBreach empowers detection engineers to move from reactive tuning to validated resilience at scale. The **SafeBreach Exposure Validation Platform** continuously simulates adversary behavior—before and after exploitation—to confirm that custom detections, alert pipelines, and log normalization work as intended.

With SafeBreach, enterprises can:

- **Validate Custom Detections:** Run tailored attack scenarios mapped to real tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs), ensuring rules trigger as expected.
- **Ensure Pipeline Integrity:** Verify alerts successfully flow into SIEMs, SOAR, and ticketing systems, closing gaps that delay incident response.
- **Normalize & Contextualize Logs:** Use parsers and correlators to convert raw telemetry into context-rich SafeBreach Events that accurately reflect risk exposure.
- **Expand Integrations:** Leverage over 60 out-of-the-box integrations, plus flexible parser-driven support for virtually any SIEM-connected log source.
- **Align to Business Risk:** Map detection coverage to MITRE ATT&CK and regulatory frameworks—like DORA, NIS2, and NIST CSF—to provide board-ready risk clarity.

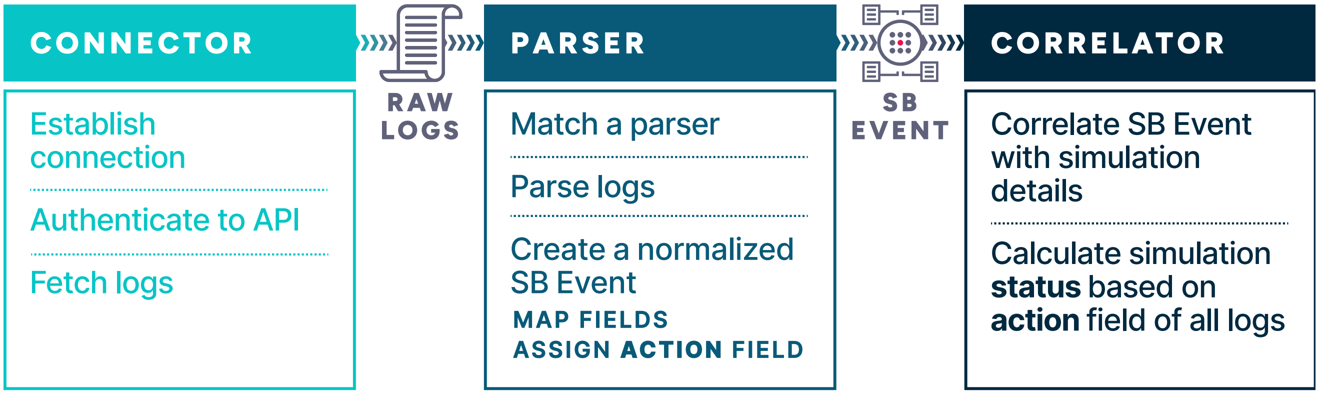
As a result, security teams have greater confidence that detections fire, alerts flow, and incidents are caught in real time, with validated evidence that proves resilience and reduces breach risk.

How It Works

SafeBreach supports two integration models, depending on the customer environment:

INDIRECT INTEGRATION VIA SIEM

splunk> ▫ IBM Radar ▫ LogRhythm



CONNECTOR

- Establish connection
- Authenticate to API
- Fetch logs

RAW LOGS

PARSER

- Match a parser
- Parse logs
- Create a normalized SB Event
  - MAP FIELDS
  - ASSIGN ACTION FIELD

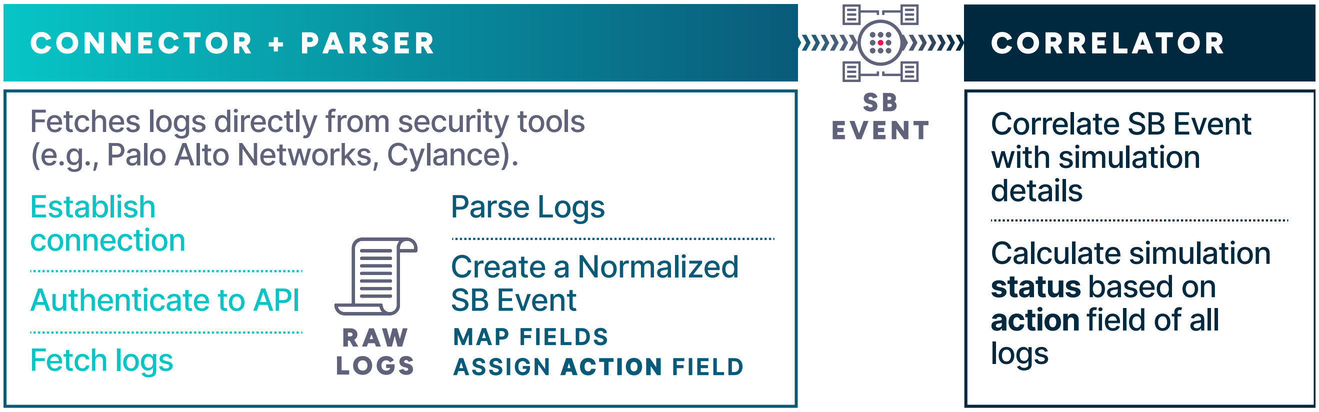
SB EVENT

CORRELATOR

- Correlate SB Event with simulation details
- Calculate simulation **status** based on **action** field of all logs

DIRECT INTEGRATION

paloalto NETWORKS ▫ cybereason ▫ CYLANCE



CONNECTOR + PARSER

Fetches logs directly from security tools (e.g., Palo Alto Networks, Cylance).

- Establish connection
- Authenticate to API
- Fetch logs

RAW LOGS

- Parse Logs
- Create a Normalized SB Event
  - MAP FIELDS
  - ASSIGN ACTION FIELD

SB EVENT

CORRELATOR

- Correlate SB Event with simulation details
- Calculate simulation **status** based on **action** field of all logs

Together, these flows provide closed-loop validation that logs are collected, detections fire, and results are reported accurately.

Spotlight: The New Parsers Experience

Parsers are central to SafeBreach's detection engineering capabilities. They transform raw logs into actionable insights by mapping fields, prioritizing actions, and ensuring context is preserved for reporting.

CHALLENGES WITH LEGACY PARSERS

- Required manual coding, leading to high support ticket volume.
- Difficulty handling complex log types (e.g., CrowdStrike FDR, ProxySG).
- Limited conditional logic, resulting in parsing errors and false positives.

THE NEW PARSER UI

SafeBreach has reimagined the parser experience with a no-code, wizard-driven interface that:

- **Boosts Detection Engineering:** Refine event correlation by defining how logs are prioritized and interpreted.
- **Provides an Easy-to-Use Wizard:** Simplifies parser creation without coding knowledge.
- **Supports Dynamic Field Mapping:** Handle nested arrays, conditional defaults, and fallback logic.
- **Offers a Parser Management Page:** Centrally manage, test, and debug parsers.

SafeBreach Benefits

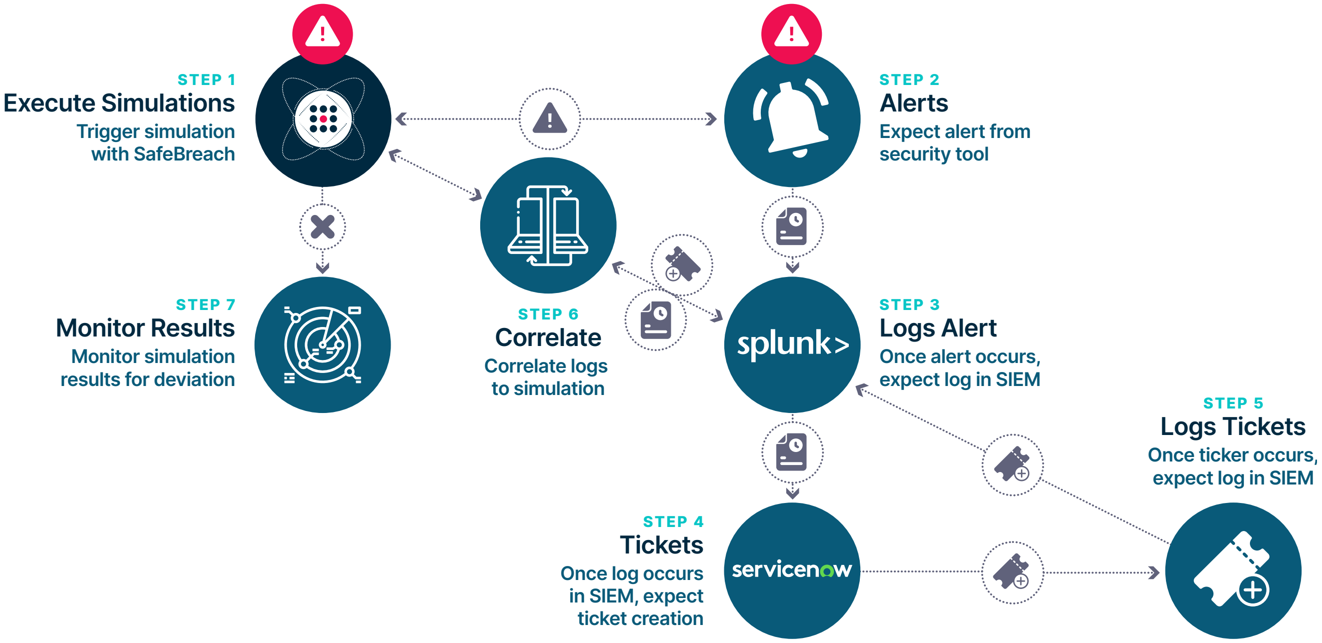
SIMPLIFY CUSTOM ATTACK CREATION

SafeBreach Studio enables teams to easily create advanced attacks, by modifying existing playbook attacks or using external data sources like PCAPs, threat intelligence, and Python scripting. These attacks can be automated to continuously validate custom detections and ensure alerts trigger as expected.

ENABLE ALERT PIPELINE VALIDATION

The SafeBreach Exposure Validation Platform simulates activity that triggers alerts and allows every stage of the alert cycle to be validated. SafeBreach integrations aggregate alerts and logs from connected security tools, consolidating data from each step of the alert pipeline into one unified view.

By incorporating SafeBreach into the alert pipeline validation workflow, organizations can validate that controls, logs, tickets, and integrations are functioning as intended—at scale.



STEP 1
Execute Simulations
Trigger simulation with SafeBreach

STEP 2
Alerts
Expect alert from security tool

STEP 3
Logs Alert
Once alert occurs, expect log in SIEM

STEP 4
Tickets
Once log occurs in SIEM, expect ticket creation

STEP 5
Logs Tickets
Once ticker occurs, expect log in SIEM

STEP 6
Correlate
Correlate logs to simulation

STEP 7
Monitor Results
Monitor simulation results for deviation

This closed-loop validation eliminates guesswork, enabling continuous assurance that the alert pipeline is healthy and ready for a real incident.

Customer Insight: Enhancing Detection Engineering Through SafeBreach

> "SafeBreach enables us to run real-time attack simulations that empower our detection engineering teams to build and refine detections proactively. We can validate the effectiveness of existing controls, identify gaps, and iterate fast—with results grounded in actual attacker behavior."
>
> **CISO**
> Large Critical Infrastructure Provider

By leveraging continuous breach and attack simulations, this large critical infrastructure provider was able to:

- **Develop targeted detections** based on real-world threat emulation.
- **Break down silos** between threat intel, engineering, and security operations (SOC) teams, creating a unified feedback loop.
- **Evaluate the efficacy of new detection tools** and configurations before full deployment.
- **Integrate BAS results into executive metrics,** tracking detection improvements over time.

This organization's detection engineering team used SafeBreach not just to validate assumptions, but also to operationalize threat detection across teams and initiatives—transforming insights into measurable, resilient defense strategies.

Why It Matters: Risk & Resilience for the Enterprise

The SafeBreach Exposure Validation Platform helps CISOs shift the narrative:

- From “We test rules” → to “We prove whether detections reduce breach risk.”
- From speculative scores → to validated evidence of resilience.
- From reactive audits → to continuous assurance, aligned with frameworks like DORA and NIS2.

SafeBreach operationalizes resilience by ensuring rules work, alerts flow, and gaps are closed before attackers exploit them to achieve outcomes like:

- **Risk Clarity:** Translate detection gaps into breach likelihood and control failure rates.
- **Strategic Justification:** Back investment decisions with validated detection data.
- **Audit Confidence:** Prove resilience to regulators and boards with evidence-driven reporting.

Get Hands-On with the SafeBreach Platform

Schedule a personalized demo today to learn why enterprise security leaders choose SafeBreach Propagate to enhance the quality, efficacy, and value of their security programs.

ABOUT SAFEBREACH

SafeBreach is the leader in enterprise-grade exposure validation, providing the world’s largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach Exposure Validation Platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit www.safebreach.com.

SafeBreach

US Headquarters

526 W Fremont Ave #2880
Sunnyvale, CA 94086

Israel Offices

HaMasger St 35, Sky Tower, Floor 8
Tel Aviv-Yafo, Israel

SAFEBREACH.COM