SafeBreach

Detection Engineering with SafeBreach

Validate custom detections, alert pipelines, & incident response processes at scale.

Detection engineering teams are often tasked with customizing security controls to better detect specific advanced TTPs and IOCs. But validating these custom detections can be extremely time-consuming and may not necessarily ensure the environment is protected, as many enterprises also rely on an alert pipeline to promptly deliver alerts from security controls to incident responders. As with any technology, alert pipelines can break in unknown and undiscovered ways. The SafeBreach breach and attack simulation (BAS) platform can streamline the entire detection engineering process by helping:

Reduce the Need for Manual Validation

Enable detection engineers to more easily run advanced attacks or create custom attacks that are triggered automatically to continuously validate custom detections at scale.

Create End-to-End Alert Pipeline Visibility

Utilize a closed-loop testing approach that triggers alerts, simulates response actions, and validates outcomes across the entire alert pipeline.

Enhance Confidence in Detection Capabilities

Validate that security teams can detect and respond to threats efficiently by proactively identifying alerting issues before they become critical.

Testmonials

"With SafeBreach, we run daily health checks to ensure our alert pipeline is running properly from A to Z. It's increased confidence that our incident responders are notified quickly when an actual threat is detected."

Principal Cyber Threat Engineer
Fortune 500 Financial Services Provider

Rediscover Your Defenses with a Powerful BAS Platform

The SafeBreach BAS platform continuously simulates real attack scenarios to help enterprises validate the efficacy and resilience of their security ecosystem. SafeBreach extends this visibility to the detection engineering process, helping security teams proactively monitor the integrity of their custom detections and alert pipeline by:

Simplifying Custom Attack Creation

Easily create advanced attacks—by modifying existing playbook attacks via **SafeBreach Studio** or utilizing tools like threat intelligence, packet capture (PCAP), and Python scripting—that run automatically and continuously to ensure custom detections are triggering alerts appropriately.

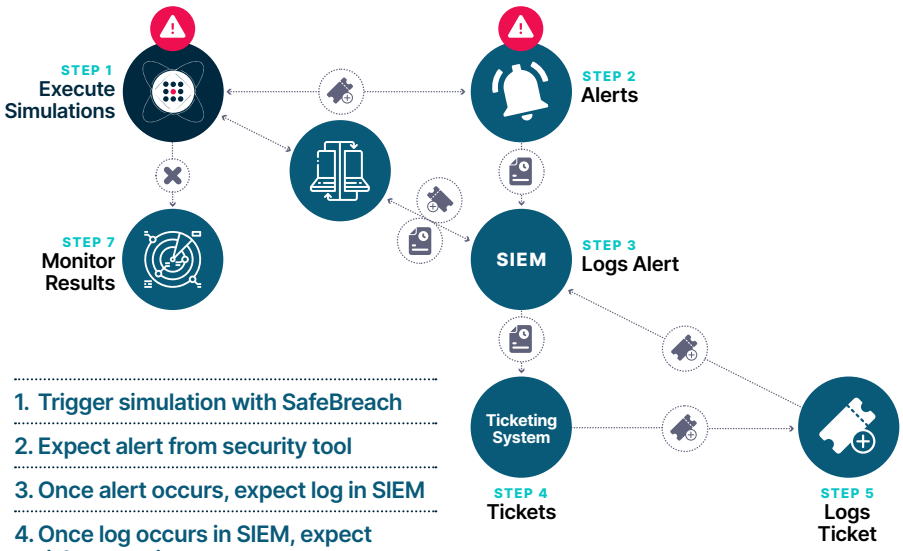
Validating All Components in the Alert Pipeline

SafeBreach simulations test the entire alert cycle—validating controls function properly, logs are sent to the SIEM, tickets are issued to incident responders when appropriate, and all integrations are active—to detect issues that can create false positives or delay necessary response.

Eliminating the Guesswork in Alert Pipeline Readiness

The continuous nature of SafeBreach attack simulations means you can run health checks as often as you wish, so alert pipeline breakage never goes undiscovered and you'll always know the entire pipeline is ready if a security incident occurs.

Alert Pipeline Validation Workflow



1. Trigger simulation with SafeBreach
2. Expect alert from security tool
3. Once alert occurs, expect log in SIEM
4. Once log occurs in SIEM, expect ticket creation
5. Once ticket occurs, expect log in SIEM
6. Correlate logs to simulation
7. Monitor simulation results for deviations

The SafeBreach Advantage

- **Largest attack playbook in the industry, with 30,000+ attack methods**
- **Only BAS vendor providing a 24-hour SLA for US-CERT and FBI Flash alerts**
- **Widest MITRE ATT&CK coverage of any BAS platform**
- **Scalable, enterprise-ready platform with simple deployment**
- **Broad technology partner ecosystem to support integration with existing controls and business systems**
- **Award-winning customer success team to help deploy and manage your BAS program**

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