What is breach and attack simulation?

Breach and Attack Simulation (BAS) is an automated way to test security controls by safely replaying known adversary techniques, mapped to frameworks like MITRE ATT&CK, against a live environment and measuring the result. It answers whether prevention controls block each technique and whether monitoring logs and alerts on it. BAS is one capability within adversarial exposure validation. It is broader and more repeatable than a point-in-time test but narrower than full attack path validation, because it replays individual techniques rather than always chaining them into a complete intrusion.

HOW IT WORKS

01 How does BAS work?

A BAS run follows a simple, safe loop:

- Select techniques. Choose the ATT&CK techniques relevant to your threat model, for example credential dumping, lateral movement, or data exfiltration.
- Execute safely. Run each technique in a controlled way that emulates the behavior without causing real damage.
- Measure prevention. Record whether the endpoint, network, or email control stopped it.
- Measure detection. Record whether the activity reached the SIEM and produced a real alert, not just a buried log line.
- Repeat. Because controls drift and content updates, the value comes from running it continuously, not once.

02 BAS vs pentesting vs attack path validation

These are complementary, not interchangeable:

- Penetration testing is human-led and creative; it finds novel, business-logic, and chained flaws a script would miss, at a point in time. (What a pentest is.)
- BAS is automated and repeatable; it measures control effectiveness against known techniques, continuously and consistently.
- Attack path validation chains techniques into a full route to a crown-jewel asset, showing not just whether a technique works but whether an attacker could reach the objective.

SOURCES

[1] MITRE ATT&CK Framework

[2] MITRE ATT&CK Techniques

[3] NIST SP 800-115 Technical Guide to Information Security Testing

All three sit under adversarial exposure validation, the practice of proving real exploitability against live defenses.

03 What does BAS prove?

A healthy BAS program surfaces problems a vulnerability scan never will:

- Prevention gaps. Techniques that pass straight through controls you assumed were blocking them.
- Detection gaps. Behavior that is logged but never triggers an alert, the difference between visibility and actual detection.
- Control drift. Protections that worked at deployment and quietly stopped working after an update or config change.
- Coverage over time. A trend line of how effectiveness changes, so regressions are caught early.

04 How do you get started with BAS?

Begin with the techniques most used against your sector rather than trying to cover all of ATT&CK at once. Validate both prevention and detection for each, fix what fails, and re-run to confirm the fix held.

BAS can run through in-house tooling or a continuous automated validation platform. Pair it with periodic human penetration testing so you get both the repeatable measurement of BAS and the creativity of a skilled tester.

Measure what your controls actually block and detect.
securelayer7.net/learn/pentest/what-is-breach-and-attack-simulation

Open online