SafeBreach

Operationalize MITRE ATT&CK™ Framework

Learn how cybersecurity teams are leveraging MITRE ATT&CK Framework.

Challenges

Cybersecurity teams face an overwhelming and rapidly expanding landscape of threats. Two very useful tools have been established to help confront them:

1. MITRE ATT&CK framework and knowledge base.
2. Breach and Attack Simulation (BAS) solutions.

First, a look at some of the most pressing security challenges:

- How can we communicate within the cyber community in common terms?
- Can our security operations function and perform at the same speed as our adversaries?
- How can we validate our security posture effectively against TTPs to report to various stakeholders?
- What are the best practices for prioritizing the long list of security gaps based on the business risk?

The MITRE ATTACK™ Knowledge Base is Indispensable

MITRE ATT&CK framework is a knowledge base of Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) that was created by MITRE Corporation. The framework organizes and categorizes thousands of threats, with more added continually, and it provides a "landscape map" that lets security teams apply their resources on a more informed basis.

Organizations can structure their investigation of threats more strategically, based on MITRE's phases of an adversary's lifecycle and the platforms they are known to target. That leads to another challenge:

How do you get from consulting the MITRE ATT&CK knowledge base to verifying that your infrastructure is well protected?

It takes more than traditional penetration testing.

Breach and Attack Simulation is Ideal for Use with MITRE ATT&CK™

An automated platform that can intelligently scale for continuous breach and attack simulation (BAS) is the only practical mechanism to stay consistently ahead of data breaches. A well-designed BAS system, supported by rigorous and extensive threat research, is the ideal vehicle to leverage MITRE ATT&CK framework.

- BAS validates all defenses continually against the full range of MITRE ATT&CK threats drawing on a playbook of executable attack methods.
- By continually simulating breach methods and mapping to MITRE ATT&CK framework, BAS exposes gaps that appear if a security tool is misconfigured or a patch is not installed.
- Constant research keeps the attack playbook growing. As new types of attacks are discovered, the execution methods to simulate them are added.
- BAS must run in production for accuracy but never impact data or compromise the actual production environment.

Operationalize MITRE ATT&CK™ Framework

SafeBreach: Advanced BAS with Prioritization of Remediation

SafeBreach is a leader in BAS technology, with the best coverage of MITRE ATT&CK threats. Its Hacker's Playbook contains over 10,000 breach methods. Companies deploy SafeBreach to:

- Simulate attacks against your production environment based on all SafeBreach Hacker's Playbook™ attacks, specific ATT&CK tactics, and techniques, or run attacks based on a threat group.
- Let security teams focus time and skills upon critical situations, and build original attacks against specific threats, with SafeBreach Breach Studio.
- Rank security gaps based on their potential impact, prioritize remediation work, safeguard the crown jewels, and prevent a catastrophic breach.
- Visually depicts attack paths within the infrastructure.
- Produce a threat intelligence-based view of the organization's security posture, based on the organized structure of the MITRE ATT&CK framework.
- Define a prioritized remediation plan based on breach method test results.

Learn More

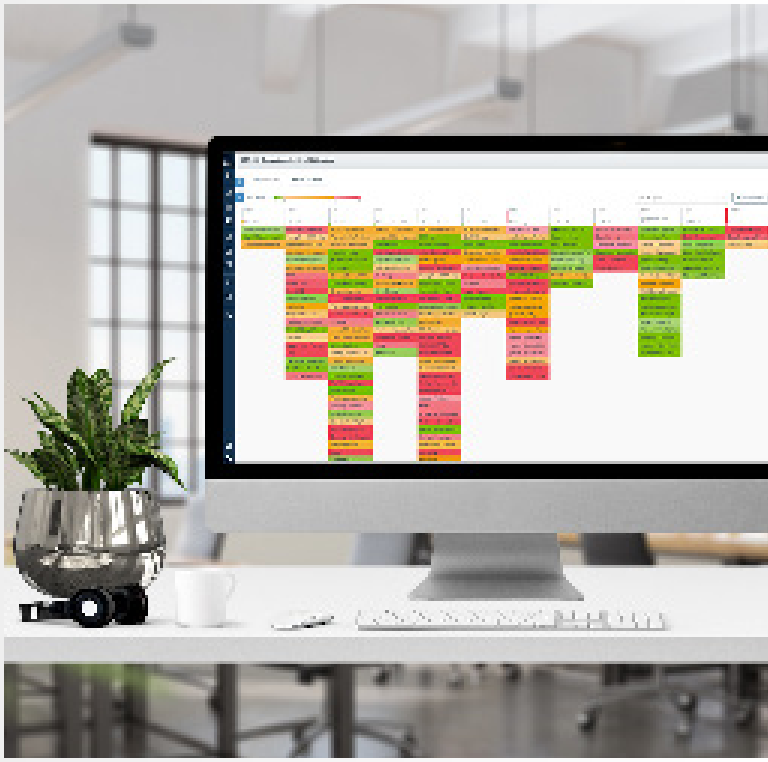
To understand how SafeBreach simulates thousands of attacks and permits the best leverage of MITRE ATT&CK Framework, download the SafeBreach MITRE ATT&CK Technical Brief.

Request a Demo

Here

Security teams can run BAS 24x7, filtering results by ATT&CK tactics, techniques or threat groups to validate their security posture and expose security gaps.

BAS provides a practical, highly flexible means to put MITRE ATT&CK to work. In turn, the framework provides structure to apply BAS for maximum improvement to security posture across the kill chain.



Highest MITRE ATT&CK Framework coverage in the industry

SafeBreach

Contributors to the MITRE ATT&CK framework

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

SafeBreach Labs, the security research arm of SafeBreach, and SafeBreach CTO Itzik Kotler, are also contributing partners to MITRE. SafeBreach Labs is a team of widely recognized ethical hackers, who have contributed to not only MITRE ATT&CK, but who have also contributed novel attack techniques at industry events and conferences such as Black Hack, DefCon, Hack in the Box, RSA, and more. Always adding to the Hacker's Playbook™ of attack methods, SafeBreach Labs continues to work with MITRE to identify new ways that attacks can be carried out, to help defender stay up-to-date, and prepared for proven, emerging, and new techniques in the wild.