

WHITE PAPER

Getting Started with MITRE ATT&CK[®] Framework and SafeBreach

Everything your enterprise needs to operationalize the MITRE ATT&CK framework

Contents

| | |
|---|----|
| Executive Summary | 3 |
| What is the MITRE ATT&CK® framework? | |
| How does MITRE ATT&CK help protect businesses and enterprises? | |
| MITRE ATT&CK and SafeBreach | |
| <hr/> | |
| Leveraging MITRE ATT&CK for Threat Informed Defense | 4 |
| ▪ Threat intelligence | |
| ▪ Detection & analytics | |
| ▪ Adversary emulation & red teaming | |
| ▪ Assessment & engineering | |
| Assessment and engineering | |
| Challenges in operationalizing MITRE ATT&CK | |
| Simulating MITRE ATT&CK TTPs using breach and attack simulation (BAS) | |
| <hr/> | |
| Operationalize MITRE ATT&CK with the SafeBreach Platform | 6 |
| Safely execute attacks | |
| Explore heat map results | |
| Dive into the details | |
| Leverage pre-built MITRE dashboards | |
| Establish & track your security baseline | |
| <hr/> | |
| SafeBreach & Tidal Security | 10 |
| <hr/> | |
| Conclusion | 11 |
| <hr/> | |

Executive Summary

What is the MITRE ATT&CK® framework?

Historically, cybersecurity practitioners protected their networks by building them into fortresses—erecting digital walls with tools that blocked all unwanted intrusions. In the last several decades, however, attackers have found their way around, under, and through those walls using ever-more sophisticated methods. As a result, there has been a massive shift toward a more threat-informed strategy, which allows security teams to not only protect against these attacks, but also detect and mitigate them before they are able to do any damage to the network or to the business.

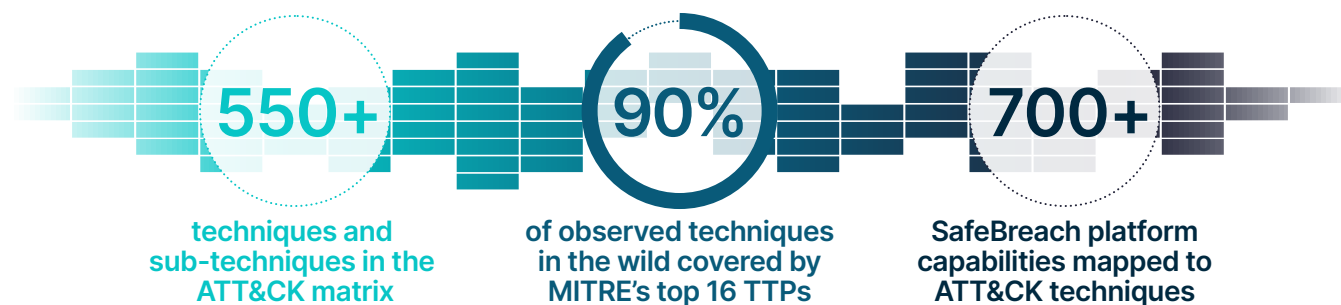
At the center of this shift is a framework called MITRE ATT&CK, which allows security teams to classify these advanced attacks and identify the tactics, techniques, and procedures (TTPs) used in order to assess their risk.

How does MITRE ATT&CK help protect businesses and enterprises?

With the threat information provided by MITRE ATT&CK, teams can be much more proactive in their ability to identify and mitigate potential threats. It gives security practitioners across multiple teams the ability to speak a common language and correlate threats against a common framework, allowing them to optimize threat detection and response. In short, it enables organizations to put a mirror up to their security program and better understand which security gaps need to be fixed in order to strengthen their defenses and withstand cyberattacks.

MITRE ATT&CK and SafeBreach

SafeBreach simulates attacks across various tactics and techniques (based on behavioral factors and indicators of compromise [IoC]) included in the MITRE ATT&CK framework, to validate security policy, configuration, and effectiveness. SafeBreach was an early contributor to the ATT&CK framework, with our initial contributions spanning methods for exfiltration, evasion, and command and control. Since then, SafeBreach has continued to leverage the framework to allow organizations to quickly visualize their security posture and bring security and infrastructure teams together to update security controls and more effectively harden defenses.



Leveraging MITRE ATT&CK for Threat-Informed Defense

Starting out with MITRE ATT&CK can seem daunting, considering there are over 193 techniques and 401 sub-techniques in the framework (as of ATT&CK v12). The thoroughness of the framework can make it difficult for teams to decide where to focus and what to prioritize. What's more, many teams are limited by time, budget, and personnel shortages that make it even more difficult to ensure full coverage.

We'll address the challenges shortly. First, let's look at how organizations typically leverage ATT&CK. ATT&CK has four primary use cases:



Threat Intelligence



Detection & Analytics



Adversary Emulation & Red Teaming



Assessment & Engineering

THREAT INTELLIGENCE

MITRE ATT&CK provides information about potential attack vectors and the adversaries known to use them. It also gives analysts a common language to use when describing adversary behavior in reporting, avoiding the headaches caused by varying interpretations amongst analysts. This normalization and structure allows the larger security community to compare adversary groups to themselves, to other groups, and to defenses, making the threat intelligence actionable.

Using the information provided within the framework, both analysts and defenders can structure their information using ATT&CK. Analysts can structure intelligence about adversary behavior, and defenders can structure information about what behavior they can detect and mitigate. By overlaying these two (or more) groups of information, security teams can create a threat-based awareness of what gaps exist within their networks and then determine whether their existing defenses are capable of detecting and responding to attacks by known adversaries.

DETECTIONS & ANALYTICS

ATT&CK helps cyber defenders develop a thorough understanding of attacker techniques and tactics, which in turn allows them to build better detection models. Rather than simply identifying known risks and blocking them ad-hoc, ATT&CK-based detections involve collecting log and event data about the attacker's behavior, mapping it to the framework. This facilitates the development of a comprehensive protection model that can potentially account for all known TTPs leveraged by the attacker, thereby potentially limiting the damage caused by the attacker.

Of course, not all unusual behaviors are malicious in and of themselves. Additionally, if alerts were triggered for every potentially suspicious behavior, this would quickly generate a lot of noise, create alert fatigue, and slow down threat detection. By correlating suspicious alerts using the MITRE ATT&CK framework, security teams can quickly identify potentially malicious intent and determine viable remediation options.

Data used to develop analytics can be gathered from various sources:

- Authentication logs
- File and registry monitoring
- Packet capture—especially east-west capture—such as that collected between hosts and enclaves in your network
- Process and process command line monitoring

Once a team has this information, they will need to collect that data into some kind of alert logging platform (SIEM) in order to run analytics against it. This may already exist as part of IT or security operations, or it might be something that needs to be developed. Once that data is there, teams can leverage threat intelligence to prioritize behaviors that they want to detect within the SIEM. Ultimately, the goal with this use case is to be able to detect an attack early in the attack lifecycle and across the entire kill chain.

ADVERSARY EMULATION & RED TEAMING (OR PURPLE TEAMING)

Adversary emulation is a type of red team activity that mimics known threats to an organization by incorporating threat intelligence to define what actions and behaviors the red team uses. This is what differentiates adversary emulation from penetration testing and other forms of red teaming.

ATT&CK can be used to test and verify defenses against common adversary techniques by enabling security teams to create adversary emulation scenarios. Adversary emulators construct scenarios to test different aspects of an adversary's TTPs. The red team then follows the scenario while operating on a target network to test how defenses would hold up against the attacks.

ASSESSMENT & ENGINEERING

MITRE ATT&CK can be used as a framework for a defensive gap assessment. Analysts can check to see if each potential attack vector applies to the organization and if solutions are in place to detect and protect against it. Once an organization assesses its capabilities and gaps using ATT&CK, it can easily communicate these results to key stakeholders to provide them with a high-level view of organizational readiness and make appropriate decisions to improve organizational security posture.

These gaps would typically be difficult to discover because they require looking for what isn't there. MITRE ATT&CK provides a comprehensive list of methods by which attackers can achieve their objectives at each stage of the cyberattack lifecycle, including a list of methods to detect and defend against these techniques.

Challenges in operationalizing MITRE ATT&CK

The MITRE ATT&CK framework is a powerful tool for enhancing cybersecurity, but as we mentioned previously, implementing it can be a challenge. Not only does the framework require a significant investment of time and resources to implement it effectively, but there is also a need for familiarity and expertise to operationalize it effectively.

Security teams constantly debate whether they should test against all techniques listed in the ATT&CK framework, or focus on just a few to start. Best practices indicate that the latter is the more strategic option, though concentrating the team's work on a specific set of attacks could instill a rigid tactical perspective that is counterproductive and wastes the flexibility afforded by the MITRE ATT&CK framework.

Should the team focus on TTPs for threat groups that are most impactful to your organization? If so, when a security gap is exposed, do you redirect your teams to remediate, or continue testing the TTPs? This may depend on how quickly the IT team can address the gap and remediate the problem. But once that is done, when should the security teams rerun the tests to ensure the security gap is resolved?

This back and forth can cause conflict between teams, deprioritize important security responses, and frustrate the security teams when their hard work is not effective in securing the organization.

Simulating MITRE ATT&CK TTPs using Breach and Attack Simulation (BAS)

If your organization is considering adopting ATT&CK or is struggling to be effective while leveraging the framework, breach and attack simulation (BAS) can accelerate your approach, reduce manual steps in operationalization, and measure the impact of the team's efforts.

An automated platform that can intelligently scale for continuous breach and attack simulation is the only practical mechanism for staying consistently ahead of data breaches. By leveraging a well-designed BAS platform that's supported by rigorous and extensive threat research, security teams (regardless of their security maturity) can easily operationalize the MITRE ATT&CK framework. Advantages include:

- The ability to leverage a constantly updated attack playbook to continuously validate all deployed defenses against various attacker TTPs listed in the MITRE ATT&CK
- The ability to simulate advanced threats and quickly identify security gaps arising from security control misconfigurations
- The ability to easily execute a full kill chain attack and carry out performance analyses based on specific tactics and techniques

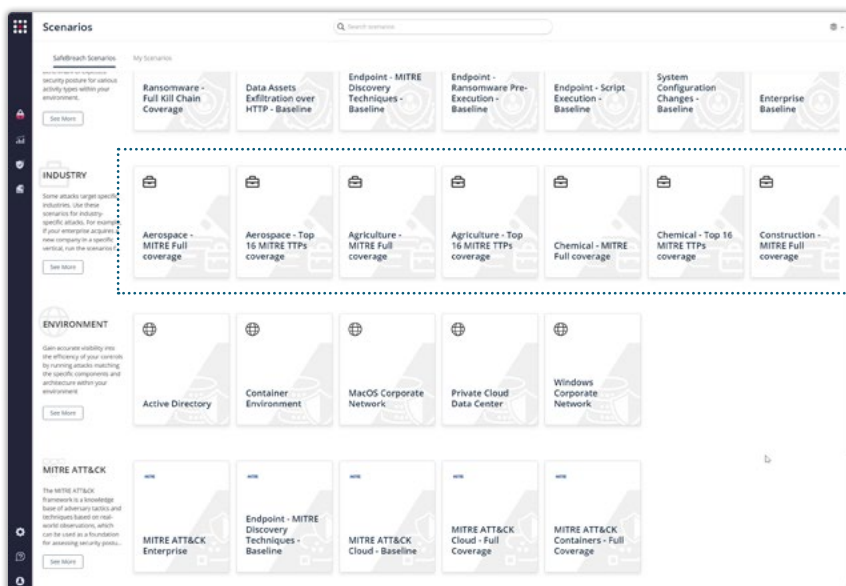
Operationalize MITRE ATT&CK with the SafeBreach Platform

SafeBreach is a pioneer in BAS technology and boasts the best coverage of MITRE ATT&CK threats in the industry. Its Hacker's Playbook currently consists of over 28,000 breach methods and is continuously updated upon the discovery of new threats. Enterprises operationalize the MITRE ATT&CK framework with SafeBreach to:

- Safely simulate attacks against their production environment based on all playbook attacks, specific MITRE ATT&CK techniques and sub-techniques, or attacks based on a particular threat group;
- Produce a threat-intelligence-based view of the organization's security posture, based on the organized structure of the MITRE ATT&CK framework;
- Effectively communicate overall organizational risk exposure based on the ATT&CK framework, as well as risk by each MITRE tactic.

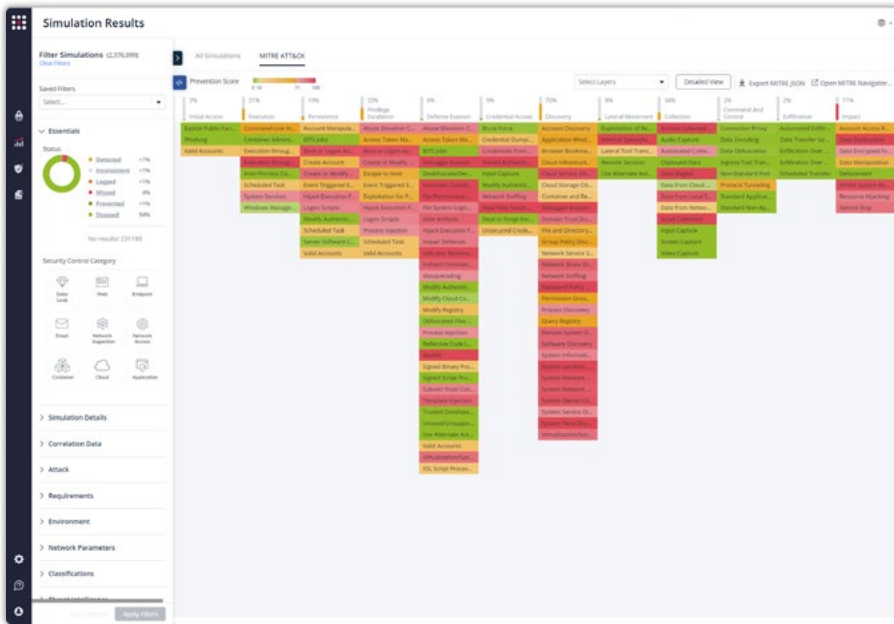
Validate Organizational Security against Top MITRE TTPs

The SafeBreach platform enables security teams to run vertical-focused / full-kill chain attack simulations against production environments based on TTPs identified in the MITRE ATT&CK framework. **SafeBreach also allows organizations to validate their deployed security controls against the top 16 TTPs listed in the MITRE ATT&CK** framework specific to their vertical/industry. These TTPs make up 90 percent of the observed techniques from April 2019 to July 2021.



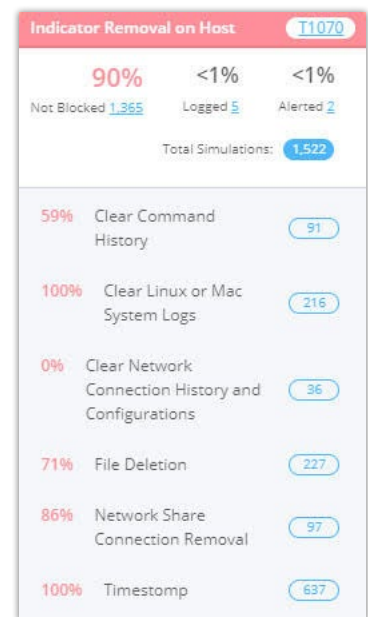
Explore Heat Map Results

SafeBreach's MITRE ATT&CK board mirrors the MITRE ATT&CK Enterprise Matrix, while providing context for each technique and tactic based on the simulation results from your environment. The interactive heatmap helps organizations quickly visualize their security posture, focus on the areas most in need of remediation, and bring security and infrastructure teams together to update security controls and more effectively harden defenses. Security teams also have the ability to export simulation results as a .json file and upload it to **MITRE ATT&CK Navigator** (a web-based tool used to visualize defensive coverage, red/blue team planning, and the frequency of detected techniques).



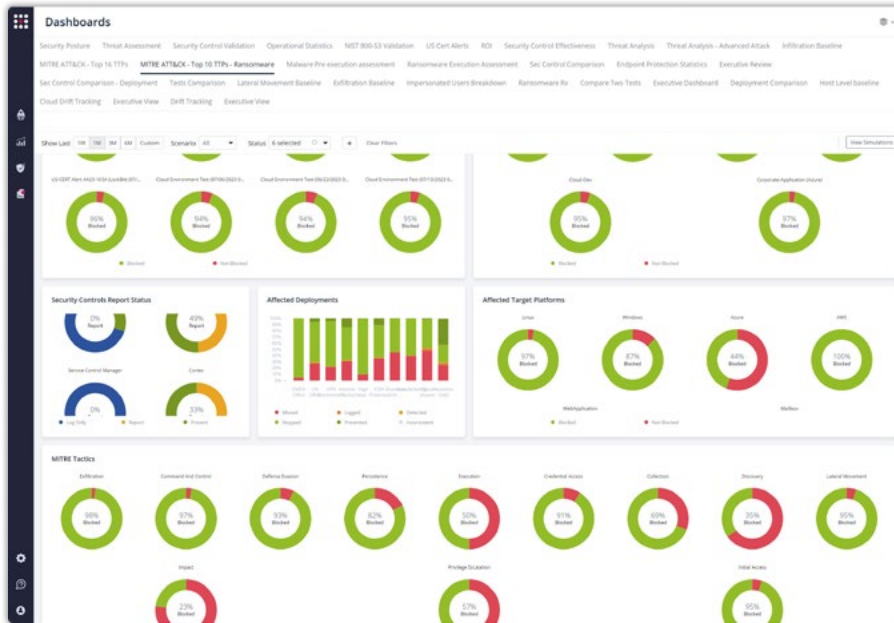
Dive into the Details

Utilize built-in tactical risk summaries with in-depth information about each MITRE ATT&CK technique and sub-technique, including links to relevant MITRE content, the ability to drill down into indications of the risk, number of simulations missed and logged, and more.



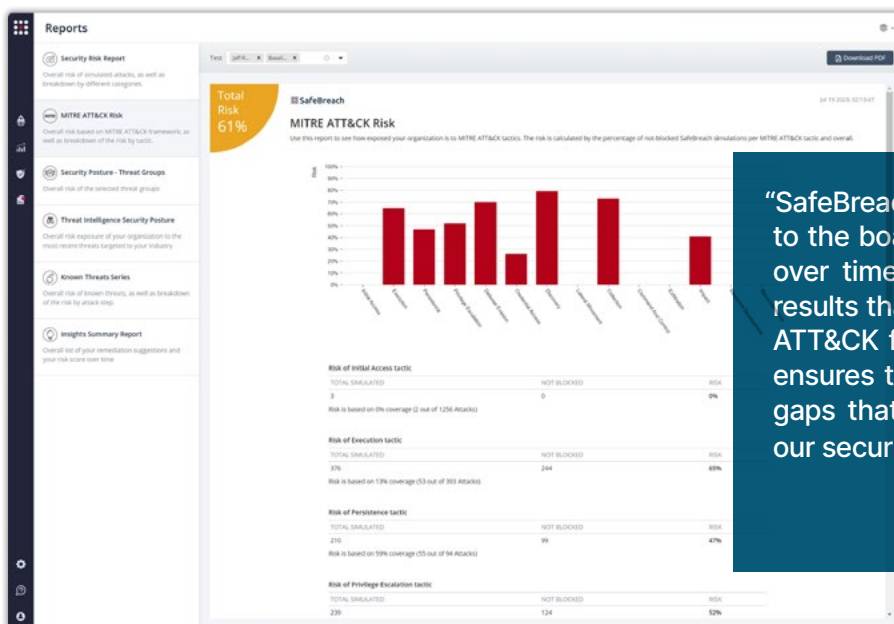
Leverage Pre-Built MITRE Dashboards

Visualize simulation results and MITRE-level mitigation and detection guidance, so you can quickly understand gaps, communicate with key stakeholders, and take meaningful action to reduce mean time to detect or discover (MTTD) and mean time to respond (MTTR). By adding MITRE-level mitigation and detection guidance to the dashboard, customers can gain a complete MITRE workflow for operationalizing the MITRE ATT&CK framework.



Establish & Track Your Security Baseline

Assess, track, and report on your organization’s overall risk score to create a baseline for continued testing and keep your team focused on performing actions that reduce the risk score over time.



“SafeBreach is instrumental in our reporting to the board to show we are reducing risk over time. Our teams monitor the attack results that are heat mapped to the MITRE ATT&CK framework. The detailed visibility ensures they are remediating the security gaps that are most important to improve our security posture.”

CISO
U.S. Security Services Corporation

SafeBreach & Tidal Security



As part of our dedication to engaging with the larger security community to ensure we're providing the maximum possible benefit, SafeBreach maintains a partnership with Tidal Cyber. Tidal was founded by a trio of senior leaders from MITRE with the mission of helping enterprises implement a threat-informed defense.

The SafeBreach + Tidal Cyber partnership enables users of the Tidal platform to quickly map the breadth and depth of coverage in SafeBreach's BAS platform against the adversary tactics and techniques of MITRE's ATT&CK knowledge base. Users of Tidal's free Community Edition can simply add SafeBreach to their matrix from the product registry and instantly visualize our ATT&CK coverage.

Conclusion

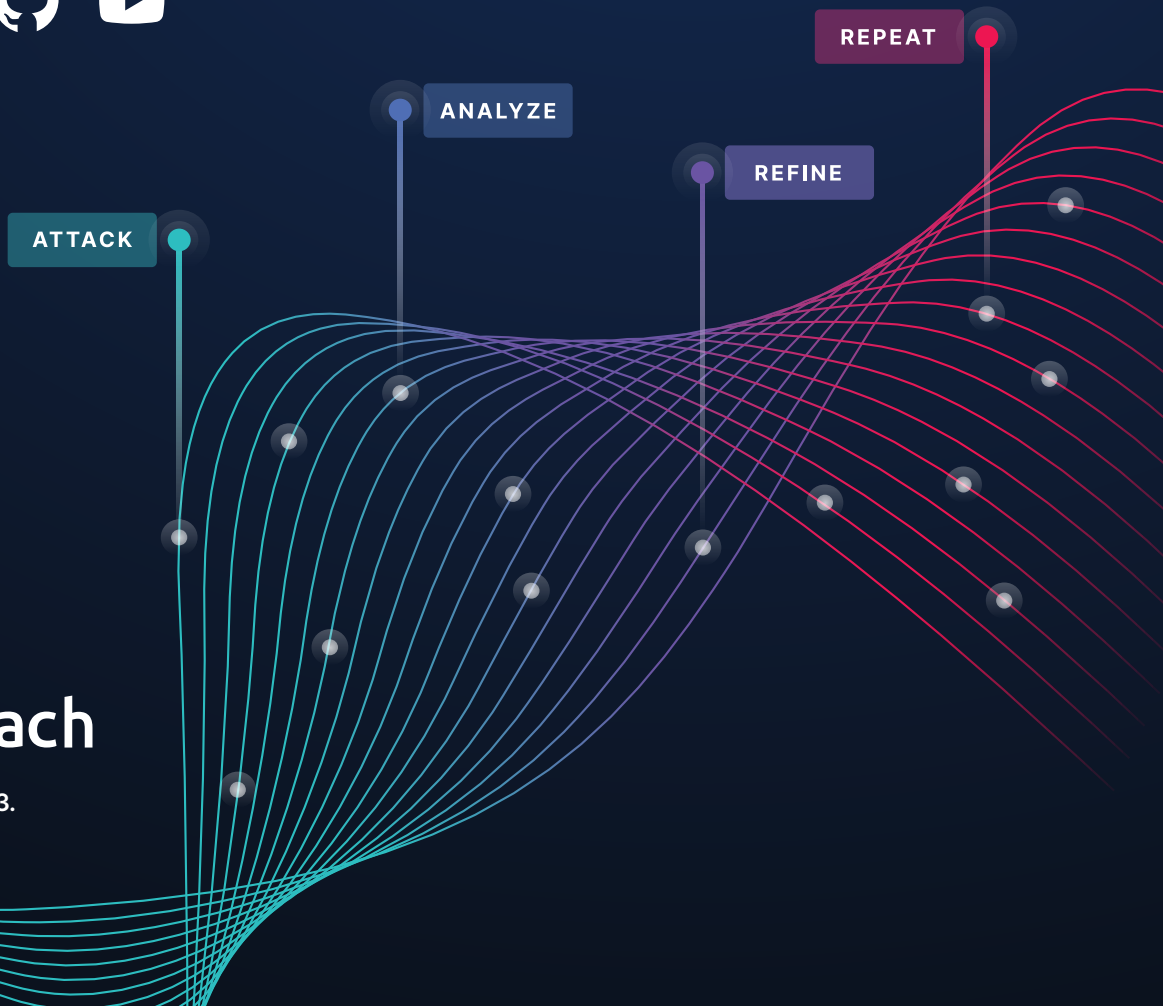
The MITRE ATT&CK framework is one of the foundational elements used to help security teams build a proactive, threat-informed defense. It is made even more powerful through the use of a breach and attack simulation platform as a part of a larger CTEM (continuous threat exposure management) program. BAS expedites the implementation of the ATT&CK framework and allows security practitioners to operationalize and report on the effectiveness of its implementation.

As adversaries continue to grow ever more sophisticated in their attacks and TTPs, both MITRE and the SafeBreach BAS platform will continually add and update our playbooks with the latest research and information, keeping our customers and our community prepared for today's biggest cybersecurity risks.

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at SafeBreach.com.



 **SafeBreach**

All content © SafeBreach 2023.
All rights reserved.