SafeBreach

WHITE PAPER

The Fundamentals of Modern Cybersecurity Red Teaming

An exploration of early-stage cybersecurity red-team considerations and guidance

SAFEBREACH.COM

Contents

Understanding What Red Teams Do 4

The Goal of Red-Team Testing 4

Weaknesses of Red-Team Methodology 5

Building & Aligning the Red Team 6

Align Red-Team Goals with Overall Business Goals 6

Select the Team 6

Create Team Relationships 7

Determine Specific Rules of Engagement & Scope 7

Selecting the Red-Team Arsenal 8

Set Up the Environment 8

Choose the Tools 9

RECONNAISSANCE TOOLS 9

NETWORK ACCESS & ANALYSIS TOOLS 10

BAS TOOLS 11

Executing the First Exercise 12

Positioning Your Team for Scalable Growth 12

Set Clear Goals 12

Determine Outcome Metrics 13

Establish a Repeatable Methodology 13

Prioritize Reliable Automation 14

Looking Toward the Future: Continuous Red Teaming 14

Introduction

The name “red team” originates from 19th-century German military preparedness exercises conducted as realistic board games between two adversaries operating under time constraints and certain rules. In cybersecurity, red-team exercises—also often called adversarial simulations—involve a simulated adversary attempting to gain access to sensitive and protected IT assets, data, networks, and other technology elements.

> **RED TEAM**
>
> “A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The red team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the blue team) in an operational environment.”
>
> **– National Institutes of Standards and Technology (NIST)**

Cyber red team exercises have long been a staple of organizational security practices, **dating back to 1997** when they were first employed by the National Security Agency (NSA) to test the federal response against cyberattacks on critical infrastructure networks. Some chief information security officers (CISOs) at larger organizations maintain standing red teams to regularly and repeatedly simulate attacks against cyber defenses. Other CISOs contract with third-party red-team experts for annual or semiannual exercises.

This paper will explore key high-level topics around red teams, including what they do, their goals, and what weaknesses exist in their methodology. We’ll discuss some of the foundational steps that can help you build a more modern red-team program, including how to identify the correct personnel, operationalize their skills, and align their activities with the overall goals of the business. We’ll also dive into the technology considerations necessary to enable a red team, including environment setup and tool selection, executing your first exercise, and positioning your team for scalability. Finally, we’ll discuss how your red team can move toward a more continuous approach by leveraging breach and attack simulation (BAS) systems.

Understanding What Red Teams Do

Red teams may combine cyberattacks with social engineering and attempts to physically infiltrate organizations to access or steal devices, gather information, or place mechanisms to capture data.

Red-Team Exercises Test:

Technology defenses

Red teams use common tools, such as network scanners and penetration-testing programs, to probe networks, devices, IP addresses, and APIs for potential vulnerabilities. In addition to using commonly available tools, sophisticated red teams may also use custom tools to simulate an advanced attacker. They may target any publicly addressable system, including hardware, software, routers, switches, and smart peripherals.

Human defenses

Red teams will direct attacks at humans, including phishing emails, browser-activated malware, SMS messages with links containing malware, and even phone calls or chat requests to reset passwords or supply sensitive information. Anyone within an organization may be tested, including staff, partners, and those with access to networks, software, hardware, cloud infrastructure, or APIs.

Physical defenses

More recently, red teams also include tests of physical security measures and controls. This might include access controls for offices or data centers, requests for after-hours entry at key facilities, and even surveillance to look for weaknesses in security coverage at entrances, gates, and other access points.

The Goal of Red-Team Testing

Rather than merely testing one-off security controls like a firewall or an antivirus system, red-team testing is more holistic in nature and designed to test the security posture of organizations and their employees. Beyond the posture, the exercise is designed to test responses and adaptations that illuminate how well people and systems adjust to hostile acts. This is a critical difference from simple penetration testing (although red teams usually incorporate some elements of penetration testing), which is an exercise to penetrate cybersecurity defenses that is generally focused only on the technology and not on the people. This form of testing is more circumscribed and is not conducted in a war-game format.

94%

of organizations that run red-team testing gain some level of successful penetration.

Deloitte.

In contrast, a red team exercise not only identifies security flaws and seeks to penetrate defenses, but also tests how the organization reacts and how effectively it responds to any successful attack. Most proficient red teams will figure out a way to exploit some flaw. Often, red teams are pitted against blue teams—their defensive counterpart tasked with detecting, responding to, and blunting cyberattacks. More recently, we have seen the emergence of purple teams, where red and blue teams are combined into a single unit that switches roles frequently to better learn from each other and to gain fresh perspectives.

Weaknesses of Red-Team Methodology

A key drawback of red-team testing is that it requires considerable expertise, financial resources, and coordinated planning. Organizations must synchronize multiple parties, create war-game environments and IT setups, develop or train on methods for preparation, and complete postmortems. Equally as important, red-team exercises are rarely, if ever, comprehensive and are not continuous.

Red-team exercises are human-directed, which can lead to some creative and unanticipated attack patterns and vectors, but also means they are limited to the cognitive abilities of human attackers. While they may include network scan results as a means of targeting, for example, they cannot exhaust all possible options because the exercises are time-bound. Red-team exercises are also usually tightly structured and focused on specific goals or targets, often using tactics of a specific type of attacker. This means the exercise can test only a limited subset of the actual attack surface, as a live adversary faces no such limits or time restrictions.

For these reasons, red-team exercises can only provide snapshots of an organization's security posture and may not be relevant or effective a few months or even weeks later. In modern software development processes, new code is added or existing code is changed daily or weekly. This creates new attack vectors and accelerates security drift, rapidly dating red-team findings and efficacy. The natural evolution of IT and applications also increases the exposed attack surface quickly with the growth of the Internet of Things (IoT), cloud computing, cloud-native software architectures, and distributed applications. This broader attack surface means red teaming can cover an ever-smaller portion of potential threats.

Building & Aligning the Red Team

Building a red team doesn't have to be complicated, but it does require a commitment to assembling the right people, processes, and technology. In this section, we'll discuss some of the foundational steps that will help you develop a modern red-team program.

Align Red-Team Goals with Overall Business Goals

The baseline rationale for red teaming is an improved security posture and reduced risk. It is worthwhile, however, to provide detailed guidance on how security risks map to the overall business risk and then design red-team exercises to match accordingly. For example, a CISO may be concerned about supply-chain risk and vulnerabilities in third-party libraries that could directly affect the enterprise. In this situation, the red team may want to design an exercise to attempt to identify third-party libraries in use by internal applications and determine whether those libraries have been properly patched and updated. While it's important not to limit exercises too tightly, focusing on specific areas of concern will allow deeper dives and provide better guidance on process changes that can eliminate root causes at the operational- or software-development level.

At a more strategic level, aligning the red team with broader business goals will help win broader budgets and buy-in. Cybersecurity organizations have traditionally struggled to communicate their proactive value to key stakeholders, including those in the C-suite and on the board. Linking red-team exercise metrics to key business objectives in a visible and measurable way is a critical step in ensuring the long-term viability and budget for these valuable programs.

Select the Team

The first step in building a modern red team is to identify whether you will build the team internally or start first with an outsourced team, which can offer a more feasible way to build a baseline, identify bias-free security gaps, and give you time to build internal buy-in and red-team capabilities inside your organization.

If you decide to build the team yourself, you'll first need to determine the size of your team and the types of experience you would like individuals to have. While it's typical to fill out a red team with security engineers, it's equally valuable to consider adding a fresh perspective with DevOps practitioners or application developers looking to try something different. It can also be helpful to mix internal hires who know your systems, applications, and environments with a few external hires who are seeing all of your IT assets and applications for the first time. Also, for key aspects of red teaming—such as social engineering and physical penetration—you will likely require external expertise, as few organizations train their security engineers in these disciplines.

Once you have made these team calculations, build a detailed budget that adequately reflects the costs to hire, train, and enable your team. This is a key step in building executive sponsorship and securing the resources necessary to ensure the success of your red team.

Create Team Relationships

Red team exercises are adversarial simulations that, if done properly, will induce better channels of communication between all involved personnel and teams as they work together to address a common threat. Make sure all the participants from the security team are known to each other and that there is an organizational chart that clearly outlines roles and responsibilities. Consider some in-person or live video conferences to break the ice. This can be an important step toward fostering relationships and creating an environment where learning is a shared goal and postmortems are relatively frictionless.

Equally important to consider are the other operational teams that should be involved, including network operations, IT, and DevOps. Each of these functional groups should be aware of red-teaming exercises and may even need to actively participate in exercises as well. You may also want to consider whether it makes sense to deploy a purple team strategy. Purple teams are a newer construct where the red team (typically tasked with attacking assets and infrastructure) and the blue team (typically tasked with protecting assets and infrastructure) may play either role in the exercise. As the industry trends toward a state of more frequent or even continuous red team exercises, be sure to also consider the resources required to create an ongoing program.

Determine Specific Rules of Engagement & Scope

The red team should work with all the other parties listed above to determine rules of engagement for any exercises. Ideally, the rules of engagement should be broad enough to allow for meaningful creativity and variation, while ensuring there are no surprises and that all participants understand they may be targeted.

Rules of Red-Team Engagement:

Time duration for the exercises

Targets that are allowed

Tactics, techniques, and procedures (TTPs) to include

For higher fidelity, red-team exercises should include key stakeholders all the way up to the C-suite. Smart attackers are increasingly targeting executives and top management with sophisticated attacks, even using deepfake voicemails and phone calls. Business email compromises that target finance teams can be one of the most damaging attacks, with millions of dollars in losses happening in a matter of minutes.

In addition, it's important to decide what information to provide the red team to help them target. This typically breaks down into three types of data access.

Red-Team Data Access:

White box access

Offers full or partial access to internal code and even scan or control configuration data.

Black box access

Offers zero access to red teams and is most analogous to attacks from the wild.

Gray box access

Offers a mixture of white box and black box access, with red teams getting access to certain types of information.

While it may sound counterintuitive, providing some upfront information can actually improve exercise efficiency and outcomes. While a white box exercise might provide the red team with details of applications and even patch status from software composition analysis testing that would not generally be available to attackers in the wild, it might help the red team more efficiently craft attacks for maximal educational impact and to stress the areas of focus in that given exercise.

Selecting the Red-Team Arsenal

Next, you'll need to assess what the arsenal of your red team should contain. For the most part, successful red teams mirror the tactics and tools of real-world adversaries, which may entail using open source or widely available software, providing the compute infrastructure necessary to mount credible attacks, and setting up separate cloud or sandboxed environments for safe red-team engagements. Rarely are purchases of expensive software or technology required, but the right tools can maximize a red team's efficacy. In this section, we'll explore the key technology considerations, including environment setup and tool selection.

Set Up the Environment

Red team environments should be set up in a simple, safe, and flexible fashion. The goal is to mimic the environment an attacker would face in the presence of a blue team, without disrupting live production systems or requiring significant configuration changes in firewalls and other security tools. If public cloud environments are used, it is critical to keep the service provider informed so as not to trigger their internal security tools and response protocols.

Above all, the security of sensitive data must be a top priority—any information that red teams dig up should always be encrypted whenever it is outside an organization's private data center. For this reason, it's best to install a command-and-control (C2) server on a machine in a private data center or, at a minimum, in a virtual private cloud (VPC). Smart red teams vary their look by using different cloud hosts, geographic locations and availability zones for data centers, DNS domains and registrars, and domain categories. Each aspect plays an important role in enabling the opportunity for multiple attack paths, so lue teams cannot easily find a single attack path and block traffic.

Choose the Tools

Red teams break down their tools and activities into a handful of basic functions that relate to the type of data access they are given to start the exercise (see previous descriptions for white, black, and gray box access). In more common black or gray box exercises, the red team approaches the exercise with little-to-no data access or knowledge about the target. In these situations, red teams will typically rely on tools for reconnaissance, access, and analysis. Fortunately, there are **dozens of free and open source tools**. A strong list can be found at **SecTools.org**. Many of the tools are built into common Linux distributions, as they have utility for network and systems administrators.

RECONNAISSANCE TOOLS

To build a picture of the components of the target, red teams use reconnaissance tools. Below, we've included a partial list of tools available for this purpose. While there are other open source tools for most of these capabilities, we have found these to be among the most popular.

Nmap is a commonly used network scanner that integrates with many popular security tools and frameworks. Red teams can use it to learn about the operating system, drivers, hardware, and much more to identify reachable devices on a target network.

Shodan functions as a search engine for Internet-connected devices and is particularly useful for finding poorly defended connected systems, like printers, smart monitors, bluetooth headsets, and more. Devices are often the easiest path to gain access into networks and trusted environments.

Slurp is a tool used to scan insecure AWS cloud storage buckets. With Slurp, red teams can scan by domain or keyword, looking for buckets that might have secret keys or other sensitive information that can be used to access AWS accounts.

Dnsrecon finds and identifies domain names and associated IP addresses on a target network. This is useful for attack targeting and for more sophisticated attacks leveraging weaknesses in DNS redirects or DNS misconfigurations.

NETWORK ACCESS & ANALYSIS TOOLS

Once reconnaissance efforts have provided a decent idea of the target and its security posture, red teams apply various exploit tools to crack passwords or mount social engineering attacks. After a red team gains access to protected assets, they then need to conduct internal analysis of the network and decide how to proceed to achieve their goal of system compromise, surveillance, or data exfiltration. Below, we've identified several popular tools that can be used by red teams as they attempt to exploit and breach systems.

```
   .        .
   \`-"'"-'/
    ] 6 6 [
   ==.  Y ,==
     /^^^\   .
    /     \  )
   (  )-(  )/     _
   -""---""---   /
  /   Ncat     \_/
 (      ____
  \_.=|____E
```

Ncat is a general-purpose tool for reading, writing, redirecting, and encrypting data across a network. It can perform a wide variety of security testing and administration tasks, including acting as a simple TCP/UDP/SCTP/SSL client and server to interact with web servers, telnet servers, mail servers, and other TCP/IP network services and the clients that use them. It can also act as a connection broker, a network gateway, and a proxy/redirect service to push traffic to other ports or hosts. Ncat is also useful for reconnaissance and is published by the same security expert who created Nmap.

Wireshark, built by a team at Sysdig, is a widely-used network protocol analyzer that provides packet-level insights into what's happening on a network. Wireshark lets you capture live traffic or analyze recorded traffic with a huge array of filters. It can parse all commonly used communications protocols and reads many common file formats for networking monitoring or security tools. Wireshark provides deep inspection of hundreds of protocols, with more being added all the time.

Aircrack-ng is a suite of tools with everything you need to analyze and crack Wi-Fi networks. It covers monitoring (packet capture and export to analysis tools), attacking (replay attacks, fake access points, packet injection), testing (checking Wi-Fi cards and drivers), and cracking for multiple security protocols, including WEP and WPA 1 and 2. A popular alternative is **Airgeddon**.

Hashcat is a password hash cracker that has GPU support, allowing it to brute-force any eight-character Windows password (the default minimum length) in a couple of hours. For Macs and Linux machines, **John the Ripper** is a viable alternative supporting hundreds of hash and cipher types.

Dradis is a reporting and collaboration tool used by information security teams to save time and ensure everyone is on the same page. The free community version has 19 integrations with widely used security tools, visual dashboards with charts and progress reports, one-click report generation, and easy access via the web.

BAS TOOLS

BAS has emerged in the past few years as a viable solution to augment red-team exercises, helping to expand coverage of the evolving attack surface and more accurately simulate the modern cybersecurity challenges faced by enterprises in keeping their applications, infrastructure, and data assets safe. BAS tools automate adversarial simulation, allowing security teams to rapidly test their applications and infrastructure for gaps and weaknesses against a wide range of exploits that may be used by attackers, including the newest and most relevant threats. BAS provides a systematic method to validate which security controls work and which attacks will not be blocked by defenses.

Because BAS tools are automated and run in a sandboxed environment segmented from actual production assets, they can run continuously to more closely emulate modern attack patterns and provide the type of consistent feedback required to fight security drift. This setup also allows BAS tools to cover far more of the attack surface—a broader coverage that enables red teams to provide metric-driven assessments of security posture based on business-centric risks.

In addition to adding elements of continuous testing and broader coverage, combining red-team exercises with automated BAS tools also allows organizations to improve the efficacy of red-team exercises. BAS tools provide the ability to scale and test against multiple scenarios, threats, and attackers at the same time and with fewer resources, so red-team experts can focus on specific, critical objectives or high-profile targets.

BAS tools can also export results into red-team tools for attack coordination. Red teams can use BAS to run precise targeted attacks, eliminating much of the required reconnaissance grunt work and freeing them to be more creative in their approaches. And, if the BAS tool continuously adds new vulnerabilities from leading databases and frequently upgrades attack playbooks and TTPs—**like the SafeBreach BAS platform**—red teams gain the benefit of using the latest security vulnerabilities as part of their exercises.

This, in turn, increases the security metabolism of organizations and reduces security drift by upping the frequency of security control testing and reconfiguration. In some cases BAS can even replace red-team tools, reducing overhead, while increasing coverage without adding headcount or headaches. Overall, adding a BAS tool to your red team's arsenal can make it possible to continuously run exercises more efficiently, at scale, and with fewer resources.

Executing the First Exercise

Once your team is in place, the environment is set, and the tools have been selected, it's time to execute your first red-team exercise. To start, it's helpful to pick a clearly defined and bounded target and rules of engagement. In other words, keep things relatively simple as you get used to the concepts and realities of red teaming in practice. Realistically, you'll want to plan for at least a month or two in advance. Document and aim for a repeatable process that can make red-team exercises quick and easy to stand up. Ideally, team members who have participated in red-team exercises before can help lead the project, set expectations, and get everyone up to speed quickly.

As a warm-up, you may want to run a simple penetration exercise as preparation for your first red-team exercise. Be prepared for a bumpy first time though, and don't be surprised if either red teamers or blue teamers get confused during the exercise. In fact, the entire goal of red teaming is to put real stress on the security teams and others who might be tested. Hold a cordial postmortem with both sides and ask for feedback on how to improve both the response to the simulated attacks and the red-team exercise itself. Keep in mind, this is just the beginning and there is room for growth and improvement.

To continually test and improve security posture and organizational response to live attacks, red-team exercises should be practiced on a continuous basis with a rotating set of participants. Cybersecurity is constantly evolving and so must your red-team exercises in order to continue to drive tangible results and map back to the objectives and business risks of an organization.

Positioning Your Team for Scalable Growth

Your business will constantly grow and change—so will your threat environment. Establishing a cybersecurity red team is critical to preventing attacks, but you will need to enact a longer-term strategy to ensure your red team's scalability and sustainability. Here are the five fundamental steps to help you prepare for the rising risks and overall threat landscape you'll face as your organization expands.

Set Clear Goals

First, you must clearly define the red team's goals around specific threat scenarios. To do this, it's important to develop a full understanding of the adversaries you face, including their past attacks, their preferred tactics and techniques, and the impact their attacks may have on your business. There are many threat intelligence services and resources—**like the MITRE ATT&CK framework**—to help identify which type of adversaries are targeting you based on your industry, geography, attacker motivations, and other factors.

Attacks produce a range of consequences—from data loss and business continuity disruption to reputational harm and financial damage—but not all will have the same level of impact on your business. Determine which attacks pose the highest risk to your organization, and prioritize your goals around those first. With a solid understanding of your business impact and adversaries, you can set focused goals around the threat scenarios most relevant to your business.

Determine Outcome Metrics

Tied closely with setting goals, your red team should have a measurable set of outcome metrics around your objectives. This starts with clearly defining the consumers (or stakeholders) of your red team's output and the types of deliverables they will need. Your red team's direct consumers may include your CISO, blue-team counterparts, or other representatives seeking quantitative risk data to inform compliance and investment decisions or strategies.

Once you know who you need to reach, you can then decide which deliverables will best meet their requirements, whether that's a high-level risk analysis or a pinpointed attack assessment. In producing these deliverables, it's key to create a common language all your consumers understand and agree upon. With this alignment in place, you can then demonstrate how closing the identified gaps will lead to quantifiable risk reduction and arrive at a clear set of outcome metrics to assess your red team's ongoing performance.

Establish a Repeatable Methodology

The threat environment is constantly changing, so the scalability of your red team will depend heavily on the repeatability of your methodology. Be prescriptive about your process from the outset, with an aim to build threat scenarios and launch attacks in a way that can be repeated continuously and at a frequency that enables you to achieve real-time risk-level monitoring.

Your repeatable red-team methodology should give you the ability to:

Attack effectively and efficiently, testing the full range of threat scenarios across relevant assets.

Process results, produce actionable data, and prioritize the findings based on business impact.

Act swiftly on your findings and report back to stakeholders in the format they need.

Ensure an Integrated Ecosystem

The ultimate goal of your red team is to better understand and improve upon your security ecosystem's effectiveness. This is why it's imperative your red team is armed with the right tools to properly integrate with your ecosystem and ensure each element generates the right contextual understanding of how it responds to an attack.

Security posture reporting should include a clear assessment of each security tool's ability to protect, prevent, and respond to threats and what type of alerts and events those tools produce. You can then unify all that information into a more holistic ecosystem analysis and output your results in a way that can be easily tracked and operationalized for continued growth and streamlined remediation efforts.

Prioritize Reliable Automation

Although we've listed it last, automation should be a primary objective of any red team plan from the outset to achieve true scalability. Talented red teamers will come and go, and building a skilled team takes a significant investment in people. Automation will help your red team stay consistent through the personnel ups and downs, but automation is not necessarily intended to replace skilled red team players. Rather, it will grant your team more bandwidth to focus on the activities where they can make the greatest impact, while leaving many of the day-to-day tasks needed to perform continuous security testing in the "hands" of a reliable, automated solution.

Automation also enables red teams to cover more of their environment and threat landscape than any individual or team could ever hope to—and with greater consistency and alignment by repeatedly testing the same scenarios without allowing the goal to become a moving target. Some organizations with the means and resources may opt to build their own red-team automation in house. Others will leverage general automation tools, and finally, there's the option to make a wise investment in a specialized security testing automation system that meets your business needs.

Looking Toward the Future: Continuous Red Teaming

Because attackers are continuously probing and attacking, cybersecurity never rests. This is more true today than ever, with the number of newly reported vulnerabilities having hit record levels in each of the past four years. Red teaming is a useful exercise that can help stress-test your security posture in a holistic way, understand how well people and systems react in case of a serious cyberattack, and identify areas for improvement. But, as pointed out above, traditional red-team approaches could be dramatically improved to better reflect the current reality of constant attacks and their growing sophistication.

Just as software development has moved toward continuous integration and continuous delivery (CI/CD) to support more frequent, reliable, and automated code changes, we believe red teaming will begin to transition away from specific bounded exercises toward a more continuous approach that consistently and reliably tests security posture. To do this, red teams will have to change the way they operate, the tools they use, and the mindset with which they plan their approach. To keep up with code velocity and rapid iterations, red teaming must become an "always-on" capability, rather than a special exercise requiring months of planning and execution.

While this may sound challenging, a BAS platform can provide the tool red teams need to enable continuous simulations of a wide variety of TTPs and playbooks of known attacks customized to the needs and risks of an organization.

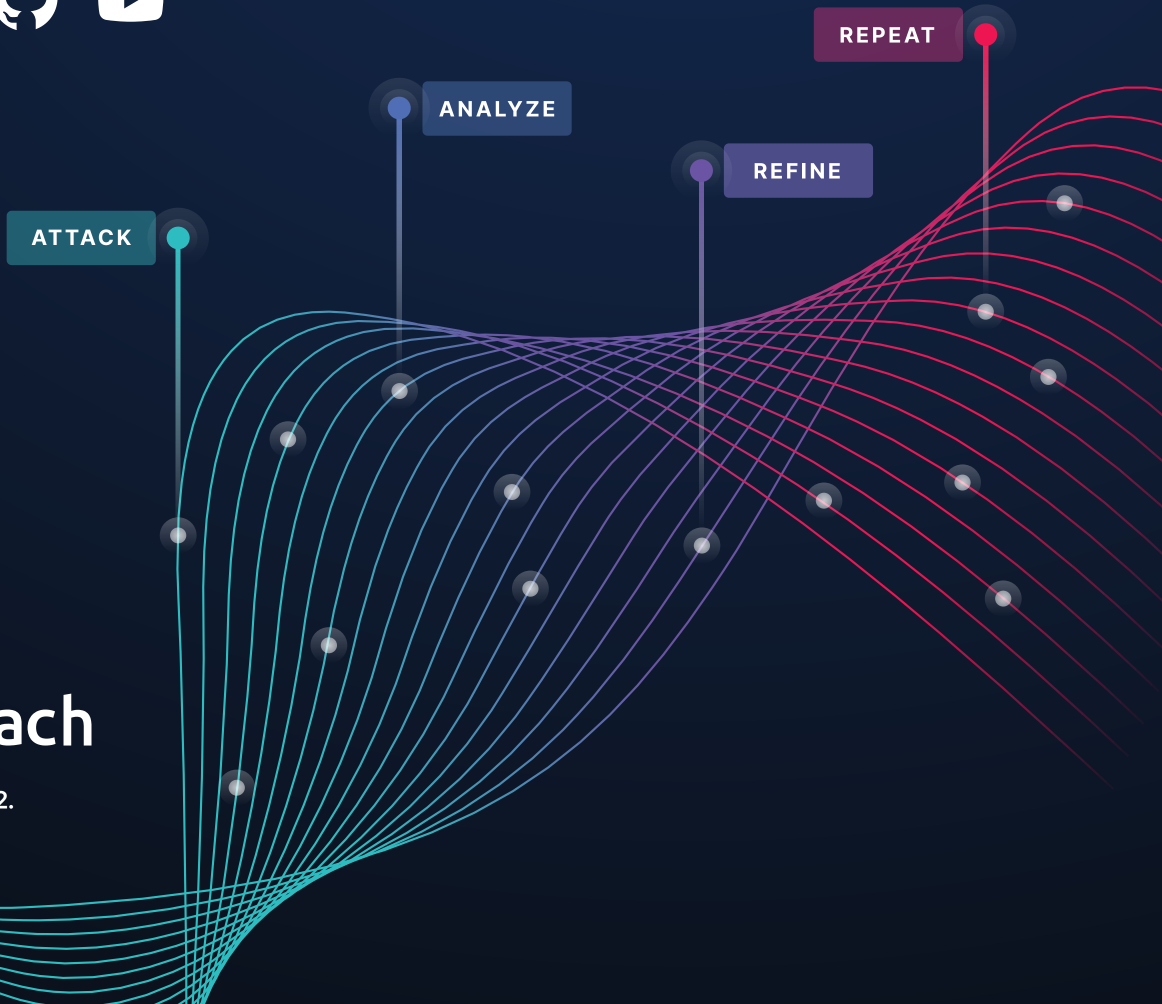
Check out **SafeBreach.com** for more red-team resources, and **schedule a personalized demo** now to discover how the SafeBreach BAS solution can become your red team's secret weapon.

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