ATTACKIQ®

TOP 6

Ways to Use Breach and Attack Simulation

CONTENTS

INTRODUCTION

Cybersecurity has become a top-tier security concern for organizations all over the world. With Gartner predicting that security and risk management spending will increase to the tune of $150 billion in 2021, chief information security officers (CISOs) need to maximize their cybersecurity investments and be confident that those investments protect their vital data effectively.

Breach and attack simulation (BAS) platforms are a means to that end. They help cybersecurity leaders find security gaps, prioritize program investments, and set up their organizations for success.

Here are 6 solutions that illustrate some of the most common applications of a breach and attack simulation platform.

AUTOMATED SECURITY CONTROL VALIDATION

Security teams need more than point-in-time status data about their security posture to achieve cybersecurity readiness. Companies use breach and attack simulation as a primary and foundational means to test and validate their security controls and ensure they work as they should. Real-time, continuous and—importantly—automated security control validation is critical for asset protection and to prevent attacks.

Information from an old, initial audit quickly becomes stale; a test conducted in early October should not be trusted as "true north" later that month, not to mention in January. Continuous automated security control validation is accomplished by running adversary attack emulations across controls to prove their effectiveness, or to expose security operations that require management attention.

Why is this new? Traditionally, "blue team" network defenders have focused their strategies on meeting baseline cybersecurity best-practices: correcting misconfigurations, administering patches, and deploying best-in-class commercial products. By using an automated security control validation platform, blue teams can now better validate security controls using adversary emulation as opposed to relying on a sporadic manual process to ensure they're working—and correct them quickly if they're not.

On the other side of the coin, with automated security control validation, red teams can quickly and easily run new tests and make them routine. Automated security control validation can operate at scale with real-time performance data on controls. In a resource-constrained environment, automated testing allows red teams to exercise in a light, affordable way to improve security effectiveness and efficiency, freeing up personnel resources to focus on more strategic problems that demand human attention.

> **Ultimately, automated security control validation enables purple teaming—collaborative communication between red and blue teams—where they can share threat information on adversarial tactics, techniques, and procedures and cooperate to close defensive gaps.**

It also extends beyond the initial control assessment and into the whole security pipeline. In managing a security incident, security operations teams need confidence that they can see and respond to an event efficiently, effectively, and quickly. If you are a member of a security operations team, you can use breach and attack simulation to assess all of the security technology sensors within your organization, including event logs, network security controls, and the SIEM, to ensure that the technology works as it should. Whether you are just building your security program or choosing a new commercial security vendor for your security needs, a BAS platform will help you assess competing security technologies and determine which one best meets your requirements—now and in the future.

Read more about this collaborative approach to a threat-informed defense in the Purple Teaming for Dummies eBook.

INVESTMENT DECISION SUPPORT

Data helps you determine the state of your assets, where you are getting value (or not), and what your business strategy should be to make the most of your investments. The only way to make these decisions is with an inventory and a data-driven assessment of how well your controls are working. Using the MITRE ATT&CK® framework and a breach and attack simulation platform, security leaders can run automated assessments, study performance data, set a strategy, and decide whether to invest or divest in specific areas to mitigate a discrepancy.

There are a number of tools available to help you understand how BAS can benefit your organization. Calculators like this one, for instance, can help you see how to save money by reducing costs of manual red team and penetration testing—and most teams see quick cost savings that can then be reinvested to fuel other areas of the business.

COMPLIANCE OPTIMIZATION

Over the last decade the cybersecurity compliance landscape grew increasingly complex with regulators following an array of recommended frameworks, from **Europe's General Data Protection Regulation (GDPR)** to the **National Institute of Standards and Technology (NIST) Special Publication 800-53** and the **Department of Defense's new Cybersecurity Mature Model Certification (CMMC)** to financial regulations like New York City's Department of Financial Services regulations. Still, compliance requirements can be ambiguous, and regulators will often look to you for how to achieve the objectives that they have set for you.

Compliance in and of itself does not equal security, however, and you can use a BAS platform to achieve increased security effectiveness while also proving to regulators that you are meeting their regulatory standards. We call this BAS-enabled solution "compliance optimization." In the compliance optimization process, you map your regulatory and compliance controls, conduct continuous tests against those specified controls to generate evidence about their effectiveness, make necessary changes to improve performance, and train your auditors to understand and report on your compliance readiness reporting. Regulators will want to see that your company has a process for validating effectiveness—and they'll want to see documentation. The compliance optimization process provides real proof of security effectiveness while concurrently reducing your regulatory and compliance burdens.

For more on how to conduct compliance optimization, enroll in our compliance optimization course, "*Uniting Threat and Risk Management with NIST 800-53 & MITRE ATT&CK.*"

MSSP AND COMMERCIAL SOLUTION EVALUATIONS

Many organizations use breach and attack simulation to assess commercial security solutions in the proof of concept phase and to assess Managed Security Solutions Providers (MSSP) performance after contract. Let's look at these two related concepts in turn.

Commercial Solutions Evaluations: Most technology companies allow potential customers to run a proof of concept before customers deploy the technology across their enterprise. Breach and attack simulation platforms generate performance data about which technology performs best in meeting your security requirements (to include specific regulatory or compliance needs). A number of organizations have used the platform for this initial purpose and in turn became AttackIQ customers after seeing the platform perform. As an added bonus, BAS can also be used to compare the effectiveness of commercial versus open-source security solutions.

MSSP Evaluations: One powerful breach and attack simulation solution is to assess MSSPs to maximize return on investment. If you have entered into a contract with an MSSP, you can use the platform to validate that the provider works in a timely manner and as intended during the course of the contract or during the proof of concept phase. Here's an illustration:

> **A financial services organization turned to the AttackIQ Security Optimization Platform to test its incident response security controls internally. This emulation triggered an internal control. The firm had previously contracted a large sum to an external MSSP to respond to an incident, but it took the MSSP five days to contact the firm after the test triggered the internal alert—which is far too long to avoid damage. The firm was able to contact the MSSP and ask them to alter their approach showing that a security optimization platform can do more than validate security controls—it can validate the MSSP's overall effectiveness. Such an evaluation points not just to technology effectiveness, but can also help you determine how well the external team performs in customer service functions, like responding to your requests for adjustments. This is one powerful way that a BAS platform can help organizations make the most of their financial resources.**

EXERCISE ENABLEMENT

Beyond testing analysts against specific certifications, you can use your breach and attack simulation platform to conduct a range of attacks to exercise your security team's capabilities (large or small scale) across the security organization or for a specific component of the security team. Using BAS, you can run an exercise in the actual production environment, not in a cyberrange sandbox. This makes the exercise more tangibly beneficial by focusing the team against a real-world adversary in a real-world environment.

In one case study, a U.S. military branch used the AttackIQ Security Optimization Platform to test the capabilities of its cyberdefense teams. According to a manager featured in the study, "AttackIQ holistically evaluates people, processes, and policies, as well as security technologies. We are building an...environment that will simulate attack campaigns, with the goal of helping our defenders lower their time to detect and respond to specific threats. We intend to consistently push similar attack sequences to see whether responses get faster with each iteration. If the time isn't decreasing, we will need to determine whether our systems or processes need improvement, or our soldiers need training."

MERGERS AND ACQUISITIONS

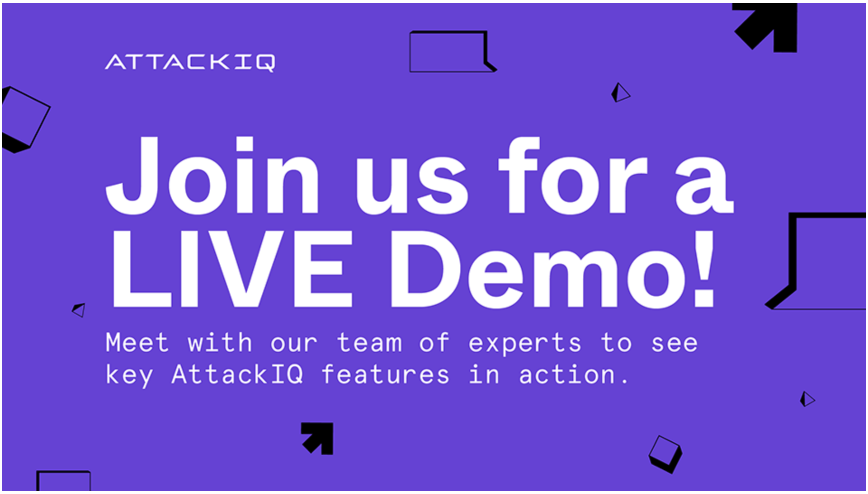
Organizations also use BAS to test the cybersecurity controls of onboarding companies during mergers and acquisitions to determine the level of risk and identify areas of improvement in advance of the deal finalizing. In this way, the acquiring company can negotiate a deal and find gaps or vulnerabilities in the onboarding company's capabilities—and then alter contract negotiations accordingly.

CONCLUSION

Breach and attack simulation platforms enable security teams to continuously validate that controls are working at scale and in production, ensure that their cybersecurity strategy is effective and efficient, and adapt to the ever-evolving threat landscape based on real-time, data-driven insights.

As the leaders in breach and attack simulation, the AttackIQ Security Optimization Platform gives customers the most consistent, trusted, and safest way to test and validate security controls. While competitors test in sandboxes, we allow you to test in production across the entire kill chain, the same as real-world adversaries do, emulating multi-stage attacks against your security infrastructure.

To learn more about how AttackIQ can help you achieve cybersecurity effectiveness and make the smartest decisions for your security program, sign up for a weekly demo.


ATTACKIQ
Join us for a LIVE Demo!
Meet with our team of experts to see key AttackIQ features in action.

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com