Cymulate
Extended Security Posture Management

Automated Pen Testing vs Breach & Attack Simulation

Ask the Right Questions, Get the Best Answers

Cymulate

Table of Contents

01 Defining Testing Goals: What Do You Need to Know?

Testing security controls is the only way to know if they are truly defending your organization. With multiple testing frameworks, tools, open-source options, and targets, there are many choices for testing plans. But, before you choose the right testing tools for your team, you need to understand what you are testing for in the first place.

Organizations want to know if an attacker can get into their system. However, there are different approaches to answering that question. One approach is to use pen-testing teams to attempt to breach your defenses.

A second approach is to test the effectiveness of each security control and the combined effectiveness of your overall security infrastructure with Breach and Attack Simulation (BAS).

This paper compares automated pen testing with BAS tools to help you determine which solution delivers the most value for your team.

02 Asking the Right Questions

In an ideal world, we could "set and forget" security controls, and attackers would decide to make honest livings. Since that's not realistic, security teams must continuously adapt defenses to fit the prevalent threat landscape. To successfully identify threats and reduce risk, teams must ask themselves two critical questions. The first question is "Are you testing the effectiveness of your security controls?" If you answer "yes" then it's a great start, but it does not indicate the type, breadth, or depth of testing being done. In actual practice, many security teams don't test all their controls against all threat vectors using the latest threat intelligence or adversary Tactics, Techniques and Procedures (TTPs).

Digging deeper, the next question is "which tools are you using to test your security controls?" Most organizations rely heavily on vendor-provided tools and automated pen testing solutions. While vendor-provided tools test the vendor's specific security solution—whether it's a web application firewall (WAF), EDR solution, or something else—automated pen testing is used to see if an attacker can penetrate specific areas of the organization. Frequently, automated pen testing is used to verify that controls meet compliance requirements, such as PCI DSS regulations, and are conducted by red teams as part of broader testing assessments and exercises.

Broadening the Questions

If you want to know if your security controls are effectively protecting against attacks, then you will need more insight:

Are interdependent controls correctly generating and delivering the right data? For example, are your web gateway, firewall, and behavior-based tools correctly alerting the SIEM when they detect suspicious activity?

Have security control configurations "drifted" over time or have they been incorrectly set? For instance, are controls actively detecting threats or were they left in monitoring mode?

If you have rolled out new technology or settings, how have they affected your security posture?

Are controls able to defend against the newest threats and variants?

Does your security defend against the latest stealth techniques, such as living off the land (LOTL) fileless attacks, deployed by sophisticated attackers?

Do you have visibility into security outcomes that require both human processes and technology?

Is your blue team able to identify and respond effectively to alerts?

03 Comparing Assessment Options

The questions you need to answer about your security controls will determine the type of testing to choose and how often testing is performed. If you only test your controls quarterly, it leaves a lot of time for threats to exploit any gaps or weaknesses between scheduled assessments because the real-world threat landscape evolves daily. Organizations need continuous insight and assessment feedback from their security controls to correctly prioritize and tune defenses. To complement point-in-time testing, BAS solutions continually challenge, measure, and optimize the effectiveness of security controls using automated testing technology.

Knowing the strength of automated pen testing and Breach and Attack Simulation (BAS) solutions enables you to choose the best testing approach, depending on your questions and data needed for decision making. Whether you are testing specific controls, multiple environments and network segments, or controls across the kill chain, you'll gain the most insight from using the tool best suited for the job.

Automated Pen Testing: Finding and Exploiting Weaknesses

Automated pen testing helps answer the question "can an attacker get in?" Automated pen tests assist in identifying vulnerable or high-risk pathways into an environment more quickly. They can emulate multiple threat actor techniques and even different payloads, but they typically don't replicate and fully automate the full TTPs of a real threat actor, so the environment could still be vulnerable to threat variants or highly expert attackers. Automated pen tests also still rely on skilled human pen testers, whose expertise can vary widely, making it difficul to gain consistent data over time or across all controls in your environment.

Even with automation, pen testing takes time to scope, conduct, and analyze, slowing your ability to respond accurately to current threats. These tools also tend to be weak at recognizing vulnerabilities in business logic, which can skew results. In addition, automated tools tend to generate more false positive alerts, which then require human investigation and analysis. Teams need the right automated pen testing tools to gain actionable data, but the variety of automated pen testing tools and approaches can actually complicate testing. For example, different attack vectors will require different testing tools. Not only does this make it more difficult to choose the right tools, but inconsistent tests also deliver results that are difficult to integrate and interpret.

BAS Tools for Qualitative and Quantitative Answers

Automated BAS tools enable you to answer a different question. Instead of "can an attacker penetrate my organization," BAS delivers answers to "how well do our controls and policies detect and stop attackers?" BAS tools model attacks, identify heat spots, and assess risk of all security elements. In addition, BAS enables continuous, comprehensive testing to challenge, measure, and optimize cyber defenses by:

01 Simulating attacks without jeopardizing production environments

02 Simulating cyberattacks across the full kill chain against all threats, including the latest attacker TTPs

03 Testing continuously with flexibility to target specific vectors, infrastructure, and internal teams for awareness against latest threats

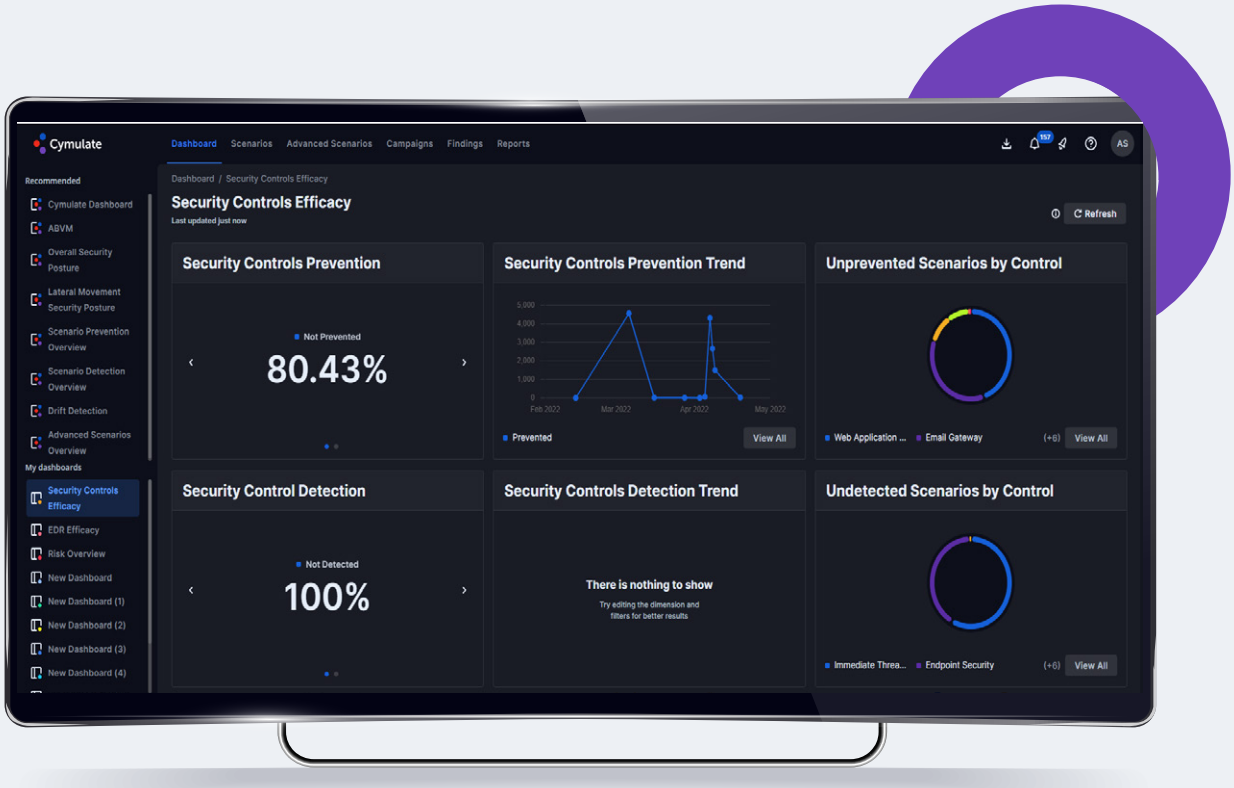
04 Automating simulations for repeatability and consistency

05 Conducting testing at any time interval—hourly, daily, weekly, or ad hoc

06 Identifying gaps and evaluate controls against the MITRE ATT&CK framework

07 Remediating exposure using actionable insights

With BAS, you can focus security control testing on techniques and paths that can be exploited by many different types of threat actors—without having to assemble teams of security experts. By utilizing technique-based frameworks, such as MITRE ATT&CK, your organization can effectively test against and neutralize multiple types of attacks simultaneously for real security against real-world threats.



The chart below provides an at-a-glance comparison of automated pen testing and BAS:

		Automated Pen Testing	Breach & Attack Simulation
Human requirements	Testing objective	Can attackers get in?	Are my security controls and policies effective?
	Expertise required	Medium-high to high internal expertise or outsourcing	Low expertise
	Testing interface	• Each script has different requirements and different tools have different interfaces, requiring user familiarity and long ramp-up times to prepare • Demands scripting and analysis expertise	• Highly visual, easy-to-use graphical user interface unified across tool • Low number of prerequisites, which accelerates preparation
Technical considerations	Scope	Challenges specific environments, specific controls or control groups, or mimic specific threats	Tests controls across entire kill chain
	Implementation	• Risky to perform on production environments • Uses real exploits seen in the wild, increasing risk of business disruption • Creating a separate testing environment can add equipment, maintenance, and support costs	• Safe to use on production environments • Uses safe simulations of threats to prevent business disruption • Customize tests to include specially developed payloads that mimic behavior of specific threats, such as ransomware, worms, and others
	System requirements	• Requires specific code libraries to be installed • Requires database to save reports • Requires separate test environment (if not running on production infrastructure) • Requires expertise to deploy, maintain, update, and use	Requires only one dedicated device

		Automated Pen Testing	Breach & Attack Simulation
Technical considerations	Maintenance	• Commercial tools require regular updating, which can reduce effectiveness if not updated in a timely manner • Open source tools should be monitored for availability of new features, ensuring that they include latest TTPs and align with changes in threat landscape	• Automatically updated without requiring organization to maintain. • Latest techniques and threat loCsare incorporated as soon as they are uncovered.
Testing deliverables	Visibility across vectors	Separate tests for separate vectors with little or no correlation or unified visibility	In-depth visibility across kill chain
	MITRE ATT&CK technique coverage	Limited coverage	Broad coverage
	Risk metric/ measurement/ exposure scores	• Defined individually by tool • Using multiple tools yields multiple scores across attack vectors, TTPs, and other characteristics	• Consistent across tests and vectors • Demonstrates security performance and proves effective spending over time • Enables comparing strength of competing security products • Simplifies discussions with executives, boards of directors, and risk managers
	Testing frequency	• Depends on customization capabilities of chosen tool • Requires expertise to customize	Continuously, scheduled, or ad hoc out of the box
	Automated reporting	• Depends on customization capabilities of chosen tool • Requires expertise to customize	Ready-to-use reports for executive and technical teams
	Automated alerting against baseline	• Depends on customization capabilities of chosen tool • Requires expertise to customize	Automatically included

Cymulate

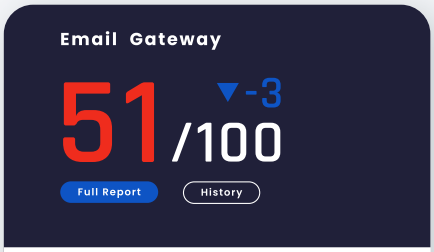
The Choice is Yours

For many organizations, there is no "either-or" choice of testing and assessment tools. The reality is you will need to continually challenge your security controls, uncover emerging weak spots, and tune controls to improve effectiveness. When cyber adversaries continue to up their games, you and your executive team need assurance that controls across the kill chain are indeed delivering the protection you need—every day, every hour, or every moment.

BAS tools deliver the continuous security control and cyber risk assessment data needed to achieve that goal.

Breach & Attack Simulation

1 Simulate
Simulate attacks across any vector.



2 Evaluate
Know where your company is exposed.

3 Remediate
Fix your security gaps.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632