Cymulate Business Justification

There is no downtime for cybersecurity. InfoSec professionals must constantly protect their organization against a wide variety of threats and answer on-demand:

- Are we secured?
- Where are controls performing strongly, and where do gaps exist?
- Do we have too many tools, or too few?
- Are my information security teams overwhelmed, or able to stay ahead of threat activity?
- Will our Incident Response protocols work as expected?
- Can I clearly report to senior leadership and the board on all of this?
- What will all these answers look like next week, next month, next quarter, next year?
- Will our cybersecurity programs scale adequately over time as the business grows and the threat landscape changes?

Many methodologies have evolved to assist organizations in getting a handle on this rapidly-shifting sphere. Continuous Threat Exposure Management (CTEM) devised by Gartner, the MITRE ATT&CK Framework® managed by MITRE, national standards from the Cybersecurity & Infrastructure Agency (CISA) in the United States, and Cybersecurity Emergency Response Teams (CERT's) throughout the world. They each define guidelines for a secure security program. However, their implementation does not guarantee protection when systems are not validated for correct operations or an emerging threat bypasses a tool that is functioning properly, but not designed for that level of detection.

As cybersecurity programs and practices evolve, organizations naturally have a need to find tools to effectively evaluate those operations. In the earlier stages of maturity, Breach and Attack Simulation (BAS) provides an effective starting point – noting that vendor implementations of BAS systems can vary widely and many will require highly experienced offensive testing staff. Next-generation designs that are cloud-based and operate with simulated attacks will be easiest to operate.

Where BAS alone may feel insufficient, organizations will add extended security validation through Attack-based Vulnerability Management (ABVM). This is designed to bring together BAS assessment results with information from a Vulnerability Manager (such as Qualys, Tenable, or InsightVM) to help more effectively prioritize remediation based on the conditions, strengths, and gaps within the security stack of the organization.

As cybersecurity maturity continues to evolve within an organization, they will want to assess their defenses against lateral movement propagation, more complex Web Application Firewalls, and next-generation network firewalls.

Cymulate Benefits

The Cymulate Platform is designed by offensive testing professionals and is built to scale and grow with the expertise and needs of the various security teams using it. The platform provides easy-to-use and extensive BAS. Unlike traditional BAS solutions, the platform also allows for expansion into extended control sets and the use of custom attack scripting and binaries for advanced validation programs.

Core Security Validation

Allows for any technology staffer from an IT Administrator to a Red-Teamer to perform broad-spectrum, non-disruptive and non-destructive assessments of Email Gateways, Web Gateways, and Endpoint Security. Through automation and continuous updates, the organization gains the benefits of BAS, without overwhelming cybersecurity employees.

Extended Security Validation

Brings the idea of BAS to areas of a cybersecurity practice not typically included in BAS solutions. This includes Attack-Based Vulnerability Management (ABVM) and brings together Cymulate assessment results with information from Vulnerability Managers to help understand and prioritize patching. Additionally, lateral movement assessments (using Cymulate's Hopper) challenge Network Detection and Response platforms and network segmentation. Data exfiltration defenses like Data Loss Prevention tools also be fully assessed for efficacy. Additionally, the external attack surface can be visualized from the perspective of an attacker, allowing the organization to determine and prioritize patching of true risk.

Full Kill-Chain Validation

Allows the organization to look at the whole as more than the sum of its parts. By creating entire attack flows from building blocks provided by Cymulate, blue-teamers and others who are less experienced in offensive testing can safely and accurately determine the efficacy of the security stack in its entirety – from infiltration to execution to potential impacts of any gaps that can be leveraged.

Advanced Scenario Validation

Extends the Platform to meet the needs of experienced offensive testing staff and red teams. With the ability to use custom code, scripting, binaries, and other objects; Advanced Scenarios deliver the flexibility necessary for more targeted and intrusive testing under the watchful eye of highly skilled professionals.

Automation

Is woven into every aspect of the Cymulate Platform. The Core Security and Extended Security Validation capabilities provide repeated assessments both on-demand and on set schedules for assessing exposures, confirming remediation, and closure of security gaps. With Advanced scenario automation the offensive testing staff can complete more testing, in more areas, more often. The automation will replace manual processes and discovery tasks to reduce employee burnout and enable employee productivity.

Multi-Level Reporting

Is native to the Cymulate Platform. In-depth technical reporting is available within the User Interfaces of the Cymulate Dashboard. It is also available offline in multiple formats for ease of use by technology professionals. This reporting also provides detailed remediation guidance so that corrective action can be taken quickly and effectively. Executive Reporting is available for every assessment and lays out the business rational and provides straightforward data for the decision-making by technology teams and those in other business practice areas (Finance, Board Members, etc.).

Integration and API Access

Share data from Cymulate allowing it to be used in other process systems and for security controls to feed data into Cymulate for correlation. Integrations allow technology teams to more quickly and effectively tune and troubleshoot security controls by seeing both the witnessed results of the actions Cymulate has taken, combined with the details of what that control saw and did – without violating Separation of Duty. API access allows the ticketing system and other orchestration tools to ingest data from Cymulate to power workflows, advise staff, and perform business intelligence.

Summation

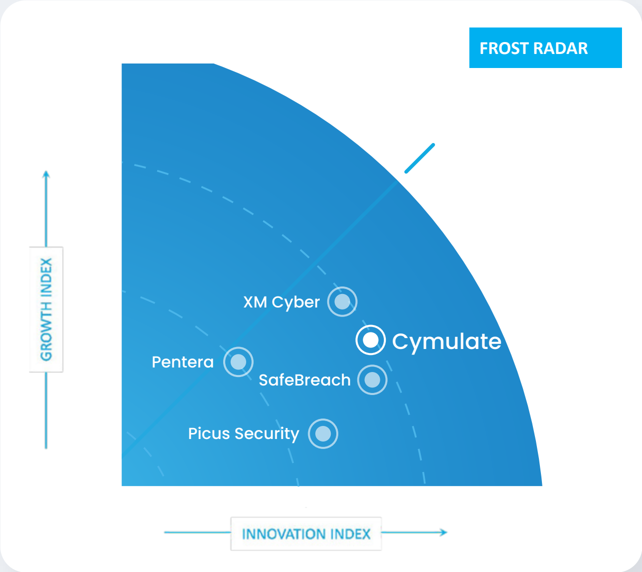
Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and to gain evidence for compliance and regulatory purposes.

Testimonials

Analyst Reviews

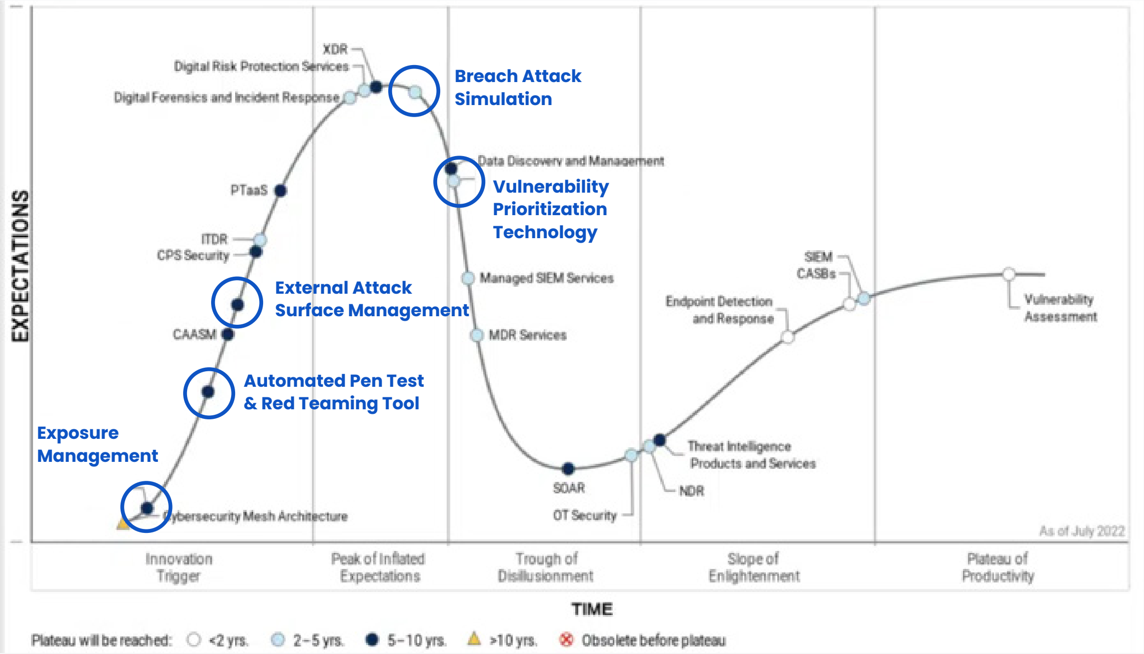
“As security becomes a business priority, Cymulate enables and empowers all stakeholders of the organization, including top management and business heads, to take risk-informed business decisions, without overwhelming the security teams or the CISO.”
Frost Radar™, 2022

“Cymulate provides high confidence that an enterprise is being protected by properly deployed security controls that are configured without vulnerabilities and operating according to expected security parameters.”
Tag Cyber Report, 2022



Frost Radar™ Breach and Attack Simulation Report, 2022

Cymulate has the widest coverage of emerging technologies in the Gartner Hype Cycle for Security Operations.



Gartner® Hype Cycle for Emerging Tech, 2022

Gartner Peer Insights

Cymulate

Cymulate Reviews

In Breach and Attack Simulation (BAS) Tools

4.8 ★★★★★ 100 Ratings

User Experience	Security Benefits	Business Impact
“Low operation cost and full automation out of the box” - Analyst	“In-depth security validation for the security minded” -Security and Risk Management	“Provides the most comprehensive picture a CISO needs to address his concerns and perform optimally” - Director of Information Security
“Easy to integrate the product in a corporate environment - Security and Risk Management	“The NextGen red team/blue team security testing tool” - Security and Risk Management	“Super easy to use and answers the tough boardroom questions” - CISO
“Fast visibility on your weak areas” - Infrastructure and Operations	"Like having a pen tester at your beck and call” - Security and Risk Management	“We have optimized our resources by using Cymulate” - CISO
“Easy validation, best reporting” - Analyst	“Great tool to stay up on emerging threats” - Infrastructure and Operations	“Elevates our relationship with clients as their partner and trusted security advisor” - Reseller Security Lead

Customer Quotes

> “With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk.”
>
> - Avinash Dharmadhikari, CISO, Persistent Systems

> “With Cymulate, I can validate controls against emerging threats faster than I could before.”
>
> - CSO, Global Hedge Fund

> “It is an efficient and productive solution for our team because we can use it to easily test the efficacy in a fire-and-forget automated manner.”
>
> - Ben Bennett, ISIO Chief Information Security Officer, ISIO

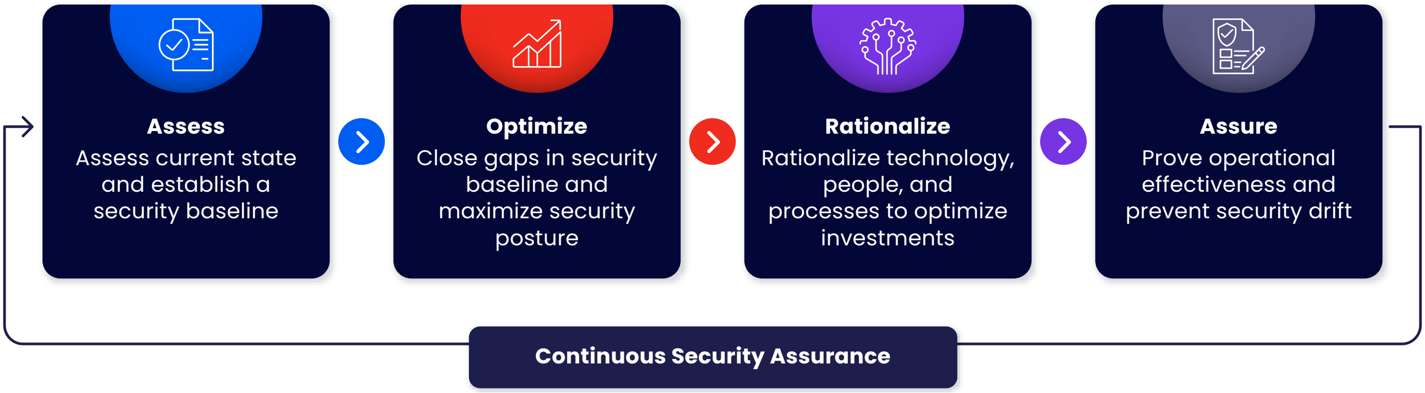
Scale and Grow with a Security Team's Maturity

The Cymulate Difference

Capability	Cymulate	Regular BAS	Difference
Core Security Testing	●	◕	In addition to basic BAS controls, Cymulate provides Immediate Threats, Email and Web Gateway, WAF, Endpoint, and Exfiltration assessments
Full Kill-Chain Testing	●	◕	Unique end-to-end attack testing out of the box
Automation	●	◕	Native and API-driven automation for both pre-built and custom assessment templates
Purple Team Framework	●	○	Wizard with a library of ready-made methods, production-safe payload, scripting, binaries, and other objects
Custom Code/Custom Binary Assessments	●	◔	Bypasses restrictions on event types that can be processed
Technical & Executive Reporting	●	◑	Interactive, dynamic, customizable, and exportable automated reporting
Integrations	◕	◑	Integrations for a wide variety of EDR/XDR, SIEM/SOAR, Firewall, and ITSM providers and support for custom queries.
API Support	◕	◑	API support for the entire of the platform
Vulnerability Management (VM)	●	○	VM prioritization based on in-context validation of exposure not compensated for by security controls
Remediation Ticketing	●	○	Integration with ticketing services to streamline remediation management

Full capability ● ◕ ◑ ◔ ○ No capability

How it Works



Assess
Assess current state and establish a security baseline

Optimize
Close gaps in security baseline and maximize security posture

Rationalize
Rationalize technology, people, and processes to optimize investments

Assure
Prove operational effectiveness and prevent security drift

Continuous Security Assurance

How Cymulate Increases Cybersecurity ROI

01 Cymulate validates the efficacy of each SIEM and SOAR tool by automatically correlating the number of production-safe attacks they detected, preempted, or mitigated to optimize existing defenses.

02 Measuring existing tools' effectiveness, identifying security gaps, and providing actionable remediation recommendations enable Cymulate to gain visibility into an organization's cybersecurity stack to eliminate overlapping capabilities and locate gaps.

03 With Attack-Based Vulnerability Management, organizations prioritize patching and reduce emergency patching workloads.

04 Immediate Threat Intelligence provides the ability to rapidly assess cyber resilience against emerging threats to prevent downtime due to delayed or inadequate patching.

05 Continuous security validation immediately detects security drift and enables remediation before the security posture shifts from a known good state to a bad state.

06 Cymulate's security risk score is quantified based on measurable events, providing a reliable numerical score that can be used as a base to harmonize baselines and KPIs, and monitor trends.

07 The platform's fact-based, quantified data enables informed decision-making.

08 Cymulate's data also facilitates M&A cyber due diligence in cases of prospective acquisition.

09 The platform can reduce cyber-insurance costs by providing documented proof that controls are indeed in place, continuously tested, and preventing security drift.

10 The platform provides an in-depth, quantified evaluation of an organization's cyber resilience which reassures potential investors about resilience to emerging threats and demonstrates the ability to vet prospective vendors for cyber risk.

11 To combat the investment of compliance requirements, Cymulate covers the most advanced continuous security validation technologies and automatically generates comprehensive risk assessment reports with a level of detail considerably superior to the current - and foreseeable future – regulators' demands.

12 By shrinking the number of false-positive alerts, rationalizing the tool stack, and automating the majority of repetitive tasks, Cymulate reduces the load of tasks with a negative impact on cybersecurity staff, freeing their time to conduct more high-level risk analysis, improving their job satisfaction level and reducing employee turnover.

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and to gain evidence for compliance and regulatory purposes.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com