Cymulate

What Makes Cybersecurity Posture Validation a Business Essential

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?

The Cymulate platform automatically validates that security programs are effective, continuously optimizes remediation efforts and admissible risk levels, and rationalizes requests for additional budget or headcount.

Named 2022 FROST RADAR™ Breach and Attack Simulation Report Innovation Leader, Cymulate's quantified risk evaluation bridges the communication gap between business leaders and tech teams that too often results from the lack of real, reliable, and accurate cybersecurity performance metrics.

Cymulate Security Posture Validation Platform Use Cases

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.

Breach and Attack Simulation (BAS)
Leverages simulated cyberattacks for security control validation, SIEM/SOAR optimization, security validation of cloud environments, and SOC & Incident Response optimization

Threat Exposure Assessment
Includes External Attack Surface Management, Full Kill Chain attack mapping, and validation of access and segmentation security policies

Attack-Based Vulnerability Prioritization
Identifies exploitable vulnerabilities and makes staff patching efforts more effective

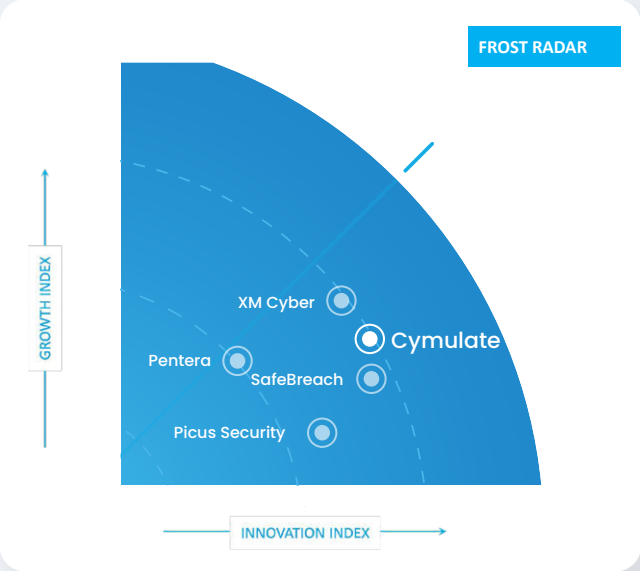
Business Benefits

- Measuring existing tools' effectiveness, identifying security gaps, and providing actionable remediation recommendations enables Cymulate to gain visibility into an organization's cybersecurity stack to eliminate overlapping capabilities and locate gaps.
- With Attack-Based Vulnerability Management, organizations prioritize patching and reduce emergency patching workloads.
- Immediate Threat Intelligence provides the ability to rapidly assess cyber resilience against emerging threats to prevent downtime due to delayed or inadequate patching.
- Continuous security validation immediately detects security drift and enables remediation before the security posture shifts from a known good state to a bad state.
- 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
- 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.
- The platform's fact-based, quantified data enables informed decision-making.
- Cymulate's data also facilitates M&A cyber due diligence in cases of prospective acquisition.
- The platform reduces cyber-insurance costs by providing documented proof that controls are indeed in place, continuously tested, and preventing security drift.
- 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.
- 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.
- 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 emploee turnover.

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

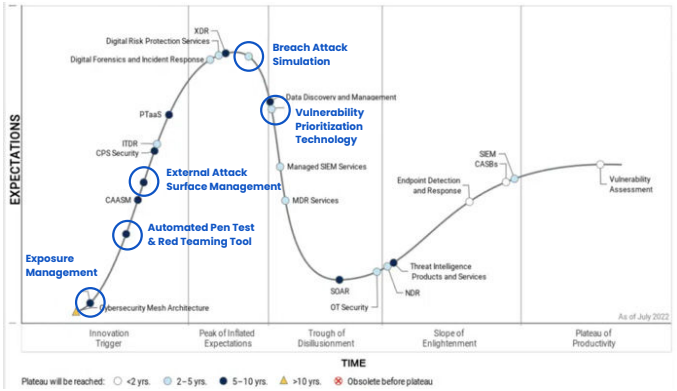
"Cymulate provides high confidence that an enterprise is being protected by properly deployed security controls that are configured without vulnerabilities and operating according to expected security parameters."
Tag Cyber Report, 2022



Frost Radar™ Breach and Attack Simulation Report, 2022

Cymulate

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



Gartner® Hype Cycle for Emerging Tech, 2022

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

Gartner Peer Insights

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
"Fast, effective, automated security efficacy testing" - Other CxO	"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

Summation

The Cymulate solution is recognized as the industry's most innovative security validation technology by multiple analysts and awards programs. It has achieved these accolated because the platform goes beyond BAS to provide a flexible and expandable platform for security control validation that meets the organization's technical and business needs not only for today but also over time as cybersecurity resilience and maturity needs evolve. Integrations allow for validation that cannot be identified from the results of assessments alone and allows for evaluation of the efficacy of human/technology hybrid operations like Incident Response. Complete reporting for both technical teams and business decision-makers provides the rationalization of both remediation efforts and cybersecurity spending where one or more controls do need to be upgraded or replaced.